Der p-adische Logarithmus & die p-adische Exponentialfunktion

Aus der Analysis kennen wir

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \in \mathbb{Q}[[x]]$$

und

$$\ln(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \in \mathbb{Q}[[x]]$$

aber was wenn wir diese Reihen in $\mathbb{Q}$ nun stattdessen in $\mathbb{Q}_p$ betrachten? $\implies$ Wir kriegen *fast* die gleichen Eigenschaften und ein paar coole Anwendung. Wir schreiben $\ln_p$ (aufpassen: das x^n ist jetzt $(x-1)^n$) und $\exp_p$ für die p-adischen Varianten. $\ln_p(1+x)$ hat wie in $\mathbb{R}$ einen Konvergenzradius von 1, bei $\exp_p$ hingegen kommt es auf p an. Für $p = 2$ ist der Konvergenzbereich $4\mathbb{Z}_2$ und ansonsten $p\mathbb{Z}_p$. Die Formeln $\ln_p(xy) = \ln_p(x) + \ln_p(y)$ und $\exp_p(x+y) = \exp_p(x)\exp_p(y)$ bleiben erhalten, weiterhin sind $\ln_p$ und $\exp_p$ zu einander im weitesten inverse Isomorphismen.

Definition

$$\ln_p(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

Theorem Wie beim reellen Logarithmus, haben wir

$$\ln_p(xy) = \ln_p(x) + \ln_p(y)$$

Beweis Betrachte die Reihen mit $\ln(1+x) + \ln(1+y) - \ln(1+x+y+xy) = 0$

■

Korollar

1. $\log(1/x) = -\log x$
2. $\log(x^n) = n \log x$ für alle $n \in \mathbb{Z}$
   Beweis Theorem mit $x(1+x) = 1$

Erinnerung Der Konvergenzradius einer Potenzreihe f ist

$$r = \frac{1}{\limsup |a_n|_p^{1/n}}$$

(wie im Reellen)

Theorem Der p-adische Logarithmus konvergiert für
$x \in B = \{\, x \in \mathbb{Z}_p \mid |x-1|_p < 1 \,\} = 1 + p\mathbb{Z}_p$
Beweis Wir haben $|a_n|_p = p^{v_p(n)}$ und $\lim\limits_{n\to\infty} |a_n|_p^{1/n} = 1$, da

$$\exp\left(\underbrace{-\frac{v_p(n)}{n}\ln p}_{\to 0^-}\right) \to 1$$

■

Genauso können wir eine p-adische Exponentialfunktion definieren.

Definition

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \in \mathbb{Q}_p[[x]]$$

Lemma Wir haben

$$v_p(n!) = \frac{n - \sum n_i}{p-1}$$

wobei n_i die Ziffern von n sind
Bewewis Es gibt $\lfloor n/p^k \rfloor$ Zahlen $\leq n$ welche durch p^k teilbar sind und d.h.
$\lfloor n/p^k \rfloor - \lfloor n/p^{k+1} \rfloor$ Zahlen von Bewertung k. Es folgt dass

$$v_p(n!) = \sum_{k\geq 1} k\left(\lfloor n/p^k \rfloor - \lfloor n/p^{k+1} \rfloor\right) = \sum_{k\geq 1} \lfloor n/p^k \rfloor$$

da $\lfloor n/p^k \rfloor = \sum\limits_{i\geq k} n_i p^{i-k}$ kriegen wir mit viel rumgerechne das folgende

$$\begin{aligned}
\sum_{k\geq 1} \lfloor n/p^k \rfloor &= \sum_{k\geq 1}\sum_{i\geq k} n_i p^{i-k} \\
&= 1/(p-1)\cdot\left(\sum_{k\geq 1}\sum_{i\geq k} n_i p^{i-k+1} - \sum_{k\geq 1}\sum_{i\geq k} n_i p^{i-k}\right) \\
&= 1/(p-1)\cdot\left(n + \sum_{k\geq 2}\sum_{i\geq k} n_i p^{i-k+1} - \sum_{k\geq 1}\sum_{i\geq k} n_i p^{i-k} - n_0\right) \\
&= 1/(p-1)\cdot\left(n - \sum_{k\geq 0} n_k\right)
\end{aligned}$$

■

Theorem Die p-adische Exponentialfunktion konvergiert in der Scheibe
$D_p = \{\, x \in \mathbb{Q}_p \mid |x|_p < r_p \,\}$ wobei $r_p = p^{-1/(p-1)}$ und divergiert ansonsten
Beweis Da $|a_n| = |1/n!| = p^{v_p(n!)} < p^{n/(p-1)}$ wissen wir, dass es definitiv für
$|x| < p^{-1/(p-1)}$ konvergiert. Sei nun $|x| = p^{-1/(p-1)}$ und $n = p^m$; in diesem Fall haben wir

$v_p(n!) = v_p(p^m!) = \frac{p^m-1}{p-1}$. Da aber $v_p(x) = 1/(p-1)$ haben wir

$$v_p\left(\frac{x^n}{n!}\right) = v_p\left(\frac{x^{p^m}}{p^m!}\right) = \frac{p^m}{p-1} - \frac{p^m-1}{p-1} = \frac{1}{p-1}$$

dies ist aber nicht von m abhängig, also kann $x^n/n!$ nicht gegen null gehen, und die Reihe nicht konvergieren.

■

Wie genau sieht D_p denn eigentlich aus?

Proposition $D_2 = 4\mathbb{Z}_2$ und ansonsten $D_p = p\mathbb{Z}_p$ für $p \neq 2$
Beweis Sei $p = 2$, dann ist $D_2 = \{\, x \in \mathbb{Q}_2 \mid |x|_2 < 1/2 \,\} = \{\, x \in \mathbb{Q}_2 \mid v_2(x) > 1 \,\} = 2^2\mathbb{Z}_2$.
Sei $p > 2$, wir haben

$$1/p < p^{-1/(p-1)} = \frac{1}{\sqrt[p-1]{p}} < 1$$

und somit ist $D_p = p\mathbb{Z}_p$

■

Proposition Analog zum Logarithmus haben wir $\exp_p(x+y) = \exp_p(x)\exp_p(y)$ falls $x, y \in D_p$
Beweis Analoger Beweis

$$\begin{aligned}
\exp_p(x+y) &= \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!}\binom{n}{k} x^{n-k}y^k \\
&= \sum_{n=0}^{\infty}\sum_{k=0}^{n} \frac{1}{n!}\frac{n!}{(n-k)!k!} x^{n-k}y^k \\
&= \sum_{n=0}^{\infty}\sum_{k=0}^{n} \frac{x^{n-k}}{(n-k)!}\frac{y^k}{k!} \\
&= \left(\sum_{m=0}^{\infty}\frac{x^m}{m!}\right)\left(\sum_{k=0}^{\infty}\frac{y^k}{k!}\right) \\
&= \exp_p(x)\exp_p(y)
\end{aligned}$$

■

Theorem Seien $f(X) = \sum a_n X^n$ und $g(X) = \sum b_n X^n$ zwei formale Potenzreihen mit $g(0) = 0$. Sei $h(X) = f(g(X))$. Falls die folgenden Voraussetzungen gegeben sind:

1. $g(x)$ konvergiert
2. $f(g(x))$ konvergiert
3. Für jedes n haben wir $|b_n x^n|_p \leq |g(x)|_p$
   dann konvergiert $h(x)$ und $f(g(x)) = h(x)$
   Beweis siehe z.B. Theorem 5.4.3. in Gouvea S. 124-127

Lemma Wir haben $|\exp_p(x)-1|_p<1$, $|\log_p(1+x)|_p<p^{-1/(p-1)}$, $\ln_p \exp_p x = x$, und $\exp_p \ln_p(1+x)=1+x$, für $x\in D_p$
Beweis Wir haben

$$|\frac{x^n}{n!}| = |x|^n p^{v_p(n!)} < |x|^n p^{n/(p-1)} < p^{-n/(p-1)}p^{n/(p-1)} = 1$$

es folgt dass

$$|\exp_p(x)-1| = \left|\sum_{n=1}^{\infty}\frac{x^n}{n!}\right| < 1$$

Wir können aber sogar noch ein besseres Resultat kriegen. Angenommen $n\geq 2$, dann ist

$$v_p\left(\frac{x^{n-1}}{n!}\right) = (n-1)v_p(x) - v_p(n!) > \frac{n-1}{p-1} - \frac{n-\sum n_i}{p-1} = \frac{\sum n_i - 1}{p-1} \geq 0$$

Es folgt dass

$$\left|\frac{x^{n-1}}{n!}\right| < 1 \implies \left|\frac{x^n}{n!}\right| < |x|$$

Wir haben also gezeigt, dass alle $n\geq 2$ Terme in $\exp_p$ kleiner sind als x, also ist durch das *strongest wins* Prinzip $|\exp_p(x)-1| = |x|$ und außerdem $|\exp_p(x)| > |x^n/n!|$ für $n\geq 2$. Somit ist Bedingung 3 im obigen Theorem erfüllt und wir können es anwenden. Analog zeigen wir die andere Richtung: wir haben $|n!|\leq |n|$ und somit

$$|x^n/n| \leq |x^n/n!|$$

Also falls $|x|<p^{-1/(p-1)}$ sagt uns die obige Ungleichung, dass

$$|x^n/n| \leq |x^n/n!| < |x|$$

Somit kriegen wir wie oben $|\log_p(1+x)| = |x| < p^{-1/(p-1)}$, d.h. ist $\log_p(1+x)$ in der Domain von $\exp_p$ und Bedingung 3 ist erfüllt

■

(man könnte auch einen anderen Weg anstelle vom obigen Theorem nehmen, nämlich über dichte und stetigkeit, heißt fg = id von dichter Teilmenge auf kompletten Raum übertragen falls stetigkeit herrscht)

Korollar/Lemma/Proposition $\exp_p$ (und auch $\ln_p$) ist eine Isometrie
Beweis

$$\begin{aligned}|\exp_p(x)-\exp_p(y)| &= |\exp_p(y)||\exp_p(x-y)-1| \\ &= |\exp_p(x-y)-1| = |x-y|\end{aligned}$$

wobei die letzte Gleichung dadurch erfolgt, dass 1 der größte Bewertete Term in $\exp_p(y)$ ist (strongest wins). Analog zeigt man $\ln_p$

■

Theorem $\exp_p$ definiert einen Isomorphismus zwischen D_p (additive) und $1 + D_p$ (multiplikativ), wessen inverse $\ln_p$ ist

■

Korollar Die multiplikative Gruppe $1 + D_p$ ist torsionsfrei, d.h. es existiert kein $1 \neq x \in 1 + D_p$ s.d. $x^m = 1$ für ein $m \in \mathbb{Z}_{>0}$
Beweis Die additive Gruppe $D_p \subseteq \mathbb{Q}_p$ ist torsionsfrei, die Behauptung folgt durch das obige Theorem

■

Lemma Sei H eine Untergruppe einer Topologischen Gruppe G. Falls H eine Umgebung des neutralen Elementes in G enthält, dann ist H abgeschloffen
Beweis

1. Sei V die obige Umgebung. Dann ist hV eine Umgebung für jedes beliebige $h \in H$ in G, welche wiederum in H enthalten ist. D.h. ist H eine Umgebung für alle seine Elemente und somit offen in G.
2. Betrachte die Nebenklassen gH von H in G. Da translationen homöomorphismen von G sind, sind Nebenklassen offene Mengen in G. Jede Vereinigung solcher Nebenklassen ist wieder offen. Aber H ist das Komplement der Vereinigung aller Nebenklassen $gH \neq H$, d.h. ist H abgeschlossen.

■

Lemma Sei $f : X \to Y$ eine Abbildung von topologischen Räumen, dann ist f stetig genau dann wenn f mit abschlüssen quasi-kommutiert, d.h. $f(\overline{U}) \subseteq \overline{f(U)}$ für alle $U \subseteq X$
Beweis Zeigen wir zuerst die eine Richtung. Sei f stetig, dann ist $f^{-1}(\overline{f(U)})$ geschlossen und enthält U. Wir haben deshalb außerdem $\overline{U} \subseteq f^{-1}(\overline{f(U)})$, dann $f(\overline{U}) \subseteq f(f^{-1}(\overline{f(U)})) \subseteq \overline{f(U)}$. Für die andere Richtung benutzen wir eine Kontraposition. Angenommen f sei nicht stetig. Dann existiert ein abgeschlossenes $V \subseteq Y$ sodass $f^{-1}(V)$ nicht geschlossen ist. Sei $X = f^{-1}(V)$, da X nicht geschlossen ist, existiert ein $p \in \overline{X} \setminus X$. Jetzt haben wir $f(p) \in f(\overline{X})$, aber $f(p) \notin V \supseteq \overline{f(X)}$, also ist $f(\overline{X}) \not\subseteq \overline{f(X)}$

■

Erinnerung (Theorem 2.11) $\mathbb{Z}$ ist dicht in $\mathbb{Z}_p$

Erinnerung (Proposition 1.46) Die Ideale in $\mathbb{Z}_p$ sind $\{ 0 \}$ $p^n\mathbb{Z}_p$

Lemma Die abgeschlossenen Untergruppen von $\mathbb{Z}_p$ sind $\{ 0 \}$ und $p^n\mathbb{Z}_p$
Beweis Wir haben

$$|x'a - xa| = |a||x' - x| \to 0 \quad (x' \to x)$$

weswegen Multiplikation in $\mathbb{Z}_p$ stetig ist. Nun sei H eine geschlossene Untergruppe, dann für beliebiges $h \in H$ haben wir

$$\mathbb{Z}_p h \subseteq \overline{\mathbb{Z}}h \subseteq \overline{\mathbb{Z}\, h} \subseteq \overline{\mathbb{Z}\, H} \subseteq \overline{H} = H$$

wobei der zweit letzte Schritt stimmt, da abelsche Gruppen $\mathbb{Z}$-module sind. Dies zeigt dass eine geschlossene Untergruppe ein Ideal ist.

■

Satz Sei p eine ungerade Primzahl, dann ist die Einheitengruppe von $\mathbb{Z}/p^n\mathbb{Z}$ zyklisch
Beweis Wir haben eine spaltende kurze exakte Sequenz

$$1 \to 1 + p\mathbb{Z}_p \to \mathbb{Z}_p^\times \to \mathbb{F}_p^\times \to 1$$

wobei der Schnitt/die Sektion(?) durch den Teichmüller Lift gegeben ist. Wenn wir nun modulo p^n reduzieren, kriegen wir eine spaltende kurze exakte Sequenz

$$1 \to G \to (\mathbb{Z}/p^n\mathbb{Z})^\times \to \mathbb{F}_p^\times \to 1$$

wobei G das Bild von $1 + p\mathbb{Z}_p$ unter $\mathbb{Z}_p^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ ist, d.h. ein endlicher Quotient von $1 + p\mathbb{Z}_p$. Die p-adische Exponentialfunktion gibt uns wie bekannt einen Isomorphismus $p\mathbb{Z}_p \cong 1 + p\mathbb{Z}_p$; da die Reduktion mod p^n klarerweise $p^n\mathbb{Z}_p$ als Kern hat und $p^n\mathbb{Z}_p \subseteq \mathbb{Z}_p$ (Komposition mit dem Iso.), ist G durch den ersten Isomorphiesatz zyklisch. Da $|G| = |(\mathbb{Z}/p^n\mathbb{Z})^\times|/|\mathbb{F}_p| = p^{n-1}$ haben wir

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong G \times \mathbb{F}_p^\times \cong C_{p^{n-1}} \times C_{p-1}$$

welches durch den Chinesischen Restsatz (CRT) zyklisch ist.

■

Erinnerung Die Menge der $(p-1)$ten Einheitswurzeln bildet eine zyklische Gruppe (cf Proposition 1.47)

Lemma Sei $p \equiv 1 \pmod 4$, dann existiert ein $i \in \mathbb{Q}_p$ mit $i^2 = -1$
Beweis Sei g ein Erzeuger der (obigen) Gruppe, wähle nun $i := g^{\frac{p-1}{4}}$

■

Definition/Proposition Sei $p \equiv 1 \pmod 4$, und wähle $i \in \mathbb{Q}_p$ sodass $i^2 = -1$.

Definiere

$$\sin_p x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1}$$

und

$$\cos_p x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n}$$

jeweils in $\mathbb{Q}_p[[x]]$. Wie im Reellen haben wir $\exp_p x = \cos_p x + i \sin_p x$
Beweis Analog zum Reellen

Erinnerung $\mathbb{C}_p$ ist die vervollständigung von $\bar{\mathbb{Q}}_p$ (algebraischer abschluss von $\mathbb{Q}_p$) wrt $|\cdot|_p$. Es hat folgende Eigenschaften:

1. $\mathbb{C}_p$ ist algebraisch abgeschlossen
2. $\mathbb{C}_p$ ist isomorph zu $\mathbb{C}$ als Körper, jedoch nicht als topologische Räume

Theorem (Straßmann, 1928) Sei $f \in \mathbb{C}_p[[x]]$ eine nicht triviale beschränkte Potenzreihe (in der Tate algebra). Dann hat f nur endlich viele nullstellen in $\mathbb{C}_p$
Beweis siehe z.B. Robert S. 306

■

Bemerkung Im obigen Theorem kann man sogar zeigen, dass die Anzahl der Nullstellen maximal N ist wobei N der größte Index ist mit $|a_N|_p = \max |a_n|_p$

Korollar Weder $\cos_p$ noch $\sin_p$ ist periodisch. Somit ist $\exp_p$ auch nicht periodisch.

■

Appendix

$$\ln(1+x) = \int \frac{1}{1+x} dx = \int (1 - x + x^2 - x^3 + \cdots) dx = x - x^2/2 + x^3/3 + \cdots = \sum$$

Der Teichmüller Lift ist die Abbildung welche ein beliebiges $\beta \in (\mathbb{Z}/p\mathbb{Z})^\times$ zu der eindeutigen $(p-1)$sten Einheitswurzel in $\mathbb{Z}_p^\times$ schickt, welche zu β reduziert (c.f. Proposition 1.47).

Proposition 3.3: $\sum a_n$ konvergiert iff $a_n \to 0$