מספרים p־אדיים: אנליזה ופונקציות זיתא

אלעד זלינגר

תקציר

רשימות אלו מבוססות על ההרצאות בקורס "מספרים p־אדיים: אנליזה ופונקציות זיתא" (סימול 0366-4983) שהועבר על ידי פרופסור דוד סודרי בסמסטר ב' שנת הלימודים תשע"ד באוניברסיטת תל אביב. אין המרצה אחראי לכל טעות שנפלה ברשימות אלה. לתגובות, תיקונים ועוד, אנא פנו לelad88 בgmail.

תוכן עניינים

1 פונקציית זטא של רימן ומספרי ברנולי 2
1.1 ההמשכה האנליטית של פונקציית זטא 2
1.2 מספרי ברנולי 7
1.2.1 דוגמאות 18
1.2.2 נוסחה לסכום $1^k + 2^k + 3^k + \cdots + (n-1)^k$ 21
1.3 תכונות מודולו p (ראשוני) של מספרי ברנולי, קונגרואנציית Kummer 24
1.3.1 ההערכה הp־אדית על $\mathbb{Q}$ 24
2 שדה המספרים הp־אדיים 38
2.1 ערך מוחלט על שדה 38
2.1.1 דוגמאות 39
2.2 השלמת שדות 45
3 הסגור האלגברי של $\mathbb{Q}_p$ והשדה $\mathbb{C}_p$ 56
3.1 שדות קומפקטיים מקומיים ומרחבים נורמיים ממימד סופי 56
3.2 הרחבת הערך המוחלט מF לשדה הרחבה סופית וספרבילית $K \supseteq F$ 60
3.2.1 תיאור נוסף של פונקציית הנורמה $N_{K/F}$ 62
3.3 הרחבות של $\mathbb{Q}_p$ 67
3.4 הלמה של הנזל 77
3.4.1 הקרקטר של Teichmuller 84
3.5 הרחבות לא מסועפות של $\mathbb{Q}_p$ 88
3.6 השדה $\mathbb{C}_p$ 92
4 טורי חזקות p־אדיים 99
4.1 טורים (מתכנסים) מעל $\mathbb{C}_p$ 99
4.2 טורי חזקות ב$\mathbb{C}_p$ כפונקציות בעיגול ההתכנסות 103
4.3 הפונקציה המעריכית והפונקציה הלוגריתמית 109
4.4 הטור הבינומי 123
5 אינטרפולציה p־אדית 126
5.1 אינטרפולציה של סדרת מספרים שלמים ע"י פונקציה רציפה $f : \mathbb{Z}_p \to \mathbb{Z}_p$ 126
5.2 משפט Mahler 129

5.3 המשכה אנליטית של פונקציות רציפות על $\mathbb{Z}_p$ 136
6 פונקציות־L p־אדיות 143
6.1 טורי L של דיריכלה 143
6.2 הגדרת פונקציית L ה־p־אדית 148

1 פונקציית זטא של רימן ומספרי ברנולי

1.1 ההמשכה האנליטית של פונקציית זטא

הגדרה 1.1 פונקציית זטא של רימן:

$$\zeta(s) = \sum_{\text{n}=1}^{\infty} \frac{1}{n^s}$$

מוגדרת ל־$s \in \mathbb{C}$, $\Re(s) > 1$
נשים לב כי

$$|\frac{1}{n^s}| = \frac{1}{n^{\Re(s)}}$$

אם $\Re(s) \geq \delta > 1$ אז הטור מתכנס בהחלט ובמידה שווה כי

$$|\frac{1}{n^s}| < \frac{1}{n^\delta}$$

ואז ממשפט ויירשטראס $\zeta(s)$ פונקציה אנליטית בחצי המישור $\Re(s) > 1$.

משפט 1.2 ל־$\zeta(s)$ יש המשכה אנליטית לכל המישור פרט לקוטב אחד, פשוט, ב־$s = 1$.

הוכחה: נתבונן באינטגרל $\int_1^\infty \frac{[x]}{x^{s+1}} dx$. מתקיים כי

$$|\frac{[x]}{x^{s+1}}| \leq \frac{1}{x^{\Re(s)}}$$

ולכן האינטגרל מתכנס בהחלט כאשר $\Re(s) > 1$.

$$\begin{aligned}
\int_1^\infty \frac{[x]}{x^{s+1}}dx &= \sum_{n=1}^{\infty}\int_n^{n+1}\frac{n}{x^{s+1}}dx = \\
&= \sum_{n=1}^{\infty} n\left[\frac{x^{-s}}{-s}\right]_n^{n+1} \\
&= \sum_{n=1}^{\infty}\frac{n}{s}\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right) = \\
&= \frac{1}{s}\sum_{n=1}^{\infty}\left(\underbrace{\frac{1}{n^{s-1}}-\frac{1}{(n+1)^{s-1}}}_{\text{Telescopic series}}+\frac{1}{(n+1)^s}\right) \\
&= \frac{1}{s}\left(1-\lim_{k\to\infty}\frac{1}{(k+1)^{s-1}}\right)+\frac{1}{s}\sum_{n=1}^{\infty}\frac{1}{(n+1)^s} \\
&= \frac{\zeta(s)}{s}
\end{aligned}$$

קיבלנו $\zeta(s) = s\int_1^\infty \frac{[x]}{x^{s+1}}dx$. מכאן

$$\begin{aligned}
\zeta(s) &= s\int_1^\infty \frac{[x]}{x^{s+1}}dx \\
&= s\int_1^\infty \frac{x-\{x\}}{x^{s+1}}dx \\
&= s\int_1^\infty \frac{dx}{x^s} - s - s\int_1^\infty \frac{\{x\}}{x^{s+1}}dx \\
&= s\left[\frac{-x^{s+1}}{-s+1}\right]_1^\infty - s\int_1^\infty \frac{\{x\}}{x^{s+1}}dx \\
&= \frac{s}{s-1} - s\int_1^\infty \frac{\{x\}}{x^{s+1}}dx
\end{aligned}$$

באינטגרל השני, האינטגרד רציף למקוטעין וחסום ע"י $\frac{1}{x^{\Re(s)+1}}$, ולכן אינטגרבילי כאשר $\Re(s) > 0$.
הוא אנליטי בתחום זה:

$$\int_1^\infty \frac{\{x\}}{x^{s+1}}dx = \sum_{n=1}^{\infty}\underbrace{\int_n^{n+1}\frac{x-n}{x^{s+1}}dx}_{f_n(s)}$$

$f_n(s)$ אנליטית בכל המישור: נסמן

$$\varphi_n(x,s) = \frac{x-n}{x^{s+1}}$$

φ_n רציף ואנליטי בשני המשתנים בתחום $U \times [n,n+1]$ כאשר U עיגול סגור ולכן רציף במידה שווה ולכן

$$\max_{\substack{n\le x\le n+1\\ s\in U}} |\varphi_n(x,s+h)-\varphi_n(x,s)| \underset{h\to 0}{\longrightarrow} 0$$

ולכן $f_n(s)$ רציף.
תהי γ מסילה סגורה במישור. אז

$$\begin{aligned}\int_\gamma f_n(s)ds &= \int_\gamma \int_n^{n+1} \varphi_n(x,s)dxds \\ &= \int_n^{n+1} \underbrace{\left(\int_\gamma \varphi_n(x,s)ds\right)}_{0} dx\end{aligned}$$

ממשפט מוררה, $f_n(s)$ אנליטית בכל המישור.
נעריך את $f_n(s)$:

$$\begin{aligned}|f_n(s)| &\le \int_n^{n+1} \frac{1}{x^{\Re(s)+1}}dx \\ &= [\frac{x^{-\Re(s)}}{-\Re(s)}]_n^{n+1} \\ &= \frac{1}{\Re(s)}\left(\frac{1}{n^{\Re(s)}} - \frac{1}{(n+1)^{\Re(s)}}\right)\end{aligned}$$

כעת בתחום $\Re(s) \ge \delta$ מתקיים

$$\begin{aligned}\sum_{n=M}^{N+M-1} |f_n(s)| &\le \frac{1}{\Re(s)}\left(\frac{1}{N^{\Re(s)}} - \frac{1}{(N+M)^{\Re(s)}}\right) \\ &\le \frac{1}{\delta}\cdot\frac{1}{N^\delta}\underset{N\to\infty}{\longrightarrow} 0\end{aligned}$$

לכן הטור $\sum_{n=1}^{\infty} f_n(s)$ מתכנס בהחלט ובמידה שווה בכל תחום מהצורה $\Re(s) \ge \delta$ לכל $\delta > 0$. ממשפט ויירשטראס, הטור הזה אנליטי בתחום $\Re(s) > 0$.
מתקיים כי ל $\Re(s) > 1$

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \frac{\{x\}}{x^{s+1}}dx$$

מאחר והראנו כי האינטגרל האחרון פונקציה אנליטית ל$\Re(s) > 0$, נוכל להרחיב את $\zeta(s)$ (ביחידות) לפונקציה אנליטית ל$\Re(s) > 0$, $s \neq 1$ ע"י הגדרתה ע"י נוסחה זו.
נשים לב כי ל$\zeta(s)$ מהגדרה זו יש בבירור קוטב פשוט $s = 1$:

$$\lim_{s\to 1} (s-1)\,\zeta(s) = \lim_{s\to 1} \left(s - s\,(s-1)\int_1^{\infty} \frac{\{x\}}{x^{s+1}}dx\right) = 1$$

נמשיך:

$$\begin{aligned}\int_1^{\infty} \frac{\{x\}}{x^{s+1}}dx &= \sum_{n=1}^{\infty}\int_n^{n+1} \frac{x-n}{x^{s+1}}dx \\ &= \sum_{n=1}^{\infty}\int_0^{1} \frac{u}{(u+n)^{s+1}}du\end{aligned}$$

נחשב

$$\begin{aligned}\int_0^{1} \frac{u}{(u+n)^{s+1}}du &= \int_0^{1} \left(\frac{u^2}{2}\right)' \frac{1}{(u+n)^{s+1}}du \\ &= \frac{1}{2\,(1+n)^{s+1}} - \frac{1}{2}\int_0^{1} \frac{u^2(-s-1)}{(u+n)^{s+2}}du \\ &= \frac{1}{2\,(n+1)^{s+1}} + \frac{s+1}{2}\int_0^{1} \frac{u^2}{(u+n)^{s+2}}du\end{aligned}$$

לכן

$$\begin{aligned}\int_1^{\infty} \frac{\{x\}}{x^{s+1}}dx &= \sum_{n=1}^{\infty}\int_0^{1} \frac{u}{(u+n)^{s+1}}du \\ &= \frac{1}{2}\sum_{n=1}^{\infty} \frac{1}{(n+1)^{s+1}} + \frac{s+1}{2}\sum_{n=1}^{\infty}\int_0^{1} \frac{u^2}{(u+n)^{s+2}}du \\ &= \frac{1}{2}\left(\zeta(s+1) - 1\right) + \frac{s+1}{2}\int_1^{\infty} \frac{\{x\}^2}{x^{s+2}}dx\end{aligned}$$

משיקול דומה לשיקול קודם, מתקיים כי $\int_1^{\infty} \frac{\{x\}^2}{x^{s+2}}dx$ אנליטי ומתכנס כאשר $\Re(s) > -1$. לכן קיבלנו כי

$$\zeta(s) = \frac{s}{s-1} - \frac{s}{2}\left(\zeta(s+1)-1\right) - \frac{s\left(s+1\right)}{2}\int_1^\infty \frac{\{x\}^2}{x^{s+2}}dx$$

מתקיים כי $\zeta(s+1)$ אנליטית כאשר $\Re(s)+1>0$, פרט לקוטב פשוט כאשר $s+1=1$. מאחר ומפיע באגף ימין הביטוי $\frac{s}{2}\zeta(s+1)$, הקוטב ב$s=0$ מצטמצם ולכן קיבלנו ביטוי בצד ימין שאנליטי ל$\Re(s)>-1$, פרט לקוטב פשוט ב$s=1$. מכאן שוב נוכל להרחיב (ביחידות) את $\zeta(s)$ לפונקציה אנליטית בתחום $\Re(s)>-1$ פרט לקוטב פשוט כאשר $s=1$.

הנחת האינדוקציה: יהי m טבעי, ל$\zeta(s)$ יש המשכה אנליטית יחידה ל$\Re(s)>1-m$ פרט לקוטב פשוט ב$s=1$ וקיימת הזהות:

$$\begin{aligned}\zeta(s) &= \frac{1}{s-1}+1-\sum_{r=1}^{m}\left(\frac{s(s+1)\dots(s+r-1)}{(r+1)!}\right)\left(\zeta(s+r)-1\right)\\ &\quad -\frac{s(s+1)\dots(s+m)}{(m+1)!}\int_1^\infty\frac{\{x\}^{m+1}}{x^{s+m+1}}dx\end{aligned}$$

נשים לב שבדומה לקודם $\int_1^\infty \frac{\{x\}^{m+1}}{x^{s+m+1}}dx$ מתכנס ואנליטי בתחום $\Re(s)>-m$ וכי $\zeta(s+r)$ אנליטי כאשר $\Re(s)+r>1-m$, כלומר כאשר $\Re(s)>1-r-m$ ובפרט כאשר $\Re(s)>-m$, פרט לקוטב פשוט כאשר $s+r=1$, כלומר כאשר $s=1-r$. במקרה הזה, $\zeta(s+r)$ מוכפלת בין השאר ב$(s+r-1)$, מה שמבטל את הקוטב. ע"י אינטגרציה בחלקים כמקודם מקבלים מהנחת האינדוקציה את צעד האינדוקציה. לכן נוכל להרחיב את $\zeta(s)$ לפונקציה אנליטית על כל המישור פרט לקוטב פשוט ב$s=1$. ■

מסקנה 1.3 נציב $s=1-m$ לm טבעי בנוסחה הרקורסיבית. כיוון שהאינטגרל הנ"ל רציף (אנליטי) כאשר $\Re(s)>-m$, אז הגורם $s+m-1$ שעומד מימינו מאפס אותו.

$$\begin{aligned}\zeta(1-m) &= 1-\frac{1}{m}-\sum_{r=1}^{m-1}\left(\frac{(1-m)(2-m)\dots(r-m)}{(r+1)!}\right)\left(\zeta(1-m+r)-1\right)\\ &\quad -\lim_{s\to1-m}\left(\frac{s(s+1)\dots(s+m-1)}{(m+1)!}\right)\left(\zeta(s+m)-1\right)\\ &= 1-\frac{1}{m}+\frac{(-1)^m}{m\left(m+1\right)}-\sum_{r=1}^{m-1}(-1)^r\left(\frac{(m-1)(m-2)\dots(m-r)}{(r+1)!}\right)\left(\zeta(1-m+r)-1\right)\\ &= 1-\frac{1}{m}+\frac{(-1)^m}{m\left(m+1\right)}+\frac{1}{m}\sum_{r=1}^{m-1}(-1)^r\binom{m}{r+1}-\sum_{r=1}^{m-1}(-1)^r\binom{m-1}{r}\frac{\zeta(1-m+r)}{r+1}\\ &= \frac{(-1)^m}{m\left(m+1\right)}-\sum_{r=1}^{m-1}(-1)^r\binom{m-1}{r}\frac{\zeta(1-m+r)}{r+1}\end{aligned}$$

(המעבר האחרון נובע מכך ש$1-\frac{1}{m}=-\frac{1}{m}((1-1)^m-1+m)=-\frac{1}{m}\sum_{r=2}^{m}(-1)^r\binom{m}{r}$)

בפרט ניתן לקבל מנוסחה זו $\zeta(0) = -\frac{1}{2}$, $\zeta(1) = -\frac{1}{12}$.
מכאן $\zeta(1-m)$ רציונלי לכל m טבעי.

1.2 מספרי ברנולי

נתבונן בפונקציה

$$f(z) = \frac{z}{e^z - 1}$$

לפונקציה זו יש קטבים ב$z = 2\pi ik$ כאשר $0 \neq k \in \mathbb{Z}$.
נוכל לכן לפתח את f לטור טיילור מסביב לראשית:

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} z^k$$

כאשר $|z| < 2\pi$.

הגדרה 1.4 המספרים B_k נקראים מספרי ברנולי.

מטרתנו להוכיח את הטענה הבאה:

טענה 1.5 יהי k מספר טבעי אז

$$\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{(-1)^{k+1} (2\pi)^{2k}}{2(2k)!} B_{2k}$$

בכתיב של אנליסטים p־אדיים:

$$\zeta(2k) = (-1)^k \pi^{2k} \cdot \frac{2^{2k-1}}{(2k-1)!} \left(-\frac{B_{2k}}{2k} \right)$$

(נבין את הכתיבה הזו בהמשך)

לפני שנוכיח את הטענה, נצטרך הכנה:

למה 1.6 לכל n טבעי אי־זוגי קיימים פולינומים $P_n(t), Q_{n-1}(t) \in \mathbb{Z}[t]$ ממעלות $\deg P_n(t) \leq n$, $\deg Q_{n-1}(t) \leq n-1$ כך ש

$$\begin{aligned} \sin(nx) &= P_n(\sin x) \\ \cos(nx) &= \cos x \cdot Q_{n-1}(\sin x) \end{aligned}$$

הוכחה: $n = 2k+1$.
אם $n=1$ נבחר פשוט $P_1(t)=t$, $Q_0(t)=1$.
שלב האינדוקציה:

$$\begin{aligned}
\sin\left((2k+1)\,x\right) &= \sin\left((2k-1)\,x+2x\right)\\
&= \sin\left((2k-1)\,x\right)\cos\left(2x\right)+\cos\left((2k-1)\,x\right)\sin\left(2x\right)\\
&= P_{2k-1}(\sin x)\left(1-2\sin^2 x\right)+Q_{2k-2}\left(\sin x\right)\cos x\cdot 2\sin x\cos x\\
&= P_{2k-1}(\sin x)\left(1-2\sin^2 x\right)+2Q_{2k-2}\left(\sin x\right)2\sin x\left(1-\sin^2 x\right)
\end{aligned}$$

באופן דומה:

$$\begin{aligned}
\cos((2k+1)x) &= \cos((2k-1)x)\cos(2x)-\sin((2k-1)x)\sin(2x)\\
&= \cos x\cdot Q_{2k-2}(\sin x)(1-2\sin^2 x)-P_{2k-1}(\sin x)2\sin x\cos x\\
&= \cos x\left(Q_{2k-2}(\sin x)(1-2\sin^2 x)-P_{2k-1}(\sin x)2\sin x\right)
\end{aligned}$$

■

לפולינום $P_n(t)$ התכונות הבאות:

$$\begin{aligned}
\sin(nx) &= P_n(\sin x)\\
P_n(0) &= 0
\end{aligned}$$

נגזור:

$$n\cos(nx) = P_n'(\sin x)\cdot\cos x$$

ב־$x=0$ נקבל:

$$n = P_n'(0)$$

נוכל לכן לכתוב

$$\begin{aligned}
P_n(t) &= nt+a_2t^2+\ldots+a_nt^n\\
\sin(nx) &= n\sin x+a_2\sin^2 x+\ldots+a_n\sin^n x
\end{aligned}$$

כאשר $a_i\in\mathbb{Z}$. כזכור, $n=2k+1$. נקבל לכן

$$\frac{\sin(nx)}{n\sin x} = 1 + b_1\sin x + \ldots + b_{2k}\sin^{2k} x$$

כאשר $b_i \in \mathbb{Q}$.
אם נציב $x = \pm\frac{\pi r}{n}$ כאשר $r = 1,2,\ldots,k$, אגף שמאל מתאפס.
נסמן לרגע $\tilde{P}_{2k}(t) = 1 + b_1 t + \ldots + b_{2k}t^{2k}$. אז $\{\pm\sin\frac{\pi r}{n}\}_{r=1}^{k}$ הם $2k$ שורשים שונים זה מזה של $\tilde{P}_{2k}(t)$.
לכן

$$\begin{aligned}\tilde{P}_{2k}(t) &= \prod_{r=1}^{k}\left(1-\frac{t}{\sin(\frac{\pi r}{n})}\right)\left(1+\frac{t}{\sin(\frac{\pi r}{n})}\right)\\ &= \prod_{r=1}^{k}\left(1-\frac{t^2}{\sin^2(\frac{\pi r}{n})}\right)\end{aligned}$$

מסקנה 1.7

$$\frac{\sin((2k+1)x)}{(2k+1)\sin x} = \prod_{r=1}^{k}\left(1-\frac{\sin^2 x}{\sin^2(\frac{\pi r}{2k+1})}\right)$$

נציב $\frac{\pi x}{2k+1}$ במקום x ונקבל.

$$\frac{\sin(\pi x)}{(2k+1)\sin(\frac{\pi x}{2k+1})} = \prod_{r=1}^{k}\left(1-\frac{\sin^2(\frac{\pi x}{2k+1})}{\sin^2(\frac{\pi r}{2k+1})}\right)$$

נשאיף את k לאינסוף ונקבל

$$\begin{aligned}\frac{\sin(\pi x)}{(2k+1)\sin(\frac{\pi x}{2k+1})} &= \frac{\sin(\pi x)}{\pi x}\cdot\frac{\frac{\pi x}{2k+1}}{\sin(\frac{\pi x}{2k+1})}\\ \lim_{k\to\infty}\frac{\sin(\pi x)}{(2k+1)\sin(\frac{\pi x}{2k+1})} &= \frac{\sin(\pi x)}{\pi x}\end{aligned}$$

קיבלנו את המסקנה הבאה:

$$\lim_{k\to\infty}\prod_{r=1}^{k}\left(1-\frac{\sin^2(\frac{\pi x}{2k+1})}{\sin^2(\frac{\pi r}{2k+1})}\right) = \frac{\sin(\pi x)}{\pi x}$$

טענה 1.8 קיימת המכפלה $\prod_{r=1}^{\infty}\left(1-\frac{x^2}{r^2}\right)$, במובן הבא: יהי N טבעי ונניח $|x| < N$, $x \in \mathbb{C}$. אז קיים ושונה מאפס הגבול $\lim_{k\to\infty}\prod_{r=N+1}^{k}\left(1-\frac{x^2}{r^2}\right)$
ואז נגדיר

$$\prod_{r=1}^{\infty}\left(1-\frac{x^2}{r^2}\right) = \prod_{r=1}^{N}\left(1-\frac{x^2}{r^2}\right)\cdot\lim_{k\to\infty}\prod_{r=N+1}^{k}\left(1-\frac{x^2}{r^2}\right)$$

הוכחה: יהי N טבעי נתון. נניח כי $|x| < N$. נתבונן בסכום

$$\sum_{r=N+1}^{k}\log\left(1-\frac{x^2}{r^2}\right)$$

כאשר $\log$ הענף הראשי של הלוגריתם.
אם $1-\frac{x^2}{r^2} \le 0$ (בפרט ממשי), אז x^2 ממשי וכן $x^2 \ge r^2$ כי אז $|x|^2 = |x^2| \ge r^2 > N^2$ בעוד $|x| < N$.
$|\frac{x^2}{r^2}| < 1$ ולכן נוכל להשתמש בפיתוח טיילור:

$$\log(1+z) = \sum_{l=1}^{\infty}\frac{(-1)^{l+1}z^l}{l} \qquad (|z|<1)$$

כלומר

$$\log\left(1-\frac{x^2}{r^2}\right) = -\sum_{l=1}^{\infty}\frac{x^{2l}}{l\cdot r^{2l}}$$
$$\sum_{r=N+1}^{k}\log\left(1-\frac{x^2}{r^2}\right) = -\sum_{r=N+1}^{k}\sum_{l=1}^{\infty}\frac{x^{2l}}{l\cdot r^{2l}}$$

הטור $\sum_{r=N+1}^{k}\sum_{l=1}^{\infty}\frac{x^{2l}}{l\cdot r^{2l}}$ מתכנס בהחלט:

$$\begin{aligned}
|\frac{x^{2l}}{l\cdot r^{2l}}| &\le |\frac{x^2}{r^2}|^l \\
\sum_{l=1}^{\infty}|\frac{x^{2l}}{l\cdot r^{2l}}| &\le \sum_{l=1}^{\infty}|\frac{x^2}{r^2}|^l \\
&= \frac{|x|^2}{r^2}\cdot\frac{1}{1-\frac{|x|^2}{r^2}} \\
&= \frac{|x|^2}{r^2-|x|^2}
\end{aligned}$$

ע"י השוואה לטור $\sum_{r=N+1}^{\infty}\frac{1}{r^2}$, נקבל כי הטור $\sum_{r=N+1}^{\infty}\frac{|x|^2}{r^2-|x|^2}$ מתכנס.
קיים לכן הגבול

$$\lim_{k\to\infty}\sum_{r=N+1}^{k}\log\left(1-\frac{x^2}{r^2}\right) = -\sum_{r=N+1}^{\infty}\sum_{l=1}^{\infty}\frac{x^{2l}}{l\cdot r^{2l}}$$

מרציפות הפונקציה e^z, קיים הגבול

$$\lim_{k\to\infty}\prod_{r=N+1}^{k}\left(1-\frac{x^2}{r^2}\right) = \exp\left(-\sum_{r=N+1}^{\infty}\sum_{l=1}^{\infty}\frac{x^{2l}}{l\cdot r^{2l}}\right)$$

■

נשים לב כי

$$f_r(x) = \sum_{l=1}^{\infty}\frac{x^{2l}}{l\cdot r^{2l}}$$

הן אנליטיות בעיגול $|x|<N$.
כמו כן

$$\begin{aligned}|f_r(x)| &\le \frac{|x|^2}{r^2-|x|^2}\\ &< \frac{N^2}{r^2-N^2}\end{aligned}$$

ולכן $\sum_{r=N+1}^{\infty}f_r(x)$ מתכנס במידה שווה ב$|x|<N$. ממשפט ויירשטראס הוא מגדיר שם פונקציה אנליטית.
מכאן $\prod_{r=N+1}^{\infty}\left(1-\frac{x^2}{r^2}\right)$ אנליטית ב $|x|<N$.

מסקנה 1.9 $\prod_{r=1}^{\infty}\left(1-\frac{x^2}{r^2}\right)$ אנליטית בכל המישור.

טענה 1.10 לכל $x\in\mathbb{C}$ מתקיים

$$\prod_{r=1}^{\infty}\left(1-\frac{x^2}{r^2}\right) = \frac{\sin(\pi x)}{\pi x}$$

הוכחה: כיוון ששני האגפים אנליטיים במישור, די להוכיח כאשר x ממשי.
ראינו כי

$$\lim_{k\to\infty}\prod_{r=1}^{k}\left(1-\frac{\sin^2(\frac{\pi x}{2k+1})}{\sin^2(\frac{\pi r}{2k+1})}\right) = \frac{\sin(\pi x)}{\pi x}$$

אם $N\in\mathbb{N}$ מתקיים

$$\prod_{r=1}^{N}\left(1-\frac{\sin^2(\frac{\pi x}{2k+1})}{\sin^2(\frac{\pi r}{2k+1})}\right) \underset{k\to\infty}{\longrightarrow} \prod_{r=1}^{N}\left(1-\frac{x^2}{r^2}\right)$$

ואז

$$\prod_{r=1}^{\infty}\left(1-\frac{x^2}{r^2}\right) = \prod_{r=1}^{N}\left(1-\frac{x^2}{r^2}\right)\cdot\lim_{k\to\infty}\prod_{r=N+1}^{k}\left(1-\frac{x^2}{r^2}\right)$$

לכן די להוכיח כי קיים

$$\lim_{k\to\infty}\prod_{r=N+1}^{k}\frac{\left(1-\frac{\sin^2(\frac{\pi x}{2k+1})}{\sin^2(\frac{\pi r}{2k+1})}\right)}{\left(1-\frac{x^2}{r^2}\right)} = 1$$

מאחר וx ממשי, מספיק להראות כי

$$\lim_{k\to\infty}\sum_{r=N+1}^{k}\left(\log\left(1-\frac{\sin^2(\frac{\pi x}{2k+1})}{\sin^2(\frac{\pi r}{2k+1})}\right)-\log\left(1-\frac{x^2}{r^2}\right)\right) = 0$$

כאשר $|x|<N$.
מתקיים $r\geq N+1$, $|x|<N$ ולכן

$$\begin{aligned}|\frac{\pi x}{2k+1}| &< \frac{\pi r}{2k+1}\\ &\leq \frac{\pi k}{2k+1}\\ &< \frac{\pi}{2}\end{aligned}$$

מכאן

$$0<\frac{\sin^2(\frac{\pi x}{2k+1})}{\sin^2(\frac{\pi r}{2k+1})}<1$$

נשתמש שוב בפיתוח טיילור

$$\log(1-z) = -\sum_{l=1}^{\infty} \frac{z^l}{l} \qquad (|z| < 1)$$

ולכן

$$\begin{aligned} S = \sum_{r=N+1}^{k} \left(\log\left(1 - \frac{\sin^2(\frac{\pi x}{2k+1})}{\sin^2(\frac{\pi r}{2k+1})}\right) - \log\left(1 - \frac{x^2}{r^2}\right)\right) &= -\sum_{r=N+1}^{k} \sum_{l=1}^{\infty} \frac{1}{l} \left(\frac{\sin^{2l}(\frac{\pi x}{2k+1})}{\sin^{2l}(\frac{\pi r}{2k+1})} - \frac{x^{2l}}{r^{2l}} \right) \\ &= -\sum_{r=N+1}^{k} \sum_{l=1}^{\infty} \frac{1}{l} \frac{x^{2l}}{r^{2l}} \left(\frac{r^{2l}}{x^{2l}} \frac{\sin^{2l}(\frac{\pi x}{2k+1})}{\sin^{2l}(\frac{\pi r}{2k+1})} - 1 \right) \end{aligned}$$

נסמן

$$b_{r,k}(x) = \frac{r^2}{x^2} \frac{\sin^2(\frac{\pi x}{2k+1})}{\sin^2(\frac{\pi r}{2k+1})}$$

אז

$$\begin{aligned} S &= -\sum_{r=N+1}^{k} \sum_{l=1}^{\infty} \frac{1}{l} \frac{x^{2l}}{r^{2l}} \left(b_{r,k}(x)^l - 1 \right) \\ &= -\sum_{r=N+1}^{k} \sum_{l=1}^{\infty} \frac{1}{l} \frac{x^{2l}}{r^{2l}} \left(b_{r,k}(x) - 1 \right) \left(1 + b_{r,k}(x) + \cdots + b_{r,k}(x)^{l-1} \right) \end{aligned}$$

נזכר בהערכה:

$$\frac{2}{\pi} \leq \frac{\sin t}{t} \leq 1 \qquad (-\frac{\pi}{2} < t < \frac{\pi}{2})$$

לכן

$$
\begin{aligned}
b_{r,k}(x) &= \frac{r^2}{x^2}\frac{\frac{\sin^2(\frac{\pi x}{2k+1})}{\left(\frac{\pi x}{2k+1}\right)^2}}{\frac{\sin^2(\frac{\pi r}{2k+1})}{\left(\frac{\pi r}{2k+1}\right)^2}}\cdot\frac{\left(\frac{\pi x}{2k+1}\right)^2}{\left(\frac{\pi r}{2k+1}\right)^2} \\
&= \frac{\frac{\sin^2(\frac{\pi x}{2k+1})}{\left(\frac{\pi x}{2k+1}\right)^2}}{\frac{\sin^2(\frac{\pi r}{2k+1})}{\left(\frac{\pi r}{2k+1}\right)^2}} \\
&\le \frac{1}{\left(\frac{2}{\pi}\right)^2} \\
&= \frac{\pi^2}{4}
\end{aligned}
$$

נקבל כי

$$
\begin{aligned}
1+b_{r,k}(x)+\cdots+b_{r,k}(x)^{l-1} &\le 1+\frac{\pi^2}{4}+\cdots+\left(\frac{\pi^2}{4}\right)^{l-1} \\
&= \frac{1-\left(\frac{\pi^2}{4}\right)^l}{1-\frac{\pi^2}{4}} \\
&< \frac{\left(\frac{\pi^2}{4}\right)^l}{\frac{\pi^2}{4}-1} \\
&< \left(\frac{\pi}{2}\right)^{2l}
\end{aligned}
$$

ולכן

$$
S \le \sum_{r=N+1}^{k}\sum_{l=1}^{\infty}\frac{1}{l}\left(\frac{\pi x}{2r}\right)^{2l}|b_{r,k}(x)-1|
$$

נקטין מעט את התחום של x ל$\left|\frac{\pi x}{2}\right| < N$, כלומר $|x| < \frac{2N}{\pi}$ (מה שיכולנו לדרוש מראש) ונקבל

$$
\sum_{r=N+1}^{k}\sum_{l=1}^{\infty}\frac{1}{l}\left(\frac{\pi x}{2r}\right)^{2l}|b_{r,k}(x)-1| = -\sum_{r=N+1}^{k}\log\left(1-\frac{\pi^2x^2}{4r^2}\right)|b_{r,k}(x)-1|
$$

נפצל לשני סכומים: $\sqrt{k}\le r\le k$ ו$N+1\le r\le\sqrt{k}$:

$$-\sum_{\sqrt{k}\le r\le k}\log\left(1-\frac{\pi^2x^2}{4r^2}\right)\underbrace{|b_{r,k}(x)-1|}_{\le\frac{\pi^2}{4}+1}\quad\underset{k\to\infty}{\longrightarrow}\quad 0$$

כי $\sum_{r=N+1}^{\infty}\log\left(1-\frac{\pi^2x^2}{4r^2}\right)$ מתכנס, ולכן מתנאי קושי, נקבל זאת.
כאשר $N+1\le r\le\sqrt{k}$ נקבל

$$\begin{aligned}\left|\frac{\pi x}{2k+1}\right| &< \frac{\pi N}{2k+1}\underset{k\to\infty}{\longrightarrow}0\\ \frac{\pi r}{2k+1} &< \frac{\pi\sqrt{k}}{2k+1}\underset{k\to\infty}{\longrightarrow}0\end{aligned}$$

יהי $\varepsilon>0$, קיים $\delta>0$ כך שאם $|t_1|,|t_2|<\delta$ אז $\left|\frac{\left(\frac{\sin t_1}{t_1}\right)^2}{\left(\frac{\sin t_2}{t_2}\right)^2}-1\right|<\varepsilon$
יהי K טבעי כך שלכל $k\ge K$ מתקיים $\frac{\pi N}{2k+1},\frac{\pi\sqrt{k}}{2k+1}<\delta$ ואז $|b_{r,k}(x)-1|<\varepsilon$. מכאן נקבל

$$\begin{aligned}-\sum_{N+1\le r\le\sqrt{k}}\log\left(1-\frac{\pi^2x^2}{4r^2}\right)|b_{r,k}(x)-1| &< -\varepsilon\sum_{N+1\le r\le\sqrt{k}}\log\left(1-\frac{\pi^2x^2}{4r^2}\right)\\ &\le -\varepsilon\sum_{r=N+1}^{\infty}\log\left(1-\frac{\pi^2x^2}{4r^2}\right)\underset{\varepsilon\to0}{\longrightarrow}0\end{aligned}$$

■

מסקנה 1.11 נציב ix במקום x ונקבל

$$\begin{aligned}\prod_{r=1}^{\infty}\left(1+\frac{x^2}{r^2}\right) &= \frac{\sin(i\pi x)}{i\pi x}\\ &= \frac{\frac{e^{i(i\pi x)}-e^{-i(i\pi x)}}{2i}}{i\pi x}\\ &= \frac{e^{\pi x}-e^{-\pi x}}{2\pi x}\\ &= \frac{\sinh(\pi x)}{\pi x}\end{aligned}$$

משפט 1.12 לכל k טבעי

$$\zeta\left(2k\right) = \left(-1\right)^{k+1}\cdot\frac{\left(2\pi\right)^{2k}}{2\left(2k\right)!}B_{2k}$$

הוכחה: ראינו

$$\prod_{r=1}^{\infty}\left(1+\frac{x^{2}}{r^{2}}\right) = \frac{\sinh\left(\pi x\right)}{\pi x}$$
$$= e^{\pi x}\cdot\frac{1-e^{-2\pi x}}{2\pi x}$$

לא ממשי עם $0<x<1$ ניקח $\log$ ממשי מהמכפלה הנ"ל

$$\sum_{r=1}^{\infty}\log\left(1+\frac{x^{2}}{r^{2}}\right) = \pi x+\log\left(1-e^{-2\pi x}\right)-\log2-\log\pi-\log x$$

נזכר שוב כי

$$\log\left(1+\frac{x^{2}}{r^{2}}\right) = \sum_{l=1}^{\infty}\left(-1\right)^{l+1}\frac{x^{2l}}{l\cdot r^{2l}}$$

ולכן

$$\sum_{r=1}^{\infty}\log\left(1+\frac{x^{2}}{r^{2}}\right) = \sum_{r=1}^{\infty}\sum_{l=1}^{\infty}\left(-1\right)^{l+1}\frac{x^{2l}}{l\cdot r^{2l}}$$
$$\sum_{r=1}^{\infty}\sum_{l=1}^{\infty}\left(-1\right)^{l+1}\frac{x^{2l}}{l\cdot r^{2l}} = \pi x+\log\left(1-e^{-2\pi x}\right)-\log2-\log\pi-\log x$$

ראינו כי הטור בצד שמאל מתכנס בהחלט ובמידה שווה בכל קטע סגור ב$(0,1)$ ולכן נוכל להחליף סדר סכימה ולקבל

$$\sum_{r=1}^{\infty}\sum_{l=1}^{\infty}\left(-1\right)^{l+1}\frac{x^{2l}}{l\cdot r^{2l}} = \sum_{l=1}^{\infty}\sum_{r=1}^{\infty}\left(-1\right)^{l+1}\frac{x^{2l}}{l\cdot r^{2l}}$$
$$= \sum_{l=1}^{\infty}\frac{\left(-1\right)^{l+1}}{l}\zeta\left(2l\right)x^{2l}$$

הטור הנ"ל מתכנס ל$|x|<1$ ולכן גזיר איבר איבר.

$$\sum_{l=1}^{\infty}\frac{\left(-1\right)^{l+1}}{l}\zeta\left(2l\right)x^{2l} = \pi x+\log\left(1-e^{-2\pi x}\right)-\log2-\log\pi-\log x$$

נגזור:

$$\sum_{l=1}^{\infty} 2\left(-1\right)^{l+1}\zeta\left(2l\right)x^{2l-1} = \pi - \frac{1}{x} + \frac{2\pi e^{-2\pi x}}{1-e^{-2\pi x}}$$

נכפיל בx:

$$2\sum_{l=1}^{\infty}\left(-1\right)^{l+1}\zeta\left(2l\right)x^{2l} = -1+\pi x+\frac{2\pi x}{e^{2\pi x}-1}$$

נציב $\frac{x}{2}$ במקום x

$$\begin{aligned}2\sum_{l=1}^{\infty}\left(-1\right)^{l+1}\zeta\left(2l\right)\left(\frac{x}{2}\right)^{2l} &= -1+\frac{\pi x}{2}+\frac{\pi x}{e^{\pi x}-1}\\ &= -1+\frac{\pi x}{2}+\sum_{k=0}^{\infty}\frac{B_k}{k!}\left(\pi x\right)^k\end{aligned}$$

נשווה את המקדם ה$2k$ של כל אגף:

$$\begin{aligned}\frac{\left(-1\right)^{k+1}\zeta\left(2k\right)}{2^{2k-1}} &= \frac{B_{2k}}{(2k)!}\pi^{2k}\\ \zeta\left(2k\right) &= \frac{\left(-1\right)^{k+1}\pi^{2k}2^{2k-1}}{(2k)!}B_{2k}\end{aligned}$$

■

הערה 1.13 מההוכחה נשים לב כי קיבלנו גם $B_0 = 1$ ו$\pi B_1 + \frac{\pi}{2} = 0$ כלומר $B_1 = -\frac{1}{2}$ ו$B_{2k+1} = 0$ לכל $k > 1$. נראה בהמשך שאפשר גם למצוא זאת ישירות.

טענה 1.14 המספרים B_{2k} הם בעלי סימנים מתחלפים, $\text{sign}B_{2k} = \left(-1\right)^k$

הוכחה: ברור, מהנוסחה שהוכחנו, כי $\zeta\left(2k\right)$ חיובי. ■

טענה 1.15 מספרי ברנולי מקיימים

1. $\lim_{k\to\infty}\frac{\left|B_{2k}\right|}{\frac{2(2k)!}{(2\pi)^{2k}}} = 1$
2. $2\left(\frac{k}{\pi e}\right)^{2k} < \left|B_{2k}\right|$

הוכחה:

1. נשים לב כי $\sum_{k=2}^{\infty}\frac{1}{n^{2k}} = \zeta(2k) - 1 > 0$. מתקיים

$$\frac{1}{4^k}\left(1+\sum_{n=3}^{\infty}\frac{1}{\left(\frac{n}{2}\right)^{2k}}\right) \leq \frac{1}{4^k}\left(1+\sum_{n=3}^{\infty}\frac{4}{n^2}\right)\underset{k\to\infty}{\longrightarrow}0$$

כי $\frac{n}{2} \geq \left(\frac{n}{2}\right)^2 \geq \left(\frac{n}{2}\right)^k$

לכן $\lim_{k\to\infty}\zeta(2k) = 1$ ולכן

$$|B_{2k}|\cdot\frac{(2\pi)^{2k}}{2(2k)!} \underset{k\to\infty}{\longrightarrow} 1$$

.2

$$|B_{2k}| = \frac{2(2k)!}{(2\pi)^{2k}}\zeta(2k) > \frac{2(2k)!}{(2\pi)^{2k}}$$

מתקיים

$$e^{2k} = 1+2k+\frac{(2k)^2}{2}+\ldots+\frac{(2k)^{2k}}{(2k)!}+\ldots$$

ולכן $\frac{(2k)^{2k}}{(2k)!} < e^{2k}$. מכאן $\frac{(2k)^{2k}}{e^{2k}} < (2k)!$ ולכן

$$\begin{aligned}|\grave{B}_{2k}| &> \frac{2}{(2\pi)^{2k}}\cdot\frac{(2k)^{2k}}{e^{2k}}\\ &= 2\left(\frac{k}{e\pi}\right)^{2k}\end{aligned}$$

■

1.2.1 דוגמאות

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty}B_k\frac{t^k}{k!} \qquad (|t| < 2\pi)$$

מתקיים

$$\begin{aligned} B_0 = \lim_{t\to 0}\frac{t}{e^t-1} &= 1 \\ B_1 = \left(\frac{t}{e^t-1}\right)'|_{t=0} &= \frac{e^t-1-t\cdot e^t}{\left(e^t-1\right)^2}|_{t=0} \\ = \lim_{t\to 0}\frac{e^t-1-t\cdot e^t}{\left(e^t-1\right)^2} &= \lim_{t\to 0}\frac{e^t-e^t-t\cdot e^t}{2\left(e^t-1\right)e^t} \\ = \lim_{t\to 0}\frac{-t}{2\left(e^t-1\right)} &= -\frac{1}{2} \end{aligned}$$

הפונקציה $f\left(t\right)=\frac{t}{e^t-1}-1+\frac{1}{2}t$ היא זוגית (מבדיקה ישירה) ולכן $B_{2k+1}=0$ לכל k טבעי.

$$\begin{aligned} t &= \left(e^t-1\right)\left(\sum_{k=0}^{\infty}B_k\frac{t^k}{k!}\right) \\ &= \left(\sum_{k=0}^{\infty}B_k\frac{t^k}{k!}\right)\left(\sum_{j=1}^{\infty}\frac{t^j}{j!}\right) \\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{\infty}B_k a_{n-k}\frac{t^k}{k!} \end{aligned}$$

כאשר

$$a_j = \begin{cases} \frac{1}{j!} & j\geq 1 \\ 0 & j=0 \end{cases}$$

לכן, לכל $n\geq 2$ מתקיים

$$\sum_{k=0}^{n-1}\frac{B_k}{k!\cdot(n-k)!} = 0$$

ולכן לכל n טבעי

$$\sum_{k=0}^{n}\frac{B_k}{k!\cdot(n+1-k)!} = 0$$

כאשר $B_0=1$ כזכור.

מסקנה 1.16 B_k רציונלי לכל k.

עבור $n=2$ נקבל

$$\begin{aligned}\frac{1}{6}+\frac{1}{2}\cdot\left(-\frac{1}{2}\right)+\frac{B_2}{2} &= 0\\ B_2 &= \frac{1}{2}-\frac{1}{3}=\frac{1}{6}\end{aligned}$$

ולכן

$$\zeta\left(2\right) = \frac{\left(2\pi\right)^2}{4}\cdot\frac{1}{6}=\frac{\pi^2}{6}$$

ערכים ידועים נוספים: $B_4=-\frac{1}{30}$ ו־$\zeta\left(4\right)=\frac{\pi^4}{90}$, $B_6=\frac{1}{42}$ ו־$\zeta\left(6\right)=\frac{\pi^6}{945}$.

נחליף ברקורסיה את k ב־$n-k$ ונקבל

$$\begin{aligned}\frac{1}{n!}\sum_{k=0}^{n}\frac{n!}{(n-k)!\cdot(k+1)!}B_{n-k} &= 0\\ \sum_{k=0}^{n}\binom{n}{k}\frac{B_{n-k}}{k+1} &= 0\end{aligned}$$

לכל $n\geq 1$.

משפט 1.17 לכל k טבעי מתקיים

$$\zeta\left(1-k\right) = \frac{\left(-1\right)^{k-1}}{k}B_k$$

הוכחה: ראינו את הרקורסיה

$$\zeta\left(1-m\right) = \frac{\left(-1\right)^m}{m\left(m-1\right)}-\sum_{r=1}^{m-1}\frac{\left(-1\right)^r}{r+1}\binom{m-1}{r}\zeta(1-m+r)$$

נוכיח באינדוקציה על m:

$$\zeta\left(0\right) = -\frac{1}{2}=\frac{\left(-1\right)^{1-1}}{1}B_1$$

(כזכור $B_1=-\frac{1}{2}$)

באינדקוציה

$$
\begin{aligned}
\zeta(1-m) &= \frac{(-1)^m}{m(m-1)} - \sum_{r=1}^{m-1} \frac{(-1)^r}{r+1} \binom{m-1}{r} \frac{(-1)^{m-r-1}}{m-r} B_{m-r} \\
&= \frac{(-1)^m}{m(m-1)} + (-1)^m \sum_{r=1}^{m-1} \frac{1}{r+1} \cdot \frac{(m-1)!}{r! \cdot (m-r-1)!} \cdot \frac{1}{m-r} \cdot B_{m-r} \\
&= \frac{(-1)^m}{m(m-1)} + \frac{(-1)^m}{m} \sum_{r=1}^{m-1} \binom{m}{r} \cdot \frac{B_{m-r}}{r+1} \\
&= \frac{(-1)^m}{m(m-1)} + \frac{(-1)^m}{m} \left(-\frac{1}{m+1} - B_m + \underbrace{\sum_{r=0}^{m} \binom{m}{r} \cdot \frac{B_{m-r}}{r+1}}_{0} \right) \\
&= \frac{(-1)^{m-1}}{m} B_m
\end{aligned}
$$

■

מסקנה 1.18

1. $\zeta(-2k) = 0$ לכל k טבעי.
2. לכל $k \geq 2$ טבעי מתקיים כי $\zeta(1-k) = -\frac{B_k}{k}$.

1.2.2 נוסחה לסכום $1^k + 2^k + 3^k + \cdots + (n-1)^k$

נסמן

$$
\begin{aligned}
s_k(n) &= 1^k + 2^k + 3^k + \cdots + (n-1)^k \\
&= \sum_{j=1}^{n-1} j^k
\end{aligned}
$$

כאשר $n \geq 2, k \geq 0$ שלמים.
נתבונן בטור

$$
\begin{aligned}
\sum_{k=0}^{\infty}\frac{s_k(n)}{k!}t^k &= \sum_{k=0}^{\infty}\frac{1}{k!}\left(\sum_{j=1}^{n-1}j^k\right)t^k \\
&= \sum_{k=0}^{\infty}\sum_{j=1}^{n-1}\frac{(jt)^k}{k!} \\
&= \sum_{j=1}^{n-1}\sum_{k=0}^{\infty}\frac{(jt)^k}{k!} \\
&= \sum_{j=1}^{n-1}e^{jt} \\
&= e^t+e^{2t}+\ldots+e^{(n-1)t} \\
&= e^t\cdot\frac{e^{(n-1)t}-1}{e^t-1} \\
&= \frac{e^{nt}-e^t}{e^t-1} \\
&= \frac{e^{nt}-e^t}{t}\cdot\frac{t}{e^t-1}
\end{aligned}
$$

נפתח את צד ימין לטור טיילור ל-$|t|<2\pi$

$$
\begin{aligned}
\frac{e^{nt}-e^t}{t}\cdot\frac{t}{e^t-1} &= \left(\sum_{k=1}^{\infty}\frac{n^k-1}{k!}\cdot t^{k-1}\right)\cdot\left(\sum_{j=0}^{\infty}\frac{B_j}{j!}t^j\right) \\
&= \left(\sum_{k=0}^{\infty}\frac{n^{k+1}-1}{(k+1)!}\cdot t^{k}\right)\cdot\left(\sum_{j=0}^{\infty}\frac{B_j}{j!}t^j\right) \\
&= \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k}\frac{n^{i+1}-1}{(i+1)!}\cdot\frac{B_{k-i}}{(k-i)!}\right)t^k
\end{aligned}
$$

על ידי השוואת המקדם ה-k נקבל

$$
\begin{aligned}
\frac{s_k(n)}{k!} &= \sum_{i=0}^{k}\frac{n^{i+1}-1}{(i+1)!}\cdot\frac{B_{k-i}}{(k-i)!} \\
&= \frac{1}{(k+1)!}\sum_{i=0}^{k}\binom{k+1}{i+1}\cdot B_{k-i}\cdot\left(n^{i+1}-1\right)
\end{aligned}
$$

ולכן

$$\begin{aligned}
s_k(n) &= \frac{1}{k+1}\sum_{i=0}^{k}\binom{k+1}{i+1}\cdot B_{k-i}\cdot\left(n^{i+1}-1\right)\\
&= \frac{1}{k+1}\sum_{i=0}^{k}\frac{(k+1)!}{(i+1)!\,(k-i)!}\cdot B_{k-i}\cdot\left(n^{i+1}-1\right)\\
&= \sum_{i=0}^{k}\binom{k}{i}\cdot B_{k-i}\cdot\frac{n^{i+1}-1}{i+1}\\
&= \sum_{i=0}^{k}\binom{k}{i}\cdot B_{k-i}\cdot\frac{n^{i+1}}{i+1}-\underbrace{\sum_{i=0}^{k}\binom{k}{i}\cdot\frac{B_{k-i}}{i+1}}_{0}\\
&= \sum_{i=0}^{k}\binom{k}{i}\cdot B_{k-i}\cdot\frac{n^{i+1}}{i+1}
\end{aligned}$$

משפט 1.19 $s_k(n)$ הוא פולינום ממעלה $k+1$ ב־n ומתקיים כי

1. $s_0(n)=n-1$
2. לכל k טבעי

$$s_k(n) = \sum_{i=0}^{k}\binom{k}{i}\cdot B_{k-i}\cdot\frac{n^{i+1}}{i+1}$$

מסקנה 1.20 (דוגמה)

$$\begin{aligned}
s_2(n) &= B_2\cdot n+2\cdot\frac{B_1}{2}\cdot n^2+\frac{B_0}{3}\cdot n^3\\
&= \frac{n}{6}-\frac{n^2}{2}+\frac{n^3}{3}\\
&= \frac{n}{6}\cdot\left(1-3n+2n^2\right)\\
&= \frac{1}{6}\cdot n\,(2n-1)\,(n-1)
\end{aligned}$$

לכן

$$1^2+2^2+\ldots+(n-1)^2 = \frac{1}{6}\cdot n\,(2n-1)\,(n-1)$$

עוד סכומים ידועים:

$$
\begin{aligned}
1^3+2^3+\ldots+(n-1)^3 &= \frac{n^2(n-1)^2}{4} \\
1^4+2^4+\ldots+(n-1)^4 &= \frac{1}{30}n(n-1)(2n-1)\left(3n^2-3n-1\right) \\
1^k+2^k+\ldots+(n-1)^k &= \sum_{i=0}^{k}\binom{k}{i}\cdot B_{k-i}\cdot\frac{n^{i+1}}{i+1}
\end{aligned}
$$

1.3 תכונות מודולו p (ראשוני) של מספרי ברנולי, קונגרואנציית Kummer

1.3.1 ההערכה ה־p־אדית על $\mathbb{Q}$

הגדרה 1.21 יהי $\frac{a}{b}\neq 0$ מספר רציונלי כאשר a,b שלמים זרים. נכתוב $\frac{a}{b}=p^u\cdot\frac{a'}{b'}$ כאשר $u\in\mathbb{Z}$ ו־a',b' שלמים זרים וזרים ל־p.
נגדיר $\nu_p\left(\frac{a}{b}\right)=u$ ו־$\nu_p(0)=\infty$.

טענה 1.22

1. $\nu_p(r\cdot t)=\nu_p(r)+\nu_p(t)$
2. $\nu_p(r+t)\geq\min\{\nu_p(r),\nu_p(t)\}$ לכל $r,t\in\mathbb{Q}$. כמו כן, אם $\nu_p(r)\neq\nu_p(t)$ אז $\nu_p(r+t)=\min\{\nu_p(r),\nu_p(t)\}$.

הוכחה:

1. קל לבדוק.
2. אם אחד מ־$r,t,r+t$ הוא אפס, אז האי־שוויון ברור.
נניח לכן $r,t,r+t\neq 0$.
נכתוב $r=p^u\frac{a}{b}$ ו־$t=p^v\frac{\alpha}{\beta}$, כאשר a,b,α,β זרים ל־p.
נניח כי $u\geq v$. אז

$$
\begin{aligned}
r+t &= p^v\left(p^{u-v}\frac{a}{b}+\frac{\alpha}{\beta}\right) \\
&= p^v\cdot\frac{p^{u-v}a\beta+\alpha b}{b\beta}
\end{aligned}
$$

כאשר $u-v\geq 0$.
אם $u>v$ המונה והמכנה זרים ל־p כיוון ש־a,b,α,β זרים ל־p, גם $p^{u-v}a\beta+\alpha b$ וגם $b\beta$ זרים ל־p ולכן

$$
\nu_p(r+t) = \min\{\nu_p(r),\nu_p(t)\}
$$

אם $u=v$

$$
r+t = p^v\cdot\frac{a\beta+\alpha b}{b\beta}
$$

כיוון ש־$b\beta$ זר ל־p ו־$a\beta+\alpha b$ שלם, מתקיים כי $\nu_p(r+t)\geq v=\min\{\nu_p(r),\nu_p(t)\}$.

■

מסקנה 1.23 לכל $r \neq 0$ מתקיים

$$\nu_p\left(\frac{1}{r}\right) = -\nu_p(r)$$

נסמן $\mathcal{O}_p = \left\{r \in \mathbb{Q} \middle| \nu_p(r) \geq 0\right\}$. זהו חוג חלקי של $\mathbb{Q}$.

$$p\mathcal{O}_p = \left\{r \in \mathbb{Q} \middle| \nu_p(r) \geq 1\right\}$$

זהו אידיאל של $\mathcal{O}_p$.

$$\mathcal{O}_p \setminus p\mathcal{O}_p = \left\{r \in \mathbb{Q} \middle| \nu_p(r) = 0\right\} = \mathcal{O}_p^*$$

כאשר $\mathcal{O}_p^*$ חבורת ההפיכים של $\mathcal{O}_p$.
לכן $p\mathcal{O}_p$ האידיאל המקסימלי היחיד של $\mathcal{O}_p$.

הגדרה 1.24 אם $r \in \mathbb{Q}$ מקיים $\nu_p(r) \geq 0$, נאמר ש-r שלם ביחס ל-p (באנגלית: p-integral).

משפט 1.25 יהי p ראשוני, אז לכל $k \geq 0$ מתקיים כי pB_k שלם ביחס ל-p, כלומר $\nu_p(pB_k) \geq 0$ ($\nu_p(B_k) \geq -1 \iff$).

הוכחה:

$$\begin{aligned}
s_k(p) &= 1^k + 2^k + \ldots + (p-1)^k \\
&= \sum_{i=0}^{k} \binom{k}{i} \cdot \frac{B_{k-i}}{i+1} \cdot p^{i+1} \\
&= pB_k + \sum_{i=1}^{k} \binom{k}{i} \cdot \frac{pB_{k-i}}{i+1} \cdot p^{i}
\end{aligned}$$

אם $k = 0$ אז $pB_0 = p$ שהוא שלם ביחס ל-p ($\nu_p(p) = 1$).
יהי $1 \leq i \leq k$. נכתוב $i + 1 = p^u \cdot l$ כאשר $p \nmid l$. אז

$$p^i \geq 2^i = (1+1)^i \geq 1 + i = p^u l \geq p^u$$

ולכן

$$\nu_p\left(\frac{p^i}{i+1}\right) = \nu_p\left(p^i\right) - \nu_p(i+1) = i - u \geq 0$$

$$\begin{aligned}\nu_p(pB_k) &= \nu_p\left(s_k(p)-\sum_{i=1}^{k}\binom{k}{i}\cdot pB_{k-i}\cdot\frac{p^i}{i+1}\right)\\ &\geq \min\left\{\underbrace{\nu_p(s_k(p))}_{\geq 0},\min_{1\leq i\leq k}\left\{\underbrace{\nu_p\left(\binom{k}{i}\right)}_{\geq 0}+\underbrace{\nu_p(pB_{k-i})}_{\geq 0}+\underbrace{\nu_p\left(\frac{p^i}{i+1}\right)}_{\geq 0}\right\}\right\}\end{aligned}$$

($\nu_p(pB_{k-i})\geq 0$ מאינדוקציה, והראנו $\nu_p\left(\frac{p^i}{i+1}\right)\geq 0$. השאר מספרים שלמים) ■

נכתוב $B_k=\frac{u_k}{v_k}$ כאשר v_k טבעי וu_k שלם, ומתקיים כי u_k וv_k זרים (כאשר $k\geq 3$ אי־זוגי $u_k=0$ ו$v_k=1$).

מסקנה 1.26 v_k חופשי מריבועים

הוכחה: ראינו $\nu_p\left(p\frac{pu_k}{v_k}\right)\geq 0$ וכיוון שu_k,v_k זרים, לא ייתכן ש $p^2|v_k$ (לכל ראשוני p). ■

הגדרה 1.27 יהי $r,t\in\mathbb{Q}$. נאמר ונכתוב $r\equiv t\ (\mod p)$ אם $\nu_p(r-t)>0$. כלומר, $r-t\in p\mathcal{O}_p$.

זהו יחס השקילות המתאים לחבורת המנה החיבורית $\mathbb{Q}/p\mathcal{O}_p$

$$r\equiv t(\mod p)\iff r+p\mathcal{O}_p=t+p\mathcal{O}_p$$

ההוכחה הקודמת מראה כי

טענה 1.28 יהי $k\geq 2$ זוגי. אז

$$pB_k\equiv s_k(p)\qquad(\mod p)$$

הוכחה:

$$s_k(p)=pB_k+p\sum_{i=1}^{k}\binom{k}{i}\cdot\frac{B_{k-i}}{i+1}\cdot p^i$$

עבור $k=2$

$$\begin{aligned}s_2(p) &= pB_2+2B_1\frac{p^2}{2}+\frac{p^3}{3}\\ &= pB_2-\frac{p^2}{2}+\frac{p^3}{3}\\ &= pB_2-\frac{p^2}{6}(3-2p)\end{aligned}$$

קל לראות כי לכל ראשוני p,

$$\nu_p\left(\frac{p^2\left(3-2p\right)}{6}\right) \geq 1$$

ולכן $pB_2\equiv s_2\left(p\right)\left(\mod p\right)$.

נניח כי $k\geq 4$. כיוון ש$k-1\geq 3$ אי־זוגי, $B_{k-1}=0$.

$$s_k\left(p\right) = pB_k+p\sum_{i=2}^{k}\binom{k}{i}\cdot\frac{pB_{k-i}}{i+1}\cdot p^{i-1}$$

נראה כי $\nu_p\left(\frac{p^{i-1}}{i+1}\right)\geq 0$. נקבל כמו קודם

$$\nu_p\left(\sum_{i=2}^{k}\binom{k}{i}\cdot\frac{pB_{k-i}}{i+1}\cdot p^{i-1}\right) \geq 0$$

ונסיים.

אם $i=2$:

$$\frac{p^{i-1}}{i+1} = \frac{p}{3}$$

ואכן $\nu_p\left(\frac{p}{3}\right)\geq 0$.

נניח כי $i\geq 3$ אז מתקיים

$$p^{i-1} \geq i+1$$

באינדוקציה על $i\geq 3$:

$$p^i = p\cdot p^{i-1}\geq p\cdot\left(i+1\right)=pi+p\geq i+p\geq i+2$$

נרשום $i+1=p^ul$

$$\begin{aligned} p^{i-1} &\geq i+1=p^ul\geq p^u\\ \Longrightarrow &\quad i-1-u\geq 0\\ &= \nu_p\left(\frac{p^{i-1}}{i+1}\right)\geq 0\end{aligned}$$

■

טענה 1.29 יהי p ראשוני.

1. אם $p-1\nmid k$ אז $s_k\left(p\right)\equiv 0\left(\mod p\right)$
2. אם $p-1\mid k$ אז $s_k\left(p\right)\equiv -1\left(\mod p\right)$

הוכחה:

1. $S_k(p) \equiv -1 \pmod p$. נבחר a שלם הזר ל-p כך $a^k \neq 1 \pmod p$ (למשל שורש פרימיטיבי מודולו p).

$$\begin{aligned} a^k s_k(p) &\equiv \sum_{j=1}^{p-1} (aj)^k \\ &\equiv \sum_{j=1}^{p-1} j^k \\ &\equiv s_k(p) \pmod p \end{aligned}$$

($\mathbb{F}_p$ שדה ולכן ההעתקה $x \mapsto ax$ חד חד ערכית ועל)
אבל $a^k - 1 \neq 0 \pmod p$ ולכן $s_k(p) \equiv 0 \pmod p$.

2. לכל j שלם הזר ל-p

$$j^{p-1} \equiv 1 \pmod p$$

(זהו משפט פרמה הקטן)
ולכן $j^k \equiv 1 \pmod p$ כאשר $p-1 \mid k$ ואז $s_k(p) \equiv \sum_{j=1}^{p-1} 1 \equiv p-1 \equiv -1 \pmod p$.

■

משפט 1.30 נכתוב $B_k = \frac{u_k}{v_k}$ כמו קודם (u_k, v_k שלמים זרים עם $v_k > 0$) ויהי p מספר ראשוני.
אז $p \mid v_k \iff p-1 \mid k$.

הוכחה: $\Leftarrow$: נניח $p-1 \nmid k$ אז

$$pB_k \equiv s_k(p) \equiv 0 \pmod p$$

כלומר $\nu_p(pB_k) \geq 1$ ולכן $\nu_p(B_k) \geq 0$. $\nu_p\left(\frac{u_k}{v_k}\right) \geq 0$ ולכן $p \nmid v_k$.
$\Longrightarrow$: נניח כי $p-1 \mid k$ אז

$$pB_k \equiv s_k(p) \equiv -1 \pmod p$$

ולכן אפשר לכתוב

$$pB_k = -1 + z$$

כאשר $z \in p\mathcal{O}_p$.

$\nu_p(-1)=0$, $\nu_p(z)\geq 1$ ולכן

$$\nu_p(-1+z) = \min\{\nu_p(-1),\nu_p(z)\}=0$$

לכן $\nu_p(pB_k)=0$, $\nu_p\left(\frac{pu_k}{v_k}\right)=0$ ולכן p צריך להצטמצם מתוך v_k, כלומר $p\mid v_k$. ■

משפט 1.31 (Von Staudt, Clausen): לכל $k\geq 2$ זוגי מתקיים

$$B_k+\sum_{\substack{p-1\mid k\\ p\text{ is prime}}}\frac{1}{p} \in \mathbb{Z}$$

הוכחה: יהי q ראשוני. נניח $q\mid v_k$. אז

$$\begin{aligned} qB_k\equiv s_k(q) &\equiv -1 \pmod q\\ &\Longleftrightarrow\\ qB_k+1 &\in q\mathcal{O}_q=\{x\in\mathbb{Q}\mid V_q(x)\geq 1\}\\ &\Longrightarrow\\ B_k+\frac{1}{q} &\in \mathcal{O}_q\end{aligned}$$

לכל ראשוני $q\neq p$ כך ש$k\mid p-1$ מתקיים כמובן $\nu_q\left(\frac{1}{p}\right)=0$ ולכן $\frac{1}{p}\in\mathcal{O}_q$ וכיוון ש$\mathcal{O}_q$ חוג, נקבל כי

$$B_k+\sum_{\substack{p-1\mid k\\ p\text{ is prime}}}\frac{1}{p} \in \mathcal{O}_q$$

נניח כעת כי $q\nmid v_k$. אז $q-1\nmid k$. נסיק כי

$$qB_k\equiv s_k(q) \equiv 0 \pmod q$$

ולכן

$$\nu_q(qB_k)\geq 1 \Longrightarrow \nu_q(B_k)\geq 0$$

לכן $B_k\in\mathcal{O}_q$.

אם p ראשוני כך ש$k\mid p-1$ אז $q\neq p$ ולכן $\nu_q\left(\frac{1}{p}\right)=0$. כלומר $\frac{1}{p}\in\mathcal{O}_q$ ולכן

$$B_k+\sum_{\substack{p-1\mid k\\ p\text{ is prime}}}\frac{1}{p} \in \mathcal{O}_q$$

לכן הראינו כי לכל מספר ראשוני q מתקיים $\frac{1}{p} \in \mathcal{O}_q \sum_{\substack{p-1|k \\ p \text{ is prime}}} + B_k$, ולכן זהו מספר שלם. ■

הערה 1.32 לכל $k \geq 2$ זוגי מתקיים $6 \mid v_k$.

הוכחה: $2 \mid v_k$ כי $2-1 \mid k$ ו־$3 \mid v_k$ כי $3-1 \mid k$, שהרי k זוגי. ■

משפט 1.33 יהיו $n \geq 2$ טבעי, $k \geq 2$ זוגי. אז

$$v_k \cdot s_k(n) \equiv u_k \cdot n \pmod{n^2}$$

הוכחה: נזכר כי

$$s_k(n) = B_k \cdot n + \sum_{i=1}^{k} \binom{k}{i} \cdot B_{k-i} \cdot \frac{n^{i+1}}{i+1}$$

נניח $k = 2$:

$$\begin{aligned} s_2(n) &= B_2 \cdot n + \frac{2B_1 n^2}{2} + \frac{B_0 n^3}{3} \\ &= B_2 \cdot n - \frac{n^2}{2} + \frac{n^3}{3} \end{aligned}$$

ואז

$$v_2 s_2(n) = u_2 n - \frac{v_2}{2} n^2 + \frac{v_2}{3} n^3 \equiv u_2 n \pmod{n^2}$$

כי מההערה האחרונה $2, 3 \mid v_2$.
נוכל להניח כעת כי $k \geq 4$. כיוון ש־k זוגי, $B_{k-1} = 0$.

$$v_k s_k(n) = u_k \cdot n + v_k \cdot \left(\sum_{i=2}^{k} \binom{k}{i} \cdot B_{k-i} \cdot \frac{n^{i-1}}{i+1} \right) \cdot n^2$$

נשים לב כי $v_k \cdot \left(\sum_{i=2}^{k} \binom{k}{i} \cdot B_{k-i} \cdot \frac{n^{i-1}}{i+1} \right) \cdot n^2$ שלם כהפרש של שני מספרים שלמים.
נסמן

$$v_k \cdot \sum_{i=2}^{k} \binom{k}{i} \cdot B_{k-i} \cdot \frac{n^{i-1}}{i+1} = \frac{A}{B}$$

מנה מצומצמת של שלמים, B טבעי.
לכן $B \mid n^2$.
נרצה להראות כי $B = 1$. לשם כך, נראה כי לכל p ראשוני המחלק את n מתקיים $\nu_p\left(\frac{A}{B}\right) \geq 0$.
בפרט, לכל p ראשוני המחלק את B מתקיים $\nu_p\left(\frac{A}{B}\right) \geq 0$ וזה מחייב ש$B = 1$.
נניח כי $p \mid n$, p ראשוני, $p \geq 3$.

$$\frac{A}{B} = \frac{v_k}{3} \cdot \binom{k}{2} \cdot B_{k-2} \cdot n + v_k \cdot \sum_{i=4}^{k} \binom{k}{i} \cdot B_{k-i} \cdot n \cdot \frac{n^{i-2}}{i+1}$$

ל$k \geq 4$
(ל$k = 4$ יש אמנם גם את המחובר $i = 3$ והוא מקיים

$$\begin{aligned} \frac{v_4}{4} \cdot \binom{4}{3} \cdot B_1 \cdot n^2 &= \frac{v_4}{4} \cdot 4 \cdot -\frac{1}{2} \cdot n^2 \\ &= -\frac{v_4}{2} \cdot n^2 \end{aligned}$$

ו$\frac{v_4}{2}$ מספר שלם כי כזכור מהמסקנה האחרונה $2 \mid v_4$. לכן ניתן להזניח את האיבר הזה מודולו n^2)
כיוון ש $\nu_p\left(p \cdot B_{k-2}\right) \geq 0$ וכן $\frac{v_k}{3}$ שלם, המחובר הראשון שלם ביחס לp. (גם כאשר $p = 2$)
נתבונן במחובר השני

$$\nu_p\left(B_{k-i} \cdot n\right) \geq 0$$

נראה כי $\nu_p\left(\frac{n^{i-2}}{i+1}\right) \geq 0$.
נכתוב

$$\begin{aligned} n &= p^l n' \\ i+1 &= p^u j \end{aligned}$$

כאשר $p \nmid n', j$, $l \geq 1$, $u \geq 0$.

$$n^{i-2} = p^{l(i-2)} \left(n'\right)^{i-2}$$

$$\begin{aligned} p^{l(i-2)} \geq p^{i-2} \geq 3^{i-2} = (1+2)^{i-2} &\geq 1 + 2(i-2) \\ &= 2i - 3 \\ &\geq i + 1 \\ &= p^u j \\ &\geq p^u \end{aligned}$$

לכן $\nu_p\left(\frac{n^{i-2}}{i+1}\right)=l\left(i-2\right)-u\geq 0$.
כעת נניח $n \mid 2=p$. עכשיו, מכיוון ש־$i-k$ זוגי, גם i זוגי ולכן $i+1$ אי־זוגי ולכן $\nu_2\left(i+1\right)=0$. ■

משפט 1.34 (Voronoi): יהי $n\geq 2$ טבעי. אז לכל k טבעי ו־a הזר ל־n מתקיים

$$\left(a^k-1\right)s_k\left(n\right) \equiv kna^{k-1}\sum_{j=1}^{n-1}\left[\frac{ja}{n}\right]j^{k-1}\left(\mod n^2\right)$$

הוכחה: לכל $1\leq j\leq n-1$ נחלק את ja ב־n עם שארית:

$$ja = q_jn+r_j$$

כאשר $0\leq r_j\leq n-1$
אז

$$\begin{aligned}(ja)^k=\left(r_j+q_jn\right)^k &\equiv r_j^k+k\cdot q_j\cdot n\cdot r_j^{k-1}\left(\mod n^2\right)\\ &\equiv r_j^k+k\cdot q_j\cdot n\cdot\left(ja-q_j\cdot n\right)^{k-1}\left(\mod n^2\right)\\ &\equiv r_j^k+k\cdot q_j\cdot n\cdot\left(ja\right)^{k-1}\left(\mod n^2\right)\end{aligned}$$

כיוון ש־a הפיך מודולו n,

$$\begin{aligned}a\cdot\{1,2,3,\ldots,n-1\} &\equiv \{1,2,3,\ldots,n-1\}\left(\mod n\right)\\ aj &\equiv r_j\left(\mod n\right)\end{aligned}$$

לכן $\{1,2,\cdots,n-1\}=\{r_1,r_2,\ldots,r_{n-1}\}$.
נסכם את הקונגרואנציות ל־$j=1,2,\ldots,n-1$:

$$\begin{aligned}(ja)^k &= r_j^k+k\cdot q_j\cdot n\cdot(ja)^{k-1}\left(\mod n^2\right)\\ \sum_{j=1}^{n-1}(ja)^k &\equiv \sum_{j=1}^{n-1}r_j^k+k\cdot n\sum_{j=1}^{n-1}q_j\cdot(ja)^{k-1}\left(\mod n^2\right)\\ &\equiv \sum_{j=1}^{n-1}r_j^k+k\cdot n\sum_{j=1}^{n-1}\left[\frac{ja}{n}\right]\cdot(ja)^{k-1}\left(\mod n^2\right)\end{aligned}$$

לכן

$$\begin{aligned}a^k\cdot\sum_{j=1}^{n-1}j^k &\equiv \sum_{j=1}^{n-1}j^k+k\cdot n\cdot a^{k-1}\sum_{j=1}^{n-1}\left[\frac{ja}{n}\right]\cdot j^{k-1}\left(\mod n^2\right)\\ \left(a^k-1\right)\sum_{j=1}^{n-1}j^k &\equiv k\cdot n\cdot a^{k-1}\sum_{j=1}^{n-1}\left[\frac{ja}{n}\right]\cdot j^{k-1}\left(\mod n^2\right)\end{aligned}$$

■

משפט 1.35 יהי $n \geq 2$ טבעי, $k \geq 2$ זוגי, a זר ל־n אז

$$\left(a^k - 1\right) u_k \equiv k v_k a^{k-1} \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] \cdot j^{k-1} \left(\mod n\right)$$

הוכחה: נכפיל ב־v_k את שני האגפים ממשפט Voronoi:

$$\left(a^k - 1\right) v_k \sum_{j=1}^{n-1} j^k \equiv k \cdot n \cdot v_k \cdot a^{k-1} \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] \cdot j^{k-1} \left(\mod n^2\right)$$

מהמשפט הקודם

$$v_k \cdot s_k(n) \equiv u_k \cdot n \left(\mod n^2\right)$$

ואז

$$\left(a^k - 1\right) \cdot u_k \cdot n \equiv k \cdot n \cdot v_k \cdot a^{k-1} \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] \cdot j^{k-1} \left(\mod n^2\right)$$

נחלק ב־n ונקבל את הקונגרואנציה המבוקשת. ■

משפט 1.36 (קונגרואנציית Adams): יהי k טבעי ויהי p ראשוני כך ש־$p - 1 \nmid k$. אז $\frac{B_k}{k}$ שלם ביחס ל־p, כלומר $\nu_p\left(\frac{B_k}{k}\right) \geq 0$.

הוכחה: אם $k \geq 3$ אי־זוגי, אין מה להוכיח, כי $B_k = 0$ ואז $\nu_p\left(\frac{B_k}{k}\right) = \infty$.
אם $k = 1$ אז $\frac{B_1}{1} = -\frac{1}{2}$. כיוון ש $p - 1 \nmid k$, $p \neq 2$ ולכן $p \geq 3$. לכן $\nu_p\left(-\frac{1}{2}\right) = 0$.
נניח כי $k \geq 2$ זוגי. כיוון ש־$p - 1 \nmid k$, מתקיים כי $p \nmid v_k$. אם גם $p \nmid k$ אז

$$\nu_p\left(\frac{B_k}{k}\right) = \nu_p\left(\frac{u_k}{v_k}\right) = \nu_p\left(u_k\right) \geq 0$$

נניח כי $p \mid k$: $k = p^t \cdot k'$ כאשר $p \nmid k'$, $t \geq 1$.
נציב במשפט האחרון $n = p^t$ ויהי a זר ל־p.

$$\begin{aligned}\left(a^k - 1\right) u_k &\equiv p^t \cdot k' \cdot v_k a^{k-1} \sum_{j=1}^{p^t-1} \left[\frac{ja}{p^t}\right] \cdot j^{k-1} \left(\mod p^t\right) \\ &\equiv 0 \left(\mod p^t\right)\end{aligned}$$

לכן $p^t \mid \left(a^k-1\right)u_k$. נבחר a להיות שורש פרימיטיבי מודולו p. (יוצר של החבורה הציקלית $(\mathbb{Z}/p\mathbb{Z})^*$.)

כיוון ש$k \nmid p-1$ נסיק כי $a^k \not\equiv 1 \pmod p$.

לכן p זר לa^k-1.

כאן $p^t \mid u_k$. כיוון שu_k, v_k זרים, נקבל כי

$$\nu_p\left(\frac{B_k}{k}\right)=\nu_p\left(u_k\right)-\nu_p\left(k\right) \quad = \quad \nu_p\left(u_k\right)-t \geq 0$$

■

משפט 1.37 (קונגרואנציית Kummer): נתונים e טבעי, $k \geq 2$ זוגי וp ראשוני, כך ש$k \nmid p-1$.

יהי k' טבעי כך ש $k \equiv k' \left(\mod \underbrace{\phi\left(p^e\right)}_{=p^{e-1}(p-1)}\right)$. אז

$$\left(1-p^{k-1}\right)\cdot\frac{B_k}{k} \quad \equiv \quad \left(1-p^{k'-1}\right)\cdot\frac{B_{k'}}{k'} \pmod{p^e}$$

הערה 1.38 נאמר ש$x \equiv y \pmod{p^e} \iff \nu_p\left(x-y\right) \geq e$.

הוכחה: ראשית, כיוון ש$k \nmid p-1$, מתקיים כי $p \geq 3$ ואז $\phi\left(p^e\right)$ זוגי ולכן $k' \geq 2$ זוגי.

כיוון ש$p-1 \mid \phi\left(p^e\right)$ נסיק כי $k' \nmid p-1$.

נניח כי $t=\nu_p\left(k\right) \geq \nu_p\left(k'\right)=t'$

נציב במשפט הקודם $n=p^{e+t}$ ויהי a זר לp.

$$\left(a^k-1\right)u_k \quad \equiv \quad kv_ka^{k-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k-1} \pmod{p^{e+t}}$$
$$\left(a^{k'}-1\right)u_{k'} \quad \equiv \quad k'v_{k'}a^{k'-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k'-1} \pmod{p^{e+t}}$$

כיוון ש$k,k' \nmid p-1$, מתקיים כי $p \nmid v_k, v_{k'}$ ולכן v_k, v_k' הפיכים מודולו p^{e+t}.

$$\left(a^k-1\right)B_k \quad \equiv \quad ka^{k-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k-1} \pmod{p^{e+t}}$$
$$\left(a^{k'}-1\right)B_{k'} \quad \equiv \quad k'a^{k'-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k'-1} \pmod{p^{e+t}}$$

נכתוב $k=p^tu$ כאשר $p \nmid u$.

u הפיך מודולו p. נחלק בk:

$$\left(a^k-1\right)\frac{B_k}{k} \equiv a^{k-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k-1} \pmod{p^e}$$

באופן דומה:

$$\left(a^{k'}-1\right)\frac{B_{k'}}{k'} \equiv a^{k'-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k'-1} \left(\mod p^{e+t-t'}\right)$$

ולכן

$$\left(a^{k'}-1\right)\frac{B_{k'}}{k'} \equiv a^{k'-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k'-1} \pmod{p^e}$$

נתחיל ב$e=1$ אז

$$\begin{aligned} k &\equiv k' \pmod{(p-1)} \\ &\Longrightarrow \\ k-1 &\equiv k'-1 \pmod{(p-1)} \end{aligned}$$

אז מפרמה הקטן

$$j^{k-1} \equiv j^{k'-1} \pmod{p}$$

ולכן

$$a^{k-1} \equiv a^{k'-1} \pmod{p}$$

נקבל לכן

$$\begin{aligned} \left(a^{k'}-1\right)\frac{B_{k'}}{k'} &\equiv a^{k-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k-1} \pmod{p} \\ &\equiv \left(a^k-1\right)\frac{B_k}{k} \pmod{p} \end{aligned}$$

בנוסף

$$\left(a^{k'}-1\right)\frac{B_{k'}}{k'} \equiv \left(a^k-1\right)\frac{B_{k'}}{k'} \pmod{p}$$

ולכן

$$\left(a^{k}-1\right)\frac{B_{k}}{k}\quad\equiv\quad\left(a^{k}-1\right)\frac{B_{k'}}{k'}\left(\mod p\right)$$

נבחר a שורש פרימיטיבי מודולו p ונקבל כיוון ש$k \nmid p-1$, $p \nmid a^{k}-1$ ולכן נקבל $\frac{B_{k}}{k}\equiv\frac{B_{k'}}{k'}\left(\mod p\right)$.

נניח כעת כי $e>1$

$$\left(a^{k}-1\right)\frac{B_{k}}{k}\quad\equiv\quad a^{k-1}\sum_{\substack{j=1\\ p\nmid j}}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k-1}+a^{k-1}p^{k-1}\sum_{j=1}^{p^{e+t-1}-1}\left[\frac{ja}{p^{e+t-1}}\right]\cdot j^{k-1}\left(\mod p^{e}\right)$$

נזכר כי $\left(a^{k}-1\right)\frac{B_{k}}{k}\equiv a^{k-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k-1}\left(\mod p^{e}\right)$ אם נבחר $e-1$ במקום e נקבל

$$\left(a^{k}-1\right)\frac{B_{k}}{k}\quad\equiv\quad a^{k-1}\sum_{j=1}^{p^{e+t-1}-1}\left[\frac{ja}{p^{e+t-1}}\right]\cdot j^{k-1}\left(\mod p^{e-1}\right)$$

לכן

$$a^{k-1}p^{k-1}\sum_{j=1}^{p^{e+t-1}-1}\left[\frac{ja}{p^{e+t-1}}\right]\cdot j^{k-1}\quad\equiv\quad p^{k-1}\left(a^{k}-1\right)\frac{B_{k}}{k}\left(\mod p^{e-1+k-1}\right)$$

כלומר

$$\left(a^{k}-1\right)\frac{B_{k}}{k}\quad\equiv\quad a^{k-1}\sum_{\substack{j=1\\ p\nmid j}}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k-1}+p^{k-1}\left(a^{k}-1\right)\frac{B_{k}}{k}\left(\mod p^{e-1}\right)$$

(כי $e+k-2\geq e$)

ולכן

$$\left(a^{k}-1\right)\left(\frac{B_{k}}{k}\right)\left(1-p^{k-1}\right)\quad\equiv\quad a^{k-1}\sum_{\substack{j=1\\ p\nmid j}}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k-1}\left(\mod p^{e-1}\right)$$

וכנ"ל לk' במקום k:

$$\left(a^{k'}-1\right)\left(\frac{B_{k'}}{k'}\right)\left(1-p^{k'-1}\right)\quad\equiv\quad a^{k'-1}\sum_{\substack{j=1\\ p\nmid j}}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]\cdot j^{k'-1}\left(\mod p^{e-1}\right)$$

כיוון ש $k \equiv k' \left(\mod \phi\left(p^{e}\right)\right)$ נסיק מאחר ו j זר לp כי

$$\begin{aligned} j^{k-1} &\equiv j^{k'-1} \left(\mod p^{e}\right) \\ a^{k-1} &\equiv a^{k'-1} \left(\mod p^{e}\right) \end{aligned}$$

ולכן

$$\begin{aligned} \left(a^{k}-1\right)\left(1-p^{k-1}\right)\frac{B_{k}}{k} &\equiv \left(a^{k'}-1\right)\left(1-p^{k'-1}\right)\frac{B_{k'}}{k'} \left(\mod p^{e}\right) \\ &\equiv \left(a^{k}-1\right)\left(1-p^{k'-1}\right)\frac{B_{k'}}{k'} \left(\mod p^{e}\right) \end{aligned}$$

נבחר שוב a שורש פרימיטבי מודולו p. כמו קודם, $a^{k}-1$ זר לp ונקבל

$$\left(1-p^{k-1}\right)\frac{B_{k}}{k} \equiv \left(1-p^{k'-1}\right)\frac{B_{k'}}{k'} \left(\mod p^{e}\right)$$

כנדרש. ■

הגדרה 1.39 (Kummer): יהי $p \geq 3$ ראשוני. נאמר כי p רגולרי, אם $p \nmid u_{k}$ ל$k \leq p-3$.
(אחרת נאמר כי p אינו רגולרי)

דוגמאות למספרים ראשוניים רגולריים: $3,5,7,11,13,17,19,23,29,31,41$.
דוגמאות למספרים ראשוניים לא רגולריים: $37,59,67,101,103,131,149,157,\ldots$.

משפט 1.40 יש אינסוף מספרים ראשוניים לא רגולריים.

הוכחה: נניח בשלילה כי יש מספר סופי של ראשוניים לא רגולריים. נסמנם $p_{1},p_{2},\ldots,p_{r}$.
יהי k טבעי. נגדיר $n=k\left(p_{1}-1\right)\cdot\left(p_{2}-1\right)\cdot\ldots\cdot\left(p_{r}-1\right)$.
n זוגי ושואף לאינסוף כאשר k שואף לאינסוף.
ראינו $\left|B_{n}\right| > 2\cdot\left(\frac{n}{2\pi e}\right)^{n}$ ולכן $\left|\frac{B_{n}}{n}\right| \underset{n\to\infty}{\longrightarrow} \infty$.
נבחר k גדול מספיק כך ש$1 < \left|\frac{B_{n}}{n}\right|$. נבחר p ראשוני כך ש$1 \leq \nu_{p}\left(\frac{B_{n}}{n}\right)$.
בפרט $p \mid u_{n}$ ולכן $p \nmid v_{n}$. מכאן $p-1 \nmid n$ ובניית n, $p \neq p_{i}$ לכל $1 \leq i \leq r$.
כמו כן $p \neq 2$ ולכן $p \geq 3$.
נראה כי p אינו רגולרי.
יהי $0 \leq m < p-1$ השלם היחיד כך ש$n \equiv m \left(\mod (p-1)\right)$.
כיוון ש$p-1 \nmid n$ גם $p-1 \nmid m$ ולכן $1 \leq m < p-1$.
כיוון שn ו$p-1$ זוגיים, גם m זוגי. ממשפט Kummer

$$\frac{B_{n}}{n} \equiv \frac{B_{m}}{m} \left(\mod p\right)$$

כמו כן, כיוון שm זוגי, $m \leq p-3$ ולכן p לא רגולרי. ■

2 שדה המספרים ה־p־אדיים

2.1 ערך מוחלט על שדה

הגדרה 2.1 יהי F שדה. פונקציה

$$||: F \to \mathbb{R}_+$$

תקרא ערך מוחלט על F אם

1. $x = 0 \iff |x| = 0$
2. $|x| \cdot |y| = |x \cdot y|$ לכל $x, y \in F$
3. $|x + y| \le |x| + |y|$ לכל $x, y \in F$

הערה 2.2 נניח כי F שדה עם ערך מוחלט $||$. אז לכל $x \neq 0$:

$$|x| = |x \cdot 1| = |x| \cdot |1|$$

מאחר ו־$x \neq 0$ אז $|x| \neq 0$ ולכן $|1| = 1$.
בנוסף

$$1 = |1| = \left|(-1)^2\right| = |-1|^2$$

ומאחר ו־$|-1| > 0$ נקבל כי $|-1| = 1$.
לכן לכל $x \in F$ נקבל $|-x| = |-1| \cdot |x| = |x|$.

הגדרה 2.3 המטריקה המתאימה על F היא $d(x, y) = |x - y|$

הערה 2.4 זוהי אכן מטריקה:

1. $d(x, y) \ge 0$ ו־$d(x, y) = 0 \iff x = y$
2. $d(x, y) = d(y, x)$ כי $|x - y| = |-(x - y)| = |y - x|$.
3. לכל $x, y, z \in F$ מתקיים

$$d(x, y) \le d(x, z) + d(z, y)$$

אכן

$$|x - y| = |x - z + z - y| \le |x - z| + |z - y|$$

F הופך למרחב מטרי עם המטריקה הנ"ל. עיגול פתוח ברדיוס $r > 0$ סביב $a \in F$ הוא הקבוצה:

$$\{x \in F \mid |x - a| < r\}$$

2.1.1 דוגמאות

1. הערך המוחלט הטריוואלי:

$$|x| = \begin{cases} 0 & x=0 \\ 1 & x\neq 0 \end{cases}$$

2. על $\mathbb{C}$, $|z| = \sqrt{z\cdot\bar{z}}$. זה משרה ערך מוחלט על כל שדה חלקי של $\mathbb{C}$.
3. הערכים המוחלט על $\mathbb{Q}$: יהי p מספר ראשוני. נגדיר ל$x\in\mathbb{Q}$

$$|x|_p = \begin{cases} 0 & x=0 \\ p^{-\nu_p(x)} & x\neq 0 \end{cases}$$

לדוגמה $|50|_3 = 1$, $|50|_5 = \frac{1}{25}$

טענה 2.5 $||_p$ הינו ערך מוחלט על $\mathbb{Q}$

הוכחה:

1. ברור כי $|x|_p \geq 0$ ו$|x|_p = 0 \iff x=0$.
2. יהיו $x,y\in\mathbb{Q}$. אז אם $xy=0$ נקבל כי $x=0$ או $y=0$ ואז

$$0 = |xy|_p = |x|_p\cdot|y|_p$$

ואם $x,y\neq 0$ אז

$$|xy|_p = p^{-\nu_p(xy)} = p^{-\nu_p(x)-\nu_p(y)} = p^{-\nu_p(x)}\cdot p^{-\nu_p(y)} = |x|_p\cdot|y|_p$$

3. יהיו $x,y\in\mathbb{Q}$ נוכיח כי $|x+y|_p \leq \max\left\{|x|_p, |y|_p\right\}$ ואם $|x|_p \neq |y|_p$ אז $|x+y|_p = \max\left\{|x|_p, |y|_p\right\}$.
אם $x+y=0$ אז אי השוויון ברור.
נניח $x+y\neq 0$. אם $x=0$ או $y=0$, נקבל שוויון.
לכן נניח $0\neq x,y,x+y$.

$$|x+y|_p = p^{-\nu_p(x+y)} \leq \max\left\{p^{-\nu_p(x)}, p^{-\nu_p(y)}\right\} = \max\left\{|x|_p, |y|_p\right\}$$

כי הוכחנו $\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$.
נניח כי $|x|_p \neq |y|_p$ אז $x+y\neq 0$ (כי אחרת $x=-y$ ואז $|x|_p = |y|_p$)
אם $x=0$ או $y=0$ נקבל שוויון.
נניח כי $x,y\neq 0$ אז

$$|x+y| = p^{-\nu_p(x+y)} = \max\left\{p^{-\nu_p(x)}, p^{-\nu_p(y)}\right\} = \max\left\{|x|_p, |y|_p\right\}$$

זאת מאחר והוכחנו כי $\nu_p(x+y) = \min\{\nu_p(x), \nu_p(y)\}$ אם $\nu_p(x)\neq\nu_p(y)$.

■

הגדרה 2.6 ערך מוחלט על F שמקיים $|x+y| \leq \max\{|x|,|y|\}$ נקרא ערך מוחלט לא ארכימדי.

נשים לב כי $\mathcal{O}_p = \left\{x\in\mathbb{Q} \mid |x|_p \leq 1\right\}$ הוא "עיגול היחידה הסגור". (נראה שהוא גם פתוח)

בנוסף $p\mathcal{O}_p = \left\{x\in\mathbb{Q} \mid |x|_p < 1\right\}$ "עיגול היחידה הפתוח". (נראה שהוא גם סגור)

בנוסף $\mathcal{O}_p^* = \left\{x\in\mathbb{Q} \mid |x|_p = 1\right\}$ "מעגל היחידה (נראה שהוא גם פתוח וגם סגור)

לפי המטריקה מקיים כי $x \sim y$ אם ההפרש שלהם מתחלק בחזקה גבוהה של p.

למשל $p^n \underset{n\to\infty}{\longrightarrow} 0$ לפי $||_p$.

טענה 2.7 יהי F שדה בעל מוחלט לא ארכימדי. אז לכל $n\in\mathbb{Z}$ מתקיים $|n\cdot 1| \leq 1$.

הוכחה: יהי $n\in\mathbb{Z}$. מאחר ו $|n\cdot 1| = |(-n)\cdot 1|$ ניתן להניח כי n טבעי. מתקיים

$$|n\cdot 1| = \Bigg|\underbrace{1+1+\ldots+1}_{n}\Bigg| \leq \max\{|1|,|1|,\ldots,|1|\} = 1$$

■

הגדרה 2.8 שני ערכים מוחלטים על שדה F נקראים שקולים, אם המטריקות המתאימות משרות אותה טופולוגיה על F.

הערה 2.9 (דוגמה): יהי p מספר ראשוני יהי $r>0$. ל$x\in\mathbb{Q}$ נוכל להגדיר

$$|x|_p^{'} = \left(|x|_p\right)^r$$

אז $||_p^{'}$ שקול ל$|\cdot|_p$. אכן: נניח כי $x \neq 0$. מתקיים

$$x = p^{\nu_p(x)}\cdot y$$

כאשר $\nu_p(y) = 0$

$$\begin{aligned}|x|_p &= p^{-\nu_p(x)}\\ |x|_p^{'} &= p^{-r\nu_p(x)}\end{aligned}$$

מתקיים

$$\begin{aligned} |x|_p^{'}\cdot|y|_p^{'} &= |xy|_p^{'}\\ |x+y|_p^{'} &= |x+y|_p^r\\ &\le \max\left\{|x|_p,|y|_p\right\}^r\\ &= \max\left\{|x|_p^r,|y|_p^r\right\}\\ &= \max\left\{|x|_p^{'},|y|_p^{'}\right\}\end{aligned}$$

הערכים המוחלטים הנ"ל שקולים:

$$|x-a|_p^{'}<\delta \quad\Longleftrightarrow\quad |x-a|_p<\delta^{\frac{1}{r}}$$

ולכן הם מגדירים את אותם הכדורים הפתוחים.

הערה 2.10 בהגדרה $|x|_p=\frac{1}{p^{\nu_p(x)}}$ מתקיים כי $\frac{1}{p}$ נבחר כבסיס באופן שרירותי. אם היינו בוחרים כל $0<\rho<1$ אחר, היינו מקבלים הגדרה של ערכים מוחלט. במקרה כזה $\rho=p^{-r}$ ל$r>0$ ונקבל ערך מוחלט כמו $|\cdot|_p^{'}$.

הגדרה 2.11 נסמן ב$|\cdot|_\infty$ את הערך המוחלט של $\mathbb{Q}$ המושרה מ$\mathbb{C}$.

משפט 2.12 (אוסטרובסקי): כל ערך מוחלט (לא טריוואלי) על $\mathbb{Q}$ שקול ל$|\cdot|_\infty$ או ל$|\cdot|_p$ לp ראשוני כלשהו.

הוכחה:

1. נניח ראשית כי לכל $x\in\mathbb{Z}$ מתקיים $|x|\le 1$. מכאן יש n טבעי כך ש$|n|<1$ (כי אחרת נקבל כי $|\cdot|$ טריוואלי)
   יהי n_0 הטבעי הראשון עם $|n_0|<1$. נשים לב כי n_0 הוא ראשוני: אם $n_0=u\cdot v$ כאשר $u,v<n_0$ אז $|u|=|v|=1$ ממינימליות n_0, ואז גם $|n_0|=|u|\cdot|v|=1$. סתירה. נסמן $n_0=p$.
   יהי $q\neq p$ ראשוני. נראה כי $|q|=1$. אחרת, $|q|<1$ ואז $|q|^n\underset{n\to\infty}{\longrightarrow}0$. יהי N טבעי כך ש $|p|^N,|q|^N<\frac{1}{2}$.
   יהיו $u,v\in\mathbb{Z}$ כך ש$u\cdot p^N+v\cdot q^N=1$. אז

$$\begin{aligned} 1 &= |1|\\ &= \left|u\cdot p^N+v\cdot q^N\right|\\ & \quad |u|\cdot|p|^N+|v|\cdot|q|^N\\ &< \frac{1}{2}+\frac{1}{2}\end{aligned}$$

סתירה.
יהי $0 \neq x \in \mathbb{Q}$. נכתוב $x = p^{\nu_p(x)} \cdot y$ כך ש $\nu_p(y) = 0$. אז

$$\begin{aligned} |x| &= |p|^{\nu_p(x)} \cdot |y| \\ &= |p|^{\nu_p(x)} \\ &= \left(p^{-r}\right)^{\nu_p(x)} \\ &= |x|_p^r \end{aligned}$$

2. נניח עתה כי יש n טבעי כך ש$1 < |n|$. יהי n_0 טבעי הראשון עם התכונה הזאת. כמובן, $n_0 \geq 2$. יהי $\alpha > 0$ כך ש

$$|n_0| = n_0^{\alpha}$$

יהי n טבעי. נכתוב את הפיתוח של n לפי הבסיס n_0:

$$n = a_0 + a_1 \cdot n_0 + \ldots + a_r \cdot n_0^r$$

כאשר $0 \leq a_i < n_0$ שלמים ו$1 \leq a_r < n_0$.
ממינימליות n_0, $|a_i| < 1$

$$\begin{aligned} |n| &\leq \sum_{i=0}^{r} |a_i| \cdot |n_0|^i \\ &\leq \sum_{i=0}^{r} |n_0|^i \\ &= 1 + |n_0| + \ldots + |n_0|^r \\ &= 1 + n_0^{\alpha} + \ldots + n_0^{\alpha r} \\ &\leq n_0^{\alpha r}\left(1 + \frac{1}{n^{\alpha}} + \frac{1}{n^{2\alpha}} + \ldots + \frac{1}{n^{\alpha r}} + \ldots\right) \\ &= n_0^{\alpha r} \cdot \frac{1}{1 - \frac{1}{n_0^{\alpha}}} \end{aligned}$$

נסמן $C = \frac{1}{1 - \frac{1}{n_0^{\alpha}}}$. קיבלנו כי לכל n טבעי מתקיים

$$\begin{aligned} |n| &\leq C \cdot n_0^{\alpha r} \\ &\leq C \cdot n^{\alpha} \end{aligned}$$

(כי $n_0^r \leq n$)
לכן לכל N טבעי

$$\begin{aligned} \left|n^N\right| &\leq C \cdot n^{\alpha \cdot N} \\ |n|^N &\leq C \cdot n^{\alpha \cdot N} \\ |n| &\leq \sqrt[N]{C} \cdot n^{\alpha} \end{aligned}$$

מהמעבר לגבול כאשר $N\to\infty$ נקבל כי $|n|\le n^{\alpha}$. לכן לכל n טבעי מתקיים

$$|n| \le n^{\alpha}$$

נכתוב $n=n_0^{r+1}-\left(n_0^{r+1}-n\right)$ כאשר $n_0^r\le n\le n_0^{r+1}$.
מאי־שוויון המשולש מתקיים

$$|x-y| \ge ||x|-|y||$$

ולכן

$$|n| \ge \underbrace{|n_0|^{r+1}}_{\left(n_0^{\alpha}\right)^{r+1}}-\left|n_0^{r+1}-n\right|$$

מתקיים

$$\left|n_0^{r+1}-n\right| \le \left(n_0^{r+1}-n\right)^{\alpha}$$

ולכן

$$\begin{aligned}|n| &\ge n_0^{\alpha\cdot(r+1)}-\left(n_0^{r+1}-n\right)^{\alpha}\\ &\ge n_0^{\alpha\cdot(r+1)}-\left(n_0^{r+1}-n_0^{r}\right)^{\alpha}\\ &= n_0^{\alpha\cdot(r+1)}-n_0^{\alpha\cdot(r+1)}\left(1-\frac{1}{n_0}\right)^{\alpha}\\ &= C_1\cdot n_0^{\alpha(r+1)}\\ &> C_1n^{\alpha}\end{aligned}$$

כאשר $C_1=\left(1-\left(1-\frac{1}{n_0}\right)^{\alpha}\right)$. כמובן קודם נסיק כי $|n|\ge n^{\alpha}$ ולכן $|n|=n^{\alpha}$.
נסיק מכפליות הערך המוחלט כי לכל $x\in\mathbb{Q}$ מתקיים $|x|_{\infty}^{\alpha}=|x|$ וברור כי $|\cdot|_{\infty}^{\alpha}$ מגדיר אותן סביבות פתוחות על $\mathbb{Q}$ כמו $|\cdot|_{\infty}$ שהרי

$$|x-a|_{\infty}^{\alpha}<\delta \iff |x-a|_{\infty}<\delta^{\frac{1}{\alpha}}$$

■

טענה 2.13 יהי F שדה בעל ערך מוחלט לא ארכימדי $|\cdot|$. אז אם $|x|\ne|y|$ מתקיים כי $|x+y|=\max\{|x|,|y|\}$.

הוכחה: נניח כי $|x|>|y|$ אז

$$\begin{aligned}|x+y| &\le \max\{|x|,|y|\}=|x|\\ |x|=|x+y-y| &\le \max\{|x+y|,|y|\}\end{aligned}$$

המקסימום האחרון הוא $|x+y|$ כי אחרת נקבל כי $|x|\le|y|$ בסתירה להנחה.
לכן $|x|<|x+y|$ ובסה"כ $|x|=|x+y|$. ■

טענה 2.14 יהי $(F,|\cdot|)$ שדה בעל ערך מוחלט לא ארכימדי. נגדיר

$$\begin{aligned}\mathcal{O}_F &= \{x\in F \mid |x|\le 1\}\\ \mathcal{P}_F &= \{x\in F \mid |x|< 1\}\\ \mathcal{O}_F^* &= \{x\in F \mid |x|= 1\}\end{aligned}$$

אז $\mathcal{O}_F$ חוג חלקי של F, $\mathcal{P}_F$ אידיאל מקסימלי של $\mathcal{O}_F$, וזהו האידיאל המקסימלי היחיד של $\mathcal{O}_F$. $\mathcal{O}_F^*$ חבורת ההפיכים של החוג $\mathcal{O}_F$.
$\mathcal{O}_F$ פתוחה (וגם סגורה), $\mathcal{P}_F$ סגורה (וגם פתוחה), וכן $\mathcal{O}_F^*$ פתוחה (וגם סגורה).

הוכחה: $\mathcal{O}_F$ סגור לכפל כי אם $x,y\in\mathcal{O}_F$ אז

$$|xy| = |x|\cdot|y| \quad\le\quad 1\cdot 1 = 1$$

בנוסף $\mathcal{O}_F$ סגור לחיבור:

$$|x+y| \quad\le\quad \max\{|x|,|y|\}\le 1$$

$1\in\mathcal{O}_F$. אם $x\in\mathcal{O}_F$ אז אם מתקיים כי $\frac{1}{x}\in\mathcal{O}_F$ אז $\left|\frac{1}{x}\right|\le 1$ ולכן $|x|\ge 1$. מצד שני $|x|\le 1$ ולכן $|x|=1$.
להפך אם $|x|=1$ אז x הפיך ב$\mathcal{O}_F$ כי $\left|\frac{1}{x}\right| = \frac{1}{|x|}=1$ ולכן $\frac{1}{x}\in\mathcal{O}_F$. לכן $\mathcal{O}_F^*=\mathcal{O}_F\backslash\mathcal{P}_F$
$\mathcal{P}_F$ סגור לחיבור

$$x,y\in\mathcal{P}_F \quad\Longrightarrow\quad |x+y|\le\max\{|x|,|y|\}<1$$

ולכן $x+y\in\mathcal{O}_F$. $\mathcal{P}_F$ סגור לכפל באיברי $\mathcal{O}_F$: יהי $x\in\mathcal{O}_F$ ו$y\in\mathcal{P}_F$. אז

$$|xy| \quad=\quad |x|\cdot|y|\le|y|<1$$

לכן $\mathcal{P}_F$ אידיאל ב$\mathcal{O}_F$. אם $I\subsetneq\mathcal{O}_F$ אדיאל אז $I\cap\mathcal{O}_F^*=\emptyset$ ולכן $I\subseteq\mathcal{O}_F\setminus\mathcal{O}_F^*=\mathcal{P}_F$.
נראה כי $\mathcal{O}_F^*$ פתוחה: יהי $a\in\mathcal{O}_F^*$ נראה כי

$$\{x\in F \mid |x-a|<1\} \quad=\quad a+\mathcal{P}_F\subseteq\mathcal{O}_F^*$$

נניח כי $x\in\mathcal{P}_F$ אז $|x|<1=|a|$ מכאן

$$|a+x| \quad=\quad \max\{|a|,|x|\}=1$$

לכן $\mathcal{O}_F=\mathcal{P}_F\cup\mathcal{O}_F^*$ פתוחה (כאיחוד של שתי קבוצות פתוחות).
בנוסף $\mathcal{P}_{\mathcal{F}}=\mathcal{O}_F\cap(F\setminus\mathcal{O}_F^*)$ סגורה כחיתוך של קבוצות סגורות. ∎

טענה 2.15 יהי $(F,|\cdot|)$ שדה עם ערך מוחלט לא ארכימדי.

1. אם $a_n\xrightarrow[n\to\infty]{}a$ סדרה מתכנסת בF כך ש$a\neq 0$ אז החל ממקום מסוים $|a_n|=|a|$.

2. $F \supseteq \{a_n\}_{n=1}^{\infty}$ היא סדרת קושי $\iff$ $|a_{n+1}-a_n| \underset{n\to\infty}{\longrightarrow} 0$

הוכחה:

1. נבחר $\varepsilon = |a|$. יש N טבעי כך שלכל $n \geq N$ מתקיים $|a_n - a| < |a| = \varepsilon$. ואז

$$|a_n| \;=\; |a_n - a + a| = \max\{|a_n - a|, |a|\} = |a|$$

2. אם הסדרה היא סדרת קושי, התנאי ברור. להפך, נניח כי $|a_{n+1}-a_n| \underset{n\to\infty}{\longrightarrow} 0$. יהי $\varepsilon > 0$, קיים N טבעי כך שלכל $n > N$ מתקיים $|a_{n+1}-a_n| < \varepsilon$.
יהיו $m, n \geq N$. נניח כי $m > n$

$$\begin{aligned}|a_m - a_n| &= |a_m - a_{m-1} + a_{m-1} - a_{m-2} + \ldots + (a_{n+1} - a_n)| \\ &\leq \max\{|a_m - a_{m-1}|, |a_{m-1} - a_{m-2}|, \ldots, |a_{n+1} - a_n|\} \\ &\leq \varepsilon\end{aligned}$$

ולכן $\{a_n\}_{n=1}^{\infty}$ סדרת קושי.

■

טענה 2.16 יהי $(F, |\cdot|)$ שדה בעל ערך מוחלט. אז כל סדרת קושי ב-F היא חסומה.

הוכחה: כרגיל. ■

2.2 השלמת שדות

$(F, |\cdot|)$ שדה בעל ערך מוחלט.
תהי R קבוצת כל סדרות קושי ב-F. R חוג ביחס לחיבור וכפל סדרות לפי קואורדינטות.
קל לראות כי סכום של שתי סדרות קושי הוא סדרת קושי. באשר לכפל:

$$|x_n y_n - x_m y_m| \;\leq\; |x_n - x_m| \cdot |y_n| + |x_m| \cdot |y_n - y_m|$$

מאחר ו-x_n, y_n סדרות קושי, $|x_n| \leq A, |y_n| \leq B$ ואז

$$|x_n y_n - x_m y_m| \;\leq\; B \cdot |x_n - x_m| + A \cdot |y_n - y_m| \underset{m,n\to\infty}{\longrightarrow} 0$$

נגדיר $R \supseteq \mathfrak{M}$ קבוצת כל הסדרות ב-F השואפות לאפס. זהו אידיאל של R.

טענה 2.17 $R/\mathfrak{M}$ הוא שדה.

הוכחה: נניח כי $\{a_n\}_{n=1}^{\infty} + \mathfrak{M} \neq \mathfrak{M}$ כלומר $a_n \underset{n\to\infty}{\not\longrightarrow} 0$.
מתקיים

$$\begin{aligned}|a_n| &= |(a_n - a_m) + a_m| \\ &\geq |a_m| - |a_n - a_m|\end{aligned}$$

מאחר וa_n אינה מתכנסת לאפס, קיים $2\varepsilon_0 > 0$ כך שלכל J יש $m_J > J$ המקיים $|a_{m_J}| > 2\varepsilon_0$.
נקח N טבעי כך שלכל $m,n \geq N$ מתקיים $|a_n - a_m| < \varepsilon_0$ ונבחר $m \geq N$ כך ש $|a_m| > 2\varepsilon_0$. אז מתקיים

$$|a_n| > 2\varepsilon_0 - \varepsilon_0 = \varepsilon_0 > 0$$

לכן מתקיים לכל $n \geq N_0$ מתקיים $|a_n| > \varepsilon_0$. נסתכל על הביטוי הבא ל$m,n \geq N$

$$\left|\frac{1}{a_n} - \frac{1}{a_m}\right| = \frac{|a_n - a_m|}{|a_n a_m|} \leq \frac{|a_n - a_m|}{\varepsilon^2} \underset{n,m\to\infty}{\longrightarrow} 0$$

לכן $\left\{\frac{1}{a_n}\right\}$ סדרת קושי החל מהאינדקס N. נגדיר

$$\alpha_n = \begin{cases} 1 & n < N \\ \frac{1}{a_n} & n \geq N \end{cases}$$

אז $\{\alpha_n\}_{n=1}^{\infty} \in R$ וכן

$$(\{a_n\}_{n=1}^{\infty} + \mathfrak{M}) \cdot (\{\alpha_n\}_{n=1}^{\infty} + \mathfrak{M}) = 1 + \mathfrak{M}$$

F משוכן ב$R/\mathfrak{M}$ על ידי

$$i(a) = \{a, a, \ldots, a, \ldots\} + \mathfrak{M}$$

נגדיר

$$|\{a_n\}_{n=1}^{\infty} + \mathfrak{M}| = \lim_{n\to\infty} |a_n|$$

מתקיים

$$||a_n| - |a_m|| \leq |a_n - a_m| \underset{n,m\to\infty}{\longrightarrow} 0$$

לכן $\{|a_n|\}_{n=1}^{\infty}$ סדרת קושי ב$\mathbb{R}$ ולכן מתכנסת. קל לראות כי הגדרה זו טובה ואינה תלויה בנציג $\{a_n\}_{n=1}^{\infty}$.
זה ערך מוחלט על $R/\mathfrak{M}$:

$$\begin{aligned} |\{a_n\} + \mathfrak{M}| &= 0 \\ &\Longleftrightarrow \\ \lim_{n\to\infty} |a_n| &= 0 \\ &\Longleftrightarrow \\ \{a_n\} &\in \mathfrak{M} \end{aligned}$$

כפליות:

$$\begin{aligned} |(\{a_n\}+\mathfrak{M})\cdot(\{b_n\}+\mathfrak{M})| &= |\{a_nb_n\}+\mathfrak{M}| \\ &= \lim_{n\to\infty}|a_nb_n| \\ &= \lim_{n\to\infty}(|a_n|\cdot|b_n|) \\ &= \lim_{n\to\infty}|a_n|\cdot\lim_{n\to\infty}|b_n| \\ &= |(\{a_n\}+\mathfrak{M})|\cdot|(\{b_n\}+\mathfrak{M})| \end{aligned}$$

באופן דומה אי שוויון המשולש.

אם $a\in F$ אז $|i(a)|=\lim_{n\to\infty}|a|=|a|$.

ההוכחה כי המרחב שלם וכי $i(F)$ צפוף כרגיל.

צפיפות למשל: $i(F)$ צפוף ב$R/\mathfrak{M}$:

$$\{a_n\}_{n=1}^{\infty}+\mathfrak{M} \quad\in\quad R/\mathfrak{M}$$

נטען כי $\lim_{n\to\infty} i(a_n)=\{a_n\}_{n=1}^{\infty}+\mathfrak{M}$:

$$|(\{a_n\}_{n=1}^{\infty}+\mathfrak{M})-i(a_k)| \quad=\quad \lim_{n\to\infty}|a_n-a_k|\underset{k\to\infty}{\longrightarrow}0$$

כי a_n סדרת קושי. ■

נסמן את ההשלמה של $\left(\mathbb{Q},|\cdot|_p\right)$ ב$\mathbb{Q}_p$. השלמה זו נקראת שדה המספרים הp־אדיים (נמשיך לסמן ב$|\cdot|_p$ את הערך המוחלט של $\mathbb{Q}_p$).

יהי $x\in\mathbb{Q}_p$ $x\neq 0$ ותהי $\{x_n\}_{n=1}^{\infty}\subseteq\mathbb{Q}$ המתכנסת לx (ביחס ל$|\cdot|_p$).

כיוון שמדובר בערך מוחלט לא ארכימדי, החל ממקום מסוים $|x|_p=|x_n|_p$ ולכן $|\mathbb{Q}_p|_p=|\mathbb{Q}|_p$ ($|A|_p$ זו התמונה של $|\cdot|_p$ על הקבוצה A).

לכן יש $l\in\mathbb{Z}$ כך ש $|x|_p=p^{-l}$.

נסמן $\mathbb{Z}_p=\left\{x\in\mathbb{Q}_p \mid |x|_p\le 1\right\}$. מתקיים

$$\begin{aligned} p\mathbb{Z}_p &= \left\{x\in\mathbb{Q}_p \mid |x|_p\le p^{-1}\right\} \\ &= \left\{x\in\mathbb{Q}_p \mid |x|_p< 1\right\} \end{aligned}$$

ומתקיים

$$\mathbb{Z}_p^* \quad=\quad \left\{x\in\mathbb{Q}_p \mid |x|_p=1\right\}$$

יהי $x\in\mathbb{Q}_p$ $x\neq 0$, אז $|x|_p=p^{-l}=\left|p^l\right|_p$ כאשר l שלם.

$$\left|p^{-l}x\right|_p \quad=\quad 1$$

ולכן $\varepsilon=p^{-l}x\in\mathbb{Z}_p^*$. כלומר $x=\varepsilon p^l$ כאשר ε נקבע באופן יחיד לפי $p^{-l}=|x|_p$.

טענה 2.18 כל אידיאל אמיתי של $\mathbb{Z}_p$ הוא מהצורה $p^l\mathbb{Z}_p$ כאשר l טבעי (בפרט $\mathbb{Z}_p$ הוא חוג ראשי והאידיאלים של $\mathbb{Z}_p$ מסודרים בשרשרת $\ldots \underset{\neq}{\supseteq} p^2\mathbb{Z}_p \underset{\neq}{\supseteq} p\mathbb{Z}_p \underset{\neq}{\supseteq} \mathbb{Z}_p$).

הוכחה: יהי $I \underset{\neq}{\subseteq} \mathbb{Z}_p$ אידיאל. איברי I אינם הפיכים. לכל $x \in I$ מתקיים $|x| = p^{-l}$ כאשר l טבעי.
יהי $a \in I$ כך ש $|a| = p^{-N}$ מקסימלי (כלומר N מינימלי).
יהי $x \in I$. כיוון ש $|x| \leq |a|$ מתקיים כי $\left|a^{-1}x\right| \leq 1$ ולכן $a^{-1}x \in \mathbb{Z}_p$, ולכן $x \in a\mathbb{Z}_p$.
כלומר $I \subseteq \mathbb{Z}_p \cdot a$ ולכן $I = \mathbb{Z}_p \cdot a$.
נכתוב $a = \varepsilon \cdot P^N$ כאשר $\varepsilon \in \mathbb{Z}_p^*$. אז

$$\mathbb{Z}_p \cdot a = (\mathbb{Z}_p \cdot \varepsilon) \cdot p^N = \mathbb{Z}_p \cdot p^N$$

מתקיים

$$\begin{aligned} \mathbb{Z}_p \cdot p^N &= \left\{x \in \mathbb{Q}_p \mid |x|_p \leq p^{-N}\right\} \\ &= \left\{x \in \mathbb{Q}_p \mid |x|_p < p^{-N+1}\right\} \end{aligned}$$

■

משפט 2.19 יהי $x \in \mathbb{Z}_p$. אז קיימת סדרה יחידה $\{b_n\}_{n=1}^{\infty}$ של מספרים שלמים כך $0 \leq$ $b_n < p$ וכן

$$x = \sum_{n=0}^{\infty} b_n p^n$$

להפך, כל טור כזה מגדיר איבר ב$\mathbb{Z}_p$.

הערה 2.20 נניח כי $(F, |\cdot|)$ שדה שלם עם ערך מוחלט לא ארכימדי. אז $\sum_{n=1}^{\infty} a_n$ מתכנס בF אם ורק אם $a_n \underset{n\to\infty}{\longrightarrow} 0$, כי $s_n = \sum_{k=1}^{n} a_k$ מגדירה סדרת קושי $\iff a_n = s_n - s_{n-1} \underset{n\to\infty}{\longrightarrow} 0$.

הוכחה: (של המשפט): נשים לב כי הטור מתכנס, כיוון ש

$$\begin{aligned} |b_n \cdot p^n|_p &= |b_n|_p \cdot p^{-n} \\ &\leq p^{-n} \underset{n\to\infty}{\longrightarrow} 0 \end{aligned}$$

$\mathbb{Q}$ צפוף ב$\mathbb{Q}_p$ ולכן יש $a \in \mathbb{Q}$ כך ש

$$|x - a|_p \leq p^{-1} \cdot |x|_p$$

כיוון ש$|x|_p > p^{-1}|x|_p$ מתקיים כי

$$\begin{aligned} |a|_p &= |a - x + x|_p \\ &= |x|_p \end{aligned}$$

נכתוב $a=\frac{r}{s}$ - מנה מצומצמת של שלמים.
$1 \geq |x|_p = |a|_p$ ולכן $s \nmid p$.
יהיו $u,v\in\mathbb{Z}$ כך ש$up+vs=1$

$$\begin{aligned} |a-vr|_p &= \left|\frac{r}{s}-vr\right|_p \\ &= \left|\frac{r}{s}\right|_p \cdot |1-vs|_p \\ &= |a|_p \cdot |u|_p \cdot p^{-1} \\ &\leq p^{-1}\cdot |a|_p \\ &= p^{-1}\cdot |x|_p \end{aligned}$$

נסמן $p^{-N} = p^{-1}\cdot |x|_p$ כאשר N טבעי. מתקיים

$$\begin{aligned} |x-a|_p &\leq p^{-1}\cdot |x|_p = p^{-N} \\ |a-vr|_p &\leq p^{-N} \end{aligned}$$

לכן

$$\begin{aligned} |x-vr|_p &= |(x-a)+(a-vr)|_p \\ &\leq \max\left\{|x-a|_p, |a-vr|_p\right\} \\ &\leq p^{-N} \\ &\leq p^{-1}\cdot |x|_p \end{aligned}$$

לכן אפשר להחליף את a בvr ובקיצור להניח כי $a\in\mathbb{Z}$. (אפשר לשפץ את הארגומנט ולהראות כי למעשה $\mathbb{Z}$ צפוף ב$\mathbb{Z}_p$)
כיוון ש$a\in\mathbb{Z}$ נכתוב $a=\alpha\cdot p^{N-1}$ כאשר $\alpha\in\mathbb{Z}$ וזר לp. נחלק את α עם שארית

$$\alpha = \beta\cdot p + t$$

כאשר $0<t<p$.

$$a = \beta\cdot p^N + t\cdot p^{N-1}$$

נסמן $b=t\cdot p^{N-1}$ אז $p^{N-1}\leq b<p^N$ ו$\nu_p(b)=N-1$. מתקיים

$$|a|_p = |b|_p = p^{-N+1}$$

$$\begin{aligned} |x-b|_p &= \left|x-a+\beta\cdot p^N\right|_p \\ &\leq \max\left\{|x-a|_p, p^{-N}|\beta|_p\right\} \\ &\leq p^{-N} \\ &= p^{-1}|x|_p \end{aligned}$$

לכן אפשר להחליף את a בb ובקיצור אפשר להניח כי $p^{N-1} \le a < p^N$ ו $|x|_p = |a|_p = p^{-N+1}$.

נסמן $x - a = y$, $|y|_p \le p^{-N}$. בנוסף נסמן $a = b_{N-1}p^{N-1}$ כאשר $1 \le b_{N-1} = t < p$.

נקבל $x = b_{N-1}p^{N-1} + y$ כאשר $1 \le b_{N-1} \le p-1$ ו $|y|_p \le p^{-N}$.

ועכשיו נבצע אותו תהליך לy. כך נקבל סדרה שלמים בקטע $b_{N-1} = [1, p-1]$ $b_{N_1}, b_{N_2}, \ldots$. כאשר $N_1 < N_2 < \ldots$ וכך ש

$$x = \sum_{i=1}^{k-1} b_{N_i} p^{N_i} + y_k$$

כאשר $|y_k|_p \le p^{-N_{k-1}-1}$. כמובן

$$y_k \underset{k\to\infty}{\longrightarrow} 0$$

ולכן מתקיים

$$x = \sum_{n=0}^{\infty} b_n p^n$$

נראה יחידות: נניח כי

$$\sum_{n=0}^{\infty} a_n p^n = \sum_{n=0}^{\infty} b_n p^n$$

כאשר $0 \le a_n, b_n \le p-1$ אז

$$\begin{aligned} a_0 - b_0 &= \sum_{n=1}^{\infty} (b_n - a_n) p^n \\ &= p \sum_{n=0}^{\infty} (b_{n+1} - a_{n+1}) p^n \\ &= p \cdot \lim_{k\to\infty} \sum_{n=0}^{k} (b_{n+1} - a_{n+1}) p^n \end{aligned}$$

לכן מאחר ו

$$\left| \sum_{n=0}^{k} (b_{n+1} - a_{n+1}) p^n \right| \le \max_{0\le n\le k} \left(|b_{n+1} - a_{n+1}|_p \, p^{-n} \right) \le 1$$

נקבל

$$|a_0 - b_0|_p \le p^{-1}$$

מאחר ו

$$1 - p \le a_0 - b_0 \le p - 1$$

ובנוסף

$$p \quad | \quad a_0 - b_0$$

נקבל $a_0 - b_0 = 0$. נוכל כעת לקבל

$$a_1 + \sum_{k=2}^{\infty} a_k p^{k-1} \quad = \quad b_1 + \sum_{k=2}^{\infty} b_k p^{k-1}$$

וכך נקבל $a_1 = b_1$, $a_2 = b_2$ וכו'. ■

הערה 2.21 (דוגמה):

$$\sum_{n=0}^{\infty} p^n \quad = \quad \frac{1}{1-p}$$

$$\sum_{n=0}^{k} p^n \quad = \quad \frac{1-p^{k+1}}{1-p} \underset{k\to\infty}{\longrightarrow} \frac{1}{1-p}$$

אם $x \in \mathbb{Q}_p$, כך ש$|x|_p > 1$ אז נכתוב $|x|_p = p^N = \left|p^{-N}\right|_p$ כאשר N טבעי ולכן $\left|p^N x\right|_p = 1$

$$p^N \cdot x \quad = \quad \sum_{n=0}^{\infty} b_n p^n$$

כאשר $0 \leq b_n \leq p-1$ ומכאן נקבל

$$\begin{aligned} x &= \sum_{n=0}^{\infty} b_n p^{n-N} \\ &= \frac{b_0}{p^N} + \frac{b_1}{p^{N-1}} + \ldots + b_N + b_{N+1} \cdot p + \ldots \end{aligned}$$

באופן כללי

$$x \quad = \quad \sum_{n=-N}^{\infty} a_n p^n$$

כאשר $\{a_n\}$ נקבעת באופן יחיד.

יהי $x \in \mathbb{Q}_p$. נכתוב $x = \sum_{n=m}^{\infty} a_n p^n$ כאשר $0 \leq a_n < p$ שלמים, $m \in \mathbb{Z}$ ו$1 \leq a_m < p$.

אז

$$x \quad = \quad a_m p^m + \sum_{n=m+1}^{\infty} a_n p^n$$

ומתקיים

$$\begin{aligned}\left|\sum_{n=m+1}^{\infty}a_np^n\right|_p &\le \max_{m+1\le n}|a_np^n|\\ &\le p^{-(m+1)}\end{aligned}$$

בנוסף

$$\begin{aligned}|a_mp^m|_p &= |a_m|_p\cdot p^{-m}\\ &= p^{-m}\\ &> p^{-(m+1)}\\ &= \left|\sum_{n=m+1}^{\infty}a_np^n\right|_p\end{aligned}$$

לכן $|x|_p=p^{-m}$

$$\begin{aligned}\mathbb{Z}_p &= \left\{\sum_{n=0}^{\infty}a_np^n \mid 0\le a_n<p\right\}\\ p^N\mathbb{Z}_p &= \left\{\sum_{n=N}^{\infty}a_np^n \mid 0\le a_n<p\right\}\end{aligned}$$

מסקנה 2.22 $\mathbb{Z}$ צפוף ב$\mathbb{Z}_p$, ואפילו $\mathbb{N}$ צפוף ב$\mathbb{Z}_p$.

משפט 2.23 $\mathbb{Z}_p/p\mathbb{Z}_p\cong\mathbb{F}_p$ (איזומורפיים כשדות)

הוכחה: נגדיר

$$t\left(\sum_{n=0}^{\infty}a_np^n\right) = a_0+p\mathbb{Z}$$

נסמן $a_0=a_0(x)$.

$$x \equiv a_0(x)\,(\mod p\mathbb{Z}_p)$$

לכן אם $x\equiv y\,(\mod p\mathbb{Z}_p)$ (כאשר $x,y\in\mathbb{Z}_p$) אז $a_0(x)\equiv a_0(y)\,(\mod p\mathbb{Z}_p)$. מכאן

$$|a_0(x)-a_0(y)|_p \le p^{-1}$$

כלומר $p\mid a_0(x)-a_0(y)$ ולכן $a_0(x)=a_0(y)$ (כי $0\le a_0(x),a_0(y)\le p-1$). לכן $t(x)=t(y)$.

להפך, אם $t(x)=t(y)$ נקבל כי $a_0(x)-a_0(y)\in p\mathbb{Z}\subseteq p\mathbb{Z}_p$ כי $x\equiv y\,(\mod p\mathbb{Z}_p)$.

מתקיים

$$\begin{aligned}x+y &\equiv a_0(x)+a_0(y)\,(\mod p\mathbb{Z}_p)\\ t(x+y) &= t(a_0(x)+a_0(y))\end{aligned}$$

נחלק בp עם שארית:

$$a_0(x)+a_0(y) = p\cdot b+c_0$$

כאשר $0\le c_0<p$

$$t(a_0(x)+a_0(y)) = c_0+p\mathbb{Z}$$

בנוסף

$$\begin{aligned} t(x)+t(y) &= a_0(x)+a_0(y)+p\mathbb{Z} \\ &= c_0+p\mathbb{Z} \end{aligned}$$

לכן

$$t(x+y) = t(x)+t(y)$$

באופן דומה:

$$t(xy) = t(x)\cdot t(y)$$

לכן $t:\mathbb{Z}_p\to\mathbb{Z}/p\mathbb{Z}$ הומומורפיזם של חוגים. ברור כי t על ו

$$\begin{aligned} \ker t &= \{x\in\mathbb{Z}_p \mid t(x)=0\} \\ &= \{x\in\mathbb{Z}_p \mid a_0(x)=0\} \\ &= p\mathbb{Z}_p \end{aligned}$$

ממשפט ההומורפיזם הראשון:

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$$

■

באופן דומה נכליל:

משפט 2.24 לכל n טבעי $\mathbb{Z}_p/p^n\mathbb{Z}_p\cong\mathbb{Z}/p^n\mathbb{Z}$ איזומורפיזם של חוגים.

הוכחה: ע"י האיזומורפיזם המושרה מ$t:\mathbb{Z}_p\to\mathbb{Z}/p^n\mathbb{Z}$ המוגדר באופן דומה לקודם

$$t\left(\sum_{k=0}^{\infty}a_kp^k\right) = \sum_{k=0}^{n-1}a_kp^k+p^n\mathbb{Z}$$

הומומורפיזם על, עם $\ker t=p^n\mathbb{Z}_p$. ■

מסקנה 2.25 מתקיים

1. $[\mathbb{Z}_p:p\mathbb{Z}_p]=p$
2. $[\mathbb{Z}_p:p^n\mathbb{Z}_p]=p^n$

הערה 2.26 נשים לב לשרשרת

$$\mathbb{Z}_p \supseteq p\mathbb{Z}_p \supseteq p\mathbb{Z}_p^2 \quad \supseteq \ldots \quad \supseteq p^{n-1}\mathbb{Z}_p \supseteq p^n\mathbb{Z}_p \supseteq \ldots$$

בכל שלב בשרשרת

$$p^{n-1}\mathbb{Z}_p/p^n\mathbb{Z}_p \quad \cong \quad \mathbb{Z}_p/p\mathbb{Z}_p$$

כחבורות חיבוריות ע"י

$$p^{n-1}\cdot x + p^n\mathbb{Z}_p \quad \mapsto \quad x + p\mathbb{Z}_p$$

משפט 2.27 $\mathbb{Z}_p$ קומפקטי

הוכחה: מאחר ואנו במרחב מטרי, קומפקטיות שקולה לקומפקטיות סדרתית. תהי $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{Z}_p$ ונוכיח כי יש לה תת־סדרה מתכנסת.

יש תת סדרה $\left\{x_n^{(1)}\right\}_{n=1}^{\infty}$ כך שיש $0 \le a_0 \le 1$ כך ש$x_n^{(1)} \equiv a_0 \pmod{p}$ לכל n.

יש תת סדרה $\left\{x_n^{(2)}\right\}_{n=1}^{\infty} \subseteq \left\{x_n^{(1)}\right\}_{n=2}^{\infty}$ כך שיש $0 \le a_1 < p$ המקיים $x_n^{(2)} \equiv a_0 + a_1 p \pmod{p^2}$ לכל n וכו'.

כך נמצא לכל k תת־סדרה $\left\{x_n^{(k)}\right\} \subseteq \left\{x_n^{(k-1)}\right\}_{n=2}^{\infty}$ וכן $0 \le a_0, a_1, \ldots, a_{k-1} \le p-1$

$$x_n^{(k)} \quad \equiv \quad a_0 + a_1 p + \ldots + a_{k-1}p^{k-1} \pmod{p^k\mathbb{Z}_p}$$

לכל n.

נתבונן בתת הסדרה

$$\left\{x_1^{(k)}\right\}_{k=1}^{\infty} \quad \subseteq \quad \{x_n\}_{n=1}^{\infty}$$

זאת סדרת קושי:

$$x_1^{(k+1)} \quad \equiv \quad \sum_{n=0}^{k} a_n p^n \pmod{p^{k+1}\mathbb{Z}_p}$$

ולכן גם

$$x_1^{(k+1)} \quad \equiv \quad \sum_{n=0}^{k} a_n p^n \pmod{p^{k}\mathbb{Z}_p}$$

בנוסף

$$x_1^{(k)} \quad \equiv \quad \sum_{n=0}^{k-1} a_n p^n \pmod{p^{k}\mathbb{Z}_p}$$

מתקיים

$$\begin{aligned} x_1^{(k+1)} - x_1^{(k)} &\equiv \sum_{n=0}^{k} a_n p^n - \sum_{n=0}^{k-1} a_n p^n \left(\mod p^k \mathbb{Z}_p \right) \\ &\equiv a_k p^k \left(\mod p^k \mathbb{Z}_p \right) \end{aligned}$$

ולכן

$$\left| x_1^{(k+1)} - x_1^{(k)} \right|_p \leq p^{-k} \underset{k\to\infty}{\longrightarrow} 0$$

לכן $\left\{ x_1^{(k)} \right\}_{k=1}^{\infty}$ מתכנסת לגבול $b \in \mathbb{Q}_p$ ומכיוון ש$\mathbb{Z}_p$ סגור, $b \in \mathbb{Z}_p$. ■

מסקנה 2.28 $p^n \mathbb{Z}_p$ קומפקטי לכל n שלם, בפרט כל עיגול (פתוח או סגור) ב$\mathbb{Q}_p$ הוא קומפקטי.

הוכחה: נזכר כי עיגול ב$\mathbb{Q}_p$ הוא קבוצה מהצורה

$$\begin{aligned} \left\{ x \in \mathbb{Q}_p \mid |x-a|_p < p^{-l} \right\} &= \left\{ x \in \mathbb{Q}_p \mid |x-a|_p \leq p^{-l-1} \right\} \\ &= a + p^{l+1} \mathbb{Z}_p \end{aligned}$$

שזו קבוצה קומפקטית. ■

מסקנה 2.29 $\mathbb{Q}_p$ קומפקטי מקומית: לכל נקודה ב$\mathbb{Q}_p$ סביבה (שהיא גם סגורה) קומפקטית.

טענה 2.30 $\mathbb{Q}_p$ הוא שדה המנות של $\mathbb{Z}_p$.

הוכחה: יהי $0 \neq x \in \mathbb{Q}_p$. אז יש $\varepsilon \in \mathbb{Z}_p^*$ ויש l שלם כך ש $x = \varepsilon \cdot p^l$ ($|x|_p = p^{-l}$).
אם $l \geq 0$ אז $x \in \mathbb{Z}_p$ ואז $x = \frac{x}{1}$.
אם $l < 0$ נכתוב $l = -n$, n טבעי $x = \frac{\varepsilon}{p^n}$ מנה של שני איברים ב$\mathbb{Z}_p$. ■

הגדרה 2.31 נניח כי $A \subseteq B$ חוגים קומוטטיביים עם יחידה. נאמר ש$b \in B$ שלם מעל A אם b מקיים משוואה מהצורה

$$1 \cdot b^n + a_{n-1} \cdot b^{n-1} + \ldots + a_1 \cdot b + a_0 = 0$$

כאשר $a_0, \ldots, a_{n-1} \in A$.

משפט 2.32 קבוצת כל איברי B שהם שלמים מעל A היא חוג חלקי לB: הסגור השלם של A בתוך B.

טענה 2.33 $\mathbb{Z}_p$ סגור בשלמות ב$\mathbb{Q}_p$, כלומר אם $x \in \mathbb{Q}_p$ שלם מעל $\mathbb{Z}_p$ אז $x \in \mathbb{Z}_p$.

הוכחה: נניח כי $x = \varepsilon \cdot p^{-l}$, $|\varepsilon|_p = 1$ ו־l טבעי שלם מעל $\mathbb{Z}_p$:

$$\varepsilon^n \cdot p^{-ln} + a_{n-1} \cdot \varepsilon^{n-1} \cdot p^{-l(n-1)} + \ldots + a_1 \cdot \varepsilon \cdot p^{-l} + a_0 \quad = \quad 0$$

כאשר $a_0, \ldots, a_{n-1} \in \mathbb{Z}_p$

$$\left|\varepsilon \cdot p^{-ln}\right|_p \quad = \quad p^{ln}$$

מצד שני

$$\begin{aligned} \left|\varepsilon \cdot p^{-ln}\right|_p &= \left|-a_{n-1} \cdot \varepsilon^{n-1} \cdot p^{-l(n-1)} - \ldots - a_1 \cdot \varepsilon \cdot p^{-l} - a_0\right|_p \\ &\leq \max_{0 \leq i \leq n-1} \left|a_i p^{-li}\right|_p \\ &\leq p^{l(n-1)} \end{aligned}$$

לכן קיבלנו

$$p^{ln} \quad \leq \quad p^{l(n-1)}$$

סתירה. ■

3 הסגור האלגברי של $\mathbb{Q}_p$ והשדה $\mathbb{C}_p$

3.1 שדות קומפקטיים מקומיים ומרחבים נורמיים ממימד סופי

$(|F|, |\cdot|)$ שדה בעל ערך מוחלט $|\cdot|$ (לא טריוואלי) שהוא קומפקטי מקומית כמרחב מטרי (לכל נקודה ב־F יש סביבה שהסגור שלה קומפקטי).

$\mathbb{Q}_p$ הוא שדה קומפקטי מקומית, גם $\mathbb{R}$ ו־$\mathbb{C}$.

טענה 3.1 לכל $r > 0$ נסמן

$$B_r \quad = \quad \{x \in F \mid |x| \leq r\}$$

B_r הוא קומפקטי לכל r.

הוכחה: תהי $U_0 \subseteq F$ סביבה של 0 כך ש־$\overline{U_0}$ קומפקטי. כיוון ש־U_0 פתוחה, יש עיגול פתוח ברדיוס $\varepsilon_0 > 0$ אשר מוכל ב־U_0.

$$B_{\varepsilon_0} \quad \subseteq \quad U_0$$

B_{ε_0} קבוצה סגורה, חלקית לקבוצה הקומפקטית $\overline{U_0}$ ולכן B_{ε_0} קומפקטית.

יהי $F \ni a \neq 0$ כך ש $|a| \leq \frac{\varepsilon_0}{r}$ (יש כזה כי $|\cdot|$ לא טריוואלי, ולכן יש $1 < |x_0|$ ואז $|x_0^n| \underset{n\to\infty}{\longrightarrow} \infty$ ולכן $\left|\frac{1}{x_0}\right|^n \underset{n\to\infty}{\longrightarrow} 0$)

לכל $x \in B_r$

$$\begin{aligned} |a \cdot x| &= |a| \cdot |x| \\ &\leq \frac{\varepsilon_0}{r} \cdot r \\ &= \varepsilon_0 \end{aligned}$$

ולכן

$$aB_r \quad \subseteq \quad B_{\varepsilon_0}$$

B_r קבוצה סגורה ולכן גם $a \cdot B_r$ סגורה, וכיוון ש B_{ε_0} קומפקטי, גם aB_r קומפקטי. מכאן, גם

$$B_r \quad = \quad \frac{1}{a}\left(a \cdot B_r\right)$$

קומפקטי. ■

מסקנה 3.2 כל עיגול סגור בF קומפקטי:

$$\{x \in F \mid |x-a| \leq r\} \quad = \quad a + B_r$$

מסקנה 3.3 F שלם.

הוכחה: תהי $\{x_n\}_{n=1}^{\infty} \subseteq F$ סדרת קושי. בפרט הסדרה חסומה, ולכן יש $r > 0$ כך ש$\{x_n\}_{n=1}^{\infty} \subseteq B_r$.
כיוון שB_r קומפקטי, יש תת־סדרה $\{x_{n_k}\}_{k=1}^{\infty}$ המתכנסת לגבול $a \in F$. נראה כי $x_n \underset{n\to\infty}{\longrightarrow} a$.
יהי $\varepsilon > 0$. יש N טבעי, כך ש$|x_n - x_m| \leq \varepsilon$ לכל $m, n \geq N$ וכן יש K טבעי כך שלכל $k \geq K$

$$|x_{n_k} - a| \quad \leq \quad \varepsilon$$

אפשר לבחור K כך ש$n_k \geq N$. נקבע $k_0 \geq K$.
לכל $n \geq N$

$$\begin{aligned} |x_n - a| &\leq \left|x_n - x_{n_{k_0}}\right| + \left|x_{n_{k_0}} - a\right| \\ &\leq \varepsilon + \varepsilon \\ &= 2\varepsilon \end{aligned}$$

■

הגדרה 3.4 יהי V מרחב וקטורי מעל שדה F (מניחים כי על F נתון ערך מוחלט לא טריוואלי). פונקציה $\|\cdot\| : V \to \mathbb{R}_+$ תקרא נורמה על V ביחס ל$(F, |\cdot|)$ אם

1. $v = 0 \Longleftrightarrow \|v\| = 0$
2. $\|\lambda \cdot v\| = |\lambda| \cdot \|v\|$ לכל $\lambda \in F$ ו$v \in V$
3. $\|u + v\| \leq \|u\| + \|v\|$

הערה 3.5 $(V, \|\cdot\|)$ הוא מרחב מטרי עם $d(u,v) = \|u - v\|$

נאמר כי $(V, \|\cdot\|)$ הוא מרחב נורמי מעל $(F, |\cdot|)$.

הגדרה 3.6 שתי נורמות $\|\cdot\|_1$, $\|\cdot\|_2$ תקראנה שקולות אם קיימים $c_1, c_2 > 0$ כך ש

$$c_2 \cdot \|v\|_1 \quad \leq \quad \|v\|_2 \leq c_1 \cdot \|v\|_1$$

הערה 3.7 (דוגמה): נניח כי $\dim_F V = n$. יהי $\{v_1, \ldots, v_n\}$ בסיס לV

$$\left\|\sum_{i=1}^{n} x_i v_i\right\|_\infty \quad = \quad \max_{1\leq i\leq n} |x_i|$$

($x_1, \ldots, x_n \in F$)

טענה 3.8 נניח כי $(F, |\cdot|)$ שדה קומפקטי מקומית. יהי V מרחב וקטורי ממימד n מעל F. אז $(V, \|\cdot\|_\infty)$ (ביחס לבסיס שקבענו $\{v_1, \ldots, v_n\}$) הוא מרחב נורמי מעל $(F, |\cdot|)$ ומרחב זה שלם וקומפקטי מקומית.

הוכחה: נראה ראשית כי $\|\cdot\|_\infty$ נורמה על V:

$$\left\|\sum_{i=1}^{n} x_i v_i\right\|_\infty \quad = \quad \max_{1\leq i\leq n} |x_i| = 0$$

$$\Longleftrightarrow$$

לכל i מתקיים $|x_i| = 0 \iff x_i = 0$ לכל $i \iff \sum_{i=1}^{n} x_i v_i = 0$.

הומוגניות:

$$\begin{aligned}
\left\|\lambda \cdot \left(\sum_{i=1}^{n} x_i v_i\right)\right\|_\infty &= \left\|\sum_{i=1}^{n} \lambda x_i v_i\right\|_\infty \\
&= \max_{1\leq i\leq n} |\lambda x_i| \\
&= |\lambda| \cdot \max_{1\leq i\leq n} |x_i| \\
&= |\lambda| \cdot \left\|\sum_{i=1}^{n} x_i v_i\right\|_\infty
\end{aligned}$$

אי־שוויון המשולש:

$$\begin{aligned}
\left\|\sum_{i=1}^{n} x_i v_i + \sum_{i=1}^{n} y_i v_i\right\|_\infty &= \max_{1\leq i\leq n} |x_i + y_i| \\
&\leq \max_{1\leq i\leq n} (|x_i| + |y_i|) \\
&\leq \max_{1\leq i\leq n} |x_i| + \max_{1\leq i\leq n} |y_i| \\
&= \left\|\sum_{i=1}^{n} x_i v_i\right\|_\infty + \left\|\sum_{i=1}^{n} y_i v_i\right\|_\infty
\end{aligned}$$

שלמות: כיוון ש‏ (אם $|\cdot|$ ערך מוחלט לא ארכימדי, נקבל $\|u+v\|_\infty \le \max\{\|u\|_\infty, \|v\|_\infty\}$

$$\left\|\sum_{i=1}^n x_i v_i - \sum_{i=1}^n a_i v_i\right\| = \max_{1\le i\le n} |x_i - a_i|$$

ברור כי $\left\{v^{(k)} = \sum_{i=1}^n x_i^{(k)} v_i\right\}_{k=1}^\infty$ מתכנסת לפי $\|\cdot\|_\infty$ $\Longleftrightarrow$ $\left\{x_i^{(k)}\right\}_{k=1}^\infty$ מתכנסת לכל $1\le i\le n$ ומתקיים

$$\lim_{k\to\infty} v^{(k)} = \sum_{i=1}^n \left(\lim_{k\to\infty} x_i^{(k)}\right) v_i$$

מכאן (בסימונים הנ"ל) הסדרה $\left\{v^{(k)}\right\}_{k=1}^\infty$ היא סדרת קושי $\Longleftrightarrow$ $\left\{x_i^{(k)}\right\}_{k=1}^\infty$ היא סדרת קושי לכל $1\le i\le n$. כיוון ש-F שלם, נסיק כי $(V, \|\cdot\|_\infty)$ מרחב שלם.

קומפקטיות מקומית: יהי $r>0$, נסמן

$$D_r = \{v\in V \mid \|v\|_\infty \le r\}$$

D_r קומפקטי: תהי $\left\{v^{(k)}\right\}_{k=1}^\infty \subseteq D_r$ נציג כמו קודם:

$$v^{(k)} = \sum_{i=1}^n x_i^{(k)} v_i$$

אז $\max_{1\le i\le n}\left|x_i^{(k)}\right| \le r$. לכן

$$\left\{x_i^{(k)}\right\}_{k=1}^\infty \subseteq B_r$$

לכל i.

B_r קומפקטי ולכן לסדרה $\left\{x_i^{(k)}\right\}_{k=1}^\infty$ יש תת־סדרה מתכנסת. מכאן, כל עיגול סגור הוא קומפקטי, ולכן המרחב קומפקטי מקומית. ■

משפט 3.9 יהי V מרחב וקטורי ממימד סופי מעל F (כנ"ל), אז כל שתי נורמות על V הן שקולות.

הוכחה: נשתמש בסימונים הנ"ל. תהי $\|\cdot\|$ נורמה על V. נראה כי היא שקולה ל-$\|\cdot\|_\infty$. יהי

$v=\sum_{i=1}^{n} x_i v_i$. מתקיים

$$\begin{aligned}\|v\| &\le \sum_{i=1}^{n} |x_i| \cdot \|v_i\| \\ &\le \left(\max_{1\le i\le n} |x_i|\right) \cdot \underbrace{\left(\sum_{i=1}^{n} \|v_i\|\right)}_{C_1} \\ &\le C_1 \cdot \|v\|_\infty\end{aligned}$$

נסמן $D=\{v\in V \mid \|v\|_\infty = 1\}$. D סגורה (ביחס ל $\|\cdot\|_\infty$) וחלקית לעיגול הסגור ברדיוס 1 סביב 0 (גם ביחס ל $\|\cdot\|_\infty$), שהוא קומפקטי, ולכן D קומפקטית (ביחס ל $\|\cdot\|_\infty$).

נוכיח כי קיים $\varepsilon_0 > 0$ כך ש$\|v\| \ge \varepsilon_0$ לכל $v\in D$.

אחרת יש סדרה $\left\{v^{(j)}\right\}_{j=1}^{\infty} \subseteq D$ כך ש $\left\|v^{(j)}\right\| \underset{j\to\infty}{\longrightarrow} 0$. יש ל$\left\{v^{(j)}\right\}_{j=1}^{\infty}$ תת־סדרה מתכנסת לפי $\|\cdot\|_\infty$. לכן אפשר להניח כי $\left\{v^{(j)}\right\}_{j=1}^{\infty}$ מתכנסת ל$v\in D$.

$$\begin{aligned}\|v\| &\le \left\|v^{(j)}\right\| + \left\|v - v^{(j)}\right\| \\ &\le \left\|v^{(j)}\right\| + C_1 \left\|v - v^{(j)}\right\|_\infty \underset{j\to\infty}{\longrightarrow} 0\end{aligned}$$

ולכן $\|v\| = 0$ ולכן $v=0$. סתירה, כי $v\in D$ ולכן $\|v\|_\infty = 1$.

לכן הראנו כי קיים ε_0 כנ"ל. יהי $0\ne v\in V$, $v=\sum_{i=1}^{n} x_i v_i$. מתקיים

$$\begin{aligned}\|v\|_\infty &= \max_{1\le i\le n} |x_i| \\ &= |x_k|\end{aligned}$$

ולכן

$$\left\|\frac{1}{x_k} v\right\|_\infty = 1$$

ולכן $\frac{1}{x_k} v \in D$ ולכן $\left\|\frac{1}{x_k} v\right\| \ge \varepsilon_0$. נקבל לכן

$$\begin{aligned}\|v\| &\ge \varepsilon_0 |x_k| \\ &= \varepsilon_0 \cdot \|x\|_\infty\end{aligned}$$

■

3.2 הרחבת הערך המוחלט מF לשדה הרחבה סופית וספרבילית $K\supseteq F$

$(F, |\cdot|)$ - שדה קומפקטי מקומית. יהי $K\supseteq F$ שדה הרחבה ממימד סופי.

טענה 3.10 יש ל-$|\cdot|$ לכל היותר הרחבה אחת לערך מוחלט על K.

הוכחה: $(K,|\cdot|_1)$, $(K,|\cdot|_2)$ הם בפרט מרחבים נורמיים מעל $(F,|\cdot|)$. מהמשפט הקודם, $|\cdot|_1$ ו-$|\cdot|_2$ שקולים כנורמות על K כמרחב וקטורי מעל $(F,|\cdot|)$ ולכן יש $0<c_1,c_2$ כך שלכל $a\in K$,

$$c_2\cdot|a|_1\le|a|_2\quad\le\quad c_1\cdot|a|_1$$

נציב a^n במקום a לכל n טבעי

$$\begin{aligned}c_2\cdot|a|_1^n\le|a|_2^n\quad&\le\quad c_1\cdot|a|_1^n\\ \sqrt[n]{c_2}\cdot|a|_1\le|a|_2\quad&\le\quad\sqrt[n]{c_1}\cdot|a|_1\end{aligned}$$

במעבר לגבול $n\to\infty$ נקבל

$$|a|_1\le|a|_2\quad\le\quad|a|_1$$

ולכן $|a|_1=|a|_2$. ■

מטרתנו להראות כעת אם K הרחבה ספרבילית, אז אכן קיימת הרחבה לערך המוחלט.

נניח כי $F\subseteq K$ שדה הרחבה סופית, ספרבילית.

ראשית נניח כי $F\subseteq K$ הרחבת גלואה. יהי $\sigma\in G_{K/F}$ ($\sigma:K\to K$ אוטומורפיזם של שדות, $\sigma|_F=\mathrm{id}_F$).

נניח כי $|\cdot|_K$ הוא הרחבה של $|\cdot|$ לערך מוחלט מ-F ל-K. יהי $x\in K$. נגדיר על $\sigma\in G_{K/F}$

$$|x|_\sigma\quad=\quad|\sigma(x)|_K$$

זהו ערך מוחלט על K:

$$\begin{aligned}|xy|_\sigma&=|\sigma(xy)|_K\\&=|\sigma(x)\sigma(y)|_K\\&=|\sigma(x)|_K|\sigma(y)|_K\\&=|x|_\sigma|y|_\sigma\end{aligned}$$

ובנוסף

$$\begin{aligned}|x+y|_\sigma&=|\sigma(x+y)|_K\\&=|\sigma(x)+\sigma(y)|_K\\&\le|\sigma(x)|_K+|\sigma(y)|_K\\&=|x|_\sigma+|y|_\sigma\end{aligned}$$

כיוון ש $|x|=|x|_K=|\sigma(x)|_K$ לכל $x\in F$, נקבל כי $|\cdot|_\sigma$ מרחיב את $|\cdot|$ על F לערך מוחלט של K. מהטענה הקודמת, $|x|_\sigma=|x|_K$ לכל $x\in K$ ולכן $|x|_K=|\sigma(x)|_K$.

נתבונן בביטוי $\prod_{\sigma\in G_{K/F}}\sigma(x)$. מכפלה זו אינווריאנטית ביחס לכל $\sigma\in G_{K/F}$, ולכן, מאחר ו-K הרחבת גלואה, מכפלה זו שייכת ל-F. מסמנים

$$N_{K/F}(x)\quad=\quad\prod_{\sigma\in G_{K/F}}\sigma(x)\in F$$

וקוראים ל־$N_{K/F}(x)$ "הנורמה של x ביחס להרחבה K/F".
מתקיים

$$\begin{aligned} \left|N_{K/F}(x)\right|_F &= \left|N_{K/F}(x)\right|_K \\ &= \prod_{\sigma\in G_{K/F}} |\sigma(x)|_K \\ &= |x|_k^{\left|G_{K/F}\right|} \end{aligned}$$

אם נסמן $\left|G_{K/F}\right| = [K:F] = n$ קיבלנו

$$\begin{aligned} |x|_k^n &= \left|N_{K/F}(x)\right|_F \\ |x|_k &= \left|N_{K/F}(x)\right|_F^{\frac{1}{n}} \end{aligned}$$

כלומר, הראנו כי אם K/F הרחבת גלואה, אז המועמד היחיד לערך מוחלט על $|\cdot|_K$ הוא $|x|_k = \left|N_{K/F}(x)\right|_F^{\frac{1}{n}}$.

3.2.1 תיאור נוסף של פונקציית הנורמה $N_{K/F}$

יהי $K \supseteq F$ שדה הרחבה סופית (וספרבילית) מסדר n. לכל $t \in K$ נגדיר

$$\begin{aligned} m_t : K &\to K \\ m_t(x) &= t\cdot x \end{aligned}$$

זאת העתקה לינארית של K כמרחב וקטורי מעל F.

הגדרה 3.11 $N_{K/F}(t) = \det(m_t)$

נתבונן בפולינום האי־פריק של t מעל F:

$$x^r + b_{r-1}x^{r-1} + \ldots + b_1x + b_0 \qquad b_0, b_1, \ldots, b_{r-1} \in F$$

(קובעים אחת ולתמיד סגור אלגברי $\overline{F}$ של F ומניחים $F \subseteq K \subseteq \overline{F}$)
$F[t] \subseteq K$ השדה הנוצר ע"י t מעל F. אנחנו יודעים כי $\left\{1, t, \ldots, t^{r-1}\right\}$ בסיס של $F[t]$ כמרחב וקטורי מעל F וכי

$$[F[t]:F] = r$$

נניח כי $[K:F[t]] = l$. אנחנו יודעים כי $r\cdot l = n$.
נבחר בסיס $\{u_1, \ldots, u_l\}$ ל־K כמרחב וקטורי מעל $F[t]$. אנו יודעים כי $\left\{t^iu_j\right\}_{1\le j\le l}^{0\le i\le r-1}$ בסיס ל־K מעל F.
נייצג את m_t כמטריצה ביחס לבסיס זה.

$$\mathrm{span}_F\{t^iu_j \quad | \; 0\le i\le r-1 \quad \}$$

אינווריאנטי ביחס לm_t, והמטריצה של m_t על תת מרחב זה אינה תלויה בj.

$$\begin{aligned} m_t\left(t^i u_j\right) &= t^{i+1} u_j \\ m_t\left(t^{r-1} u_j\right) &= t^r u_j \\ &= -\left(b_0 + b_1 t + \ldots + b_{r-1} t^{r-1}\right) u_j \end{aligned}$$

נסמן

$$c_t = \begin{pmatrix} 0 & 0 & & 0 & -b_0 \\ 1 & 0 & & 0 & -b_1 \\ 0 & 1 & \ddots & 0 & -b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & & 1 & -b_{r-1} \end{pmatrix}$$

ולכן המטריצה של m_t נראית כך

$$m_t = \begin{pmatrix} c_t & & & 0 \\ & c_t & & \\ & & \ddots & \\ 0 & & & c_t \end{pmatrix}$$

(הבלוק c_t מופיע על האלכסון l פעמים וביתר המקומות יש אפסים)
מתקיים

$$N_{K/F}(t) = \left(\det c_t\right)^l$$

ובנוסף ע"י פיתוח c_l לפי שורה ראשונה,

$$\det c_t = (-1)^r b_0$$

לכן

$$\begin{aligned} N_{K/F}(t) &= \left(\det c_t\right)^l \\ &= \left((-1)^r b_0\right)^l \\ &= (-1)^{rl} b_0^l \end{aligned}$$

מתקיים

$$x^r + b_{r-1} x^{r-1} + \ldots + b_1 x + b_0 = \prod_{i=1}^{r} \left(x - \sigma_i(t)\right)$$

כאשר $\overline{F} \ni \sigma_1(t), \ldots, \sigma_r(t)$ שונים זה מזה. (מספרביליות של K מעל F)
אפשר להרחיב את $\sigma_1, \ldots, \sigma_r$ לשיכונים של השדה $F[t]$ ב$\overline{F}$ מעל F

$$\sigma_i\left(a_0 + a_1 t + \ldots + a_{r-1} t^{r-1}\right) = a_0 + a_1 \sigma_i(t) + \ldots + a_{r-1} \sigma_i(t)^{r-1}$$

ל-$a_0,\ldots,a_{r-1}\in F$.

$$(-1)^r\,\sigma_1(t)\cdot\ldots\cdot\sigma_r(t) = b_0$$

ולכן

$$(-1)^r \quad b_0 = \prod_{i=1}^{n}\sigma_i(t)$$

מתקיים כי $\{\sigma_1,\ldots,\sigma_r\}$ היא בדיוק קבוצת כל השיכונים של $F[t]\hookrightarrow\overline{F}$ מעל F.
לכל $1\le i\le r$ יש ל-σ_i בדיוק l הרחבות לשיכונים של K ב-$\overline{F}$ וכך מתקבלת קבוצת כל השיכונים של K ב-$\overline{F}$ מעל F.
הקבוצה הזאת תסומן $G_{K/F}$.

$$\begin{aligned}\prod_{\sigma\in G_{K/F}}\sigma(t) &= \prod_{i=1}^{r}\sigma_i(t)^l\\ &= \underbrace{\left(\prod_{i=1}^{r}\sigma_i(t)\right)^l}_{N_{F[t]/F}(t)}\\ &= \left((-1)^r\,b_0\right)^l\\ &= (-1)^n\,b_0^l\\ &= N_{K/F}(t)\in F\end{aligned}$$

קיבלנו גם

$$N_{K/F}(t) = \left(N_{F[t]/F}(t)\right)^{[K:F(t)]}$$

משפט 3.12 יש ל-$|\cdot|$ הרחבה (יחידה) לערך מוחלט $|\cdot|_K$ על K.

הוכחה: נגדיר ל $t\in K$

$$\begin{aligned}|t|_K &= \left|N_{K/F}(t)\right|^{\frac{1}{n}}\\ &= \left|N_{F(t)/F}(t)\right|^{\frac{1}{[F(t):F]}}\\ &= |t|_{F(t)}\end{aligned}$$

מתקיים $|t|_K=0 \iff \left|N_{K/F}(t)\right|=0 \iff N_{K/F}(t)=0 \iff t=0$.

$$N_{K/F}(t\cdot s) = N_{K/F}(t)\cdot N_{K/F}(s)$$

ולכן

$$|t\cdot s|_K = |t|_K\cdot|s|_K$$

נניח $|x|_K \leq |y|_K$. צריך להראות כי

$$\begin{array}{rcl} |x+y|_K & \leq & \max\left\{|x|_K, |y|_K\right\} = |y|_K \\ & \Longleftrightarrow & \\ |y|_k \cdot \left|1+\frac{x}{y}\right|_k & \leq & |y|_k \\ & \Longleftrightarrow & \\ \left|1+\frac{x}{y}\right|_k & \leq & 1 \end{array}$$

מספיק לכן להראות כי $|1+z|_K \leq 1$ לכל $|z|_k \leq 1$.

כיוון שמתקיים כי $|z|_{F(z)} = |z|_K$ וכי $|1+z|_{F(z)} = |1+z|_k$ וכמובן $F(z) = F(z+1)$, ניתן להניח כי $K = F(z)$. לכן $\left\{1, z, \ldots, z^{n-1}\right\}$ בסיס של K כמרחב וקטורי מעל F.

ראינו $N_{K/F}(z) = \det(m_z) = \det C_z$ כאשר C_z המטריצה המייצגת של z לפי הבסיס הנ"ל.

$$\begin{array}{rcl} N_{K/F}(1+z) & = & \det(m_{1+z}) \\ & = & \det(I+m_z) \\ & = & \det(I_n+C_z) \end{array}$$

יהי r טבעי כלשהו

$$\begin{array}{rcl} |1+z|_K^r & = & \left|N_{K/F}(1+z)\right|_K^{\frac{r}{n}} \\ & = & \left|\det(I_n+C_z)^r\right|_K^{\frac{1}{n}} \end{array}$$

באופן כללי, לשדה עם ערך מוחלט לא ארכימדי $(F, |\cdot|)$ ולכל $X \in M_n(F)$ מתקיים

$$|\det X| \leq \max_{1\leq i,j\leq n}\left(|X_{ij}|^n\right) = \|X\|_\infty^n$$

ולכן

$$\begin{array}{rcl} |1+z|_K^r & \leq & \left|\det(I_n+C_z)^r\right|_K^{\frac{1}{n}} \\ & \leq & \left\|(I_n+C_z)^r\right\|_\infty \\ & = & \left\|\sum_{i=0}^{r}\binom{r}{i}C_z^i\right\|_\infty \\ & \leq & \max_{0\leq i\leq r}\left(\underbrace{\left|\binom{r}{i}\right|}_{\leq 1}\cdot\left\|C_z^i\right\|_\infty\right) \end{array}$$

$\left|\binom{r}{i}\right| \leq 1$ כי $|\cdot|$ לא ארכימדי.

$$|1+z|_K^r \leq \max_{0\leq i\leq r}\left(\left\|C_z^i\right\|_\infty\right)$$

נראה כי $\left\{\left\|C_z^i\right\|_\infty\right\}_{i=0}^\infty$ חסומה ואז נקבל

$$|1+z|_K^r \quad \leq \quad d$$

ולכן

$$|1+z|_K \quad \leq \quad \sqrt[r]{d}$$

לכל r טבעי ולכן $|1+z|_K \leq 1$ ונקבל את הדרוש.
נוכיח כעת כי אכן $\left\{\left\|C_z^i\right\|_\infty\right\}_{i=0}^\infty$ חסומה (נשים לב כי $C_z^i = C_{z^i}$).
בשלילה, נניח כי לכל j טבעי יש i_j טבעי כך ש

$$\left\|C_z^{i_j}\right\|_\infty \quad \geq \quad j$$

תהי t_j קואורדינטה של המטריצה $C_z^{i_j}$ שם מתקבל המקסימום

$$\max_{1\leq r,s\leq n}\left|C_z^{i_j}\right|_{r,s} \quad = \quad |t_j|$$

נתבונן במטריצה

$$B_j \quad = \quad \frac{1}{t_j}C_z^{i_j}$$

היא מקיימת

$$\|B_j\|_\infty \quad = \quad 1$$

כיוון ש $\{X\in M_n(F) \mid \|X\|_\infty = 1\}$ קבוצה קומפקטית, יש תת־סדרה $\{B_{j_l}\}_{l=1}^\infty$ המתכנסת למטריצה B, כך ש $\|B\|_\infty = 1$.
נטען כי $\det B = 0$.

$$\begin{aligned}
|\det B_j| \quad &= \quad \frac{1}{\left|t_j^n\right|}\cdot\left|\det\left(C_z^{i_j}\right)\right| \\
&\leq \quad \frac{1}{j^n}\cdot\left|N_{K/F}(z)\right|^{i_j} \\
&= \quad \frac{1}{j^n}\cdot|z|_K^{n\cdot i_j}
\end{aligned}$$

אבל $|z|_K \leq 1$ ולכן $|\det B_j| \underset{j\to\infty}{\to} 0$.
מאחר ודטרמיננטה היא פונקציה רציפה (כסכומים של מכפלות של פונקציות רציפות), נקבל $\det B_{j_l} \to \det B$ ולכן נסיק $\det B = 0$.
נסמן בK $T_B : K \to K$ את ההעתקה הלינארית מעל F שהמטריצה שלה לפי הבסיס $\left\{1,z,\ldots,z^{n-1}\right\}$ היא B.

יהי $0 \neq v \in K$ כך ש$T_B(v) = 0$. נראה כי T_B מתחלפת עם m_z:

$$\begin{aligned}BC_z &= \left(\lim_{l\to\infty} B_{j_l}\right) C_z \\ &= \lim_{l\to\infty}\left(\frac{1}{t_{j_l}} C_z^{i_{j_l}}\right) C_z \\ &= \lim_{l\to\infty} C_z \left(\frac{1}{t_{j_l}} C_z^{i_{j_l}}\right) \\ &= \lim_{l\to\infty} C_z B_{j_l} \\ &= C_z B\end{aligned}$$

נסיק כי $T_B \circ T_{z^i}(v) = 0$ לכל i, כלומר $T_B\left(z^i v\right) = 0$ לכל i.

כיוון שגם $\left\{v, zv, \ldots, z^{n-1}v\right\}$ בסיס של K מעל F, נקבל $T_B = 0$ ולכן $B = 0$. זאת סתירה כי $\|B\|_\infty = 1$. ■

3.3 הרחבות של $\mathbb{Q}_p$

ממה שעשינו עד כה, נובע כי קיימת הרחבה ל$|\cdot|_p$ על $\mathbb{Q}_p$ לערך מוחלט (לא ארכימדי) על $\overline{\mathbb{Q}_p}$.

$$\begin{aligned}t &\in \overline{\mathbb{Q}_p} \\ |t|_p &= \left|N_{\mathbb{Q}_p(t)/\mathbb{Q}}(t)\right|^{\frac{1}{[\mathbb{Q}_p(t):\mathbb{Q}_p]}}\end{aligned}$$

נניח כי $\overline{\mathbb{Q}_p} \subseteq F \subseteq \mathbb{Q}_p$ שדה הרחבה סופית ממעלה n.

$$\begin{aligned}\mathcal{O}_F &= \left\{x \in F \mid |x|_p \le 1\right\} \\ \mathcal{P}_F &= \left\{x \in F \mid |x|_p < 1\right\} \\ \mathcal{O}_F^* &= \left\{x \in F \mid |x|_p = 1\right\}\end{aligned}$$

משפט 3.13

1. $\mathcal{O}_F$ הוא הסגור השלם של $\mathbb{Z}_p$ בF.
2. $\mathcal{O}_F/\mathcal{P}_F$ הוא שדה הרחבה ממעלה $\le n$ של $\mathbb{F}_p$.

הוכחה:

1. נניח כי $t \in F$ שלם מעל $\mathbb{Z}_p$. כלומר, יש $a_0, a_1, \ldots, a_{r-1} \in \mathbb{Z}_p$ כך ש

$$t^r + a_{r-1}t^{r-1} + \ldots + a_1 t + a_0 = 0$$

לכן

$$\begin{aligned}|t|_p^r &= \left|-\left(a_{r-1}t^{r-1}+\ldots+a_1t+a_0\right)\right|_p\\ &\le \max_{0\le i\le r-1}\left\{|a_i|_p\cdot|t|_p^i\right\}\\ &= |a_{i_0}|_p\cdot|t|_p^{i_0}\\ &\le |t|_p^{i_0}\end{aligned}$$

כלומר קיבלנו $|t|_p^r \le |t|_p^{i_0}$ ולכן $|t|_p^{r-i_0} \le 1$ ומאחר ו$r-i_0\ge 1$ נקבל כי $|t|_p \le 1$.
להפך, נניח כי $t\in\mathcal{O}_F$. יהי $f(x)\in\mathbb{Q}_p[x]$ הפולינום האי־פריק של t מעל $\mathbb{Q}_p$.
נראה כי $f(x)\in\mathbb{Z}_p[x]$ ואז ינבע כי t שלם מעל $\mathbb{Z}_p$.

$$f(x) = \prod(x-\sigma(t))$$

כאשר $\sigma(t)$ צמודי גלואה של t מעל $\mathbb{Q}_p$. (σ עובר על $G_{\mathbb{Q}_p(t)/\mathbb{Q}_p}$)
לכל σ כזה נרחיב את σ לאיבר $\sigma'\in G_{F/\mathbb{Q}_p}$ ואז ל$s\in F$ נגדיר

$$\begin{aligned}|s|_{\sigma'} &= |\sigma'(s)|_{\sigma'(F)}\\ &= |\sigma'(s)|_p\end{aligned}$$

זה מגדיר ערך מוחלט $|\cdot|_{\sigma'}$ על F המרחיב את $|\cdot|_p$ על $\mathbb{Q}_p$.
מיחידות הרחבת הערך המוחלט מתקיים $|s|_{\sigma'}=|s|_p$ כלומר $|s|_p=|\sigma'(s)|_p$ לכל $s\in F$.
בפרט $|\sigma(t)|_p=|t|_p$.

$$\begin{aligned}f(x) &= \prod(x-\sigma(t))\\ &= x^m+s_{m-1}x^{m-1}+\ldots+s_1x+s_0\end{aligned}$$

המקדמים s_i של $f(x)$ הם כל אחד $\pm$(פולינום סימטרי בשורשים $\sigma(t)$) וכיוון שכל $\sigma(t)$ הוא בערך מוחלט $1 \ge$, נקבל כי $|s_i|_p\le 1$ ולכן $s_i\in\mathbb{Z}_p$.

2. ברור כי $\mathcal{P}_F\cap\mathbb{Z}_p=p\mathbb{Z}_p$. לכן אם נסתכל על

$$\begin{aligned}i:\mathbb{Z}_p/p\mathbb{Z}_p &\to \mathcal{O}_F/\mathcal{P}_F\\ i(a+p\mathbb{Z}_p) &= a+\mathcal{P}_F\end{aligned}$$

אז i שיכון של שדות. לפי זה, נראה את $\mathbb{F}_p\cong\mathbb{Z}_p/p\mathbb{Z}_p$ כשדה חלקי של $\mathcal{O}_F/\mathcal{P}_F$.
נראה כי $n+1$ איברים ב$\mathcal{O}_F/\mathcal{P}_F$ תלויים לינארית מעל $\mathbb{F}_p$ (כלומר מעל תמונת i)
יהיו

$$\varepsilon_1+\mathcal{P}_F,\ldots,\varepsilon_{n+1}+\mathcal{P}_F \in \mathcal{O}_F/\mathcal{P}_F$$

$n+1$ איברים שונים מאפס ב $\mathcal{O}_F/\mathcal{P}_F$ ולכן $|\varepsilon_i|_p=1$.
כיוון ש $n=[F:\mathbb{Q}_p]$ יש $\alpha_1,\ldots,\alpha_{n+1}\in\mathbb{Q}_p$ לא כולם אפסים כך ש

$$\sum_{i=1}^{n+1}\alpha_i\varepsilon_i = 0$$

על ידי הכפלה במכנה משותף (חזקה מתאימה של p), ניתן להניח כי $\alpha_i \in \mathbb{Z}_p$ לכל i. נצמצם את החזקה הגדולה ביותר של p המחלקת את כל ה$\alpha_i \in \mathbb{Z}_p$ ולכן נוכל להניח כי חלק מהם מקיימים $\left|\alpha_i\right|_p = 1$. מודולו $\mathcal{P}_F$ נקבל

$$\sum_{i=1}^{n} \left(\alpha_i + \mathcal{P}_F\right)\left(\varepsilon_i + \mathcal{P}_F\right) = \mathcal{P}_F$$

וזאת תלות לינארית לא טריוואלית מעל $\mathbb{F}_p$, כי יש i כך ש

$$\alpha_i + \mathcal{P}_F \neq \mathcal{P}_F$$

■

נרחיב את הגדרת ν_p מ$\mathbb{Q}_p$ ל$\overline{\mathbb{Q}_p}$. יהי $\overline{\mathbb{Q}_p} \ni t \neq 0$. נגדיר

$$\nu_p(t) = -\log_p |t|_p$$

מתקיים

$$\begin{aligned}
\nu_p(t) &= -\log_p |t|_p \\
&= -\log_p \left|N_{\mathbb{Q}(t)/\mathbb{Q}_p}(t)\right|_p^{\frac{1}{[\mathbb{Q}(t)/\mathbb{Q}_p]}} \\
&= \frac{1}{[\mathbb{Q}(t)/\mathbb{Q}_p]} \nu_p\left(N_{\mathbb{Q}(t)/\mathbb{Q}_p}(t)\right)
\end{aligned}$$

אם $\overline{\mathbb{Q}_p} \supseteq F \ni t$ ו $[F:\mathbb{Q}_p] = n$, אז

$$\nu_p(t) = -\frac{1}{n} \log_p \left|N_{F/\mathbb{Q}_p}(t)\right|_p$$

ממשיך להתקיים

$$\begin{aligned}
\nu_p(xy) &= \nu_p(x) + \nu_p(y) \\
\nu_p(x+y) &\geq \min\left\{\nu_p(x), \nu_p(y)\right\}
\end{aligned}$$

יהי $\overline{\mathbb{Q}_p} \supseteq F \supseteq \mathbb{Q}_p$ שדה הרחבה של $\mathbb{Q}_p$ ממעלה n.

$$\begin{aligned}
\frac{1}{n}\mathbb{Z} &\ni \nu_p(t) = -\frac{1}{n} \underbrace{\log_p \left|N_{F/\mathbb{Q}_p}(t)\right|_p}_{\in \mathbb{Z}} \\
\mathbb{Z} &= \nu_p\left(\mathbb{Q}_p^*\right) \subseteq \nu_p\left(F^*\right) \subseteq \frac{1}{n}\mathbb{Z}
\end{aligned}$$

$\nu_p(F^*)$ היא תת חבורה של $\frac{1}{n}\mathbb{Z}$ ולכן יש f טבעי כך ש

$$\nu_p\left(F^*\right) = \frac{f}{n}\mathbb{Z}$$

כיוון ש$\nu_p(F^*) \subseteq \mathbb{Z}$, מתקיים $1 \in \frac{f}{n}\mathbb{Z}$ ולכן יש e טבעי כך ש $\frac{fe}{n} = 1$, כלומר $fe = n$ ולכן

$$\nu_p(F^*) = \frac{1}{e}\mathbb{Z}$$

($e \mid n$)

נבחר $\pi \in F^*$ כך ש

$$-\log_p\left(|\pi|_p\right) = \nu_p(\pi) = \frac{1}{e}$$

זה אומר ש

$$\begin{aligned} |\pi|_p &= p^{-\frac{1}{e}} \\ \left|N_{F/\mathbb{Q}_p}(\pi)\right|_p &= |\pi|_p^n \\ &= p^{-\frac{n}{e}} \\ &= p^{-f} \end{aligned}$$

משפט 3.14 בסימונים הנ"ל

1. לכל $x \in F^*$ יש הצגה יחידה בצורה $x = \varepsilon\pi^r$ כאשר $\varepsilon \in \mathcal{O}_F^*$ ו$r \in \mathbb{Z}$.
2. $\mathcal{P}_F = \mathcal{O}_F\pi$
3. כל אידיאל $0 \neq$ של $\mathcal{O}_F$ הוא מהצורה $\mathcal{P}_F^l = \mathcal{O}_F\pi^l$ כאשר $l \geq 0$ שלם ולכן האידיאלים השונים מאפס של $\mathcal{O}_F$ מהווים שרשרת

$$\mathcal{O}_F \supseteq \mathcal{O}_F\pi = \mathcal{P}_F \supseteq \mathcal{O}_F\pi^2 = \mathcal{P}_F^2 \supseteq \ldots \supseteq \mathcal{O}_F\pi^l = \mathcal{P}_F^l \supseteq \mathcal{O}_F\pi^{l+1} = \mathcal{P}_F^{l+1} \supseteq \ldots$$

ולכל l מתקיים $\mathcal{P}_F^l \supsetneq \mathcal{P}_F^{l+1}$.

4. $p\mathcal{O}_F = \mathcal{P}_F^e = \mathcal{O}_F\pi^e$

הוכחה:

1. יהי $x \in F^*$. אז $\nu_p(x) = \frac{r}{e}$ כאשר $r \in \mathbb{Z}$ ולכן

$$\begin{aligned} |x|_p &= p^{-\frac{r}{e}} \\ &= \left(p^{-\frac{1}{e}}\right)^r \\ &= |\pi|_p^r \\ &= |\pi^r|_p \end{aligned}$$

לכן $\varepsilon = x\pi^{-r} \in \mathcal{O}_F$ (כי $|\varepsilon|_p = |x|_p\,|\pi^{-r}|_p = 1$).

לכן $x = \varepsilon\pi^r$. אם $x = \varepsilon'\pi^{r'}$ כנ"ל אז

$$\begin{aligned} |x|_p &= |\pi|_p^{r'} \\ &= p^{-\frac{r'}{e}} \end{aligned}$$

ולכן $r' = r$ ואז גם $\varepsilon = \varepsilon'$. (קיבלנו בפרט $r = e\nu_p(x)$)

2. $1 > |\pi|_p = p^{-\frac{1}{e}}$ ולכן $\pi \in \mathcal{P}_F$ ולכן $\mathcal{O}_F\pi \subseteq \mathcal{P}_F$. להפך, אם $x \in \mathcal{P}_F$ אז $x = \varepsilon\pi^r$ ו $1 > |x| = p^{-\frac{r}{e}}$. לכן $r \geq 1$ ואז $x = \left(\varepsilon\pi^{r-1}\right)\pi \in \mathcal{O}_F\pi$.

3. יהי $\mathcal{O}_F \supsetneq I \neq 0$ אידיאל. כיוון ש$\mathcal{P}_F$ הוא האידיאל המקסימלי היחיד של $\mathcal{O}_F$, מתקיים $I \subseteq \mathcal{P}_F$ ולכן כל $x \in I \neq 0$ הוא מהצורה $x = \varepsilon\pi^r$ כאשר $r \geq 1$. נניח כי π^l הוא החזקה הראשונה השייכת לI. מתקיים כמובן, $\mathcal{P}_F^l = \mathcal{O}_F\pi^l \subseteq I$.
להפך, אם $I \ni x = \varepsilon\pi^r \neq 0$ אז גם $\pi^r \in I$ ולכן $r \geq l$ ואז

$$x = \left(\varepsilon\pi^{r-l}\right)\pi^l \in \mathcal{O}_F\pi^l = \mathcal{P}_F^l$$

בנוסף $\pi^l \in \mathcal{P}_F^l \setminus \mathcal{P}_F^{l+1}$.

4. $|\pi|_p = \pi^{-\frac{1}{e}}$, $|\pi^e|_p = p^{-1} = |p|_p$.
ולכן יש ε הפיך ($|\varepsilon|_p = 1$) כך ש$p = \varepsilon\pi^e$ ואז

$$p\mathcal{O}_F = \mathcal{O}_F\pi^e = \mathcal{P}_F^e$$

■

F הוא שדה המנות של $\mathcal{P}_F$:

$$0 \neq x = \varepsilon \cdot \pi^r$$

$\mathcal{P}_F$ הוא גם האידיאל הראשוני השונה מאפס של $\mathcal{O}_F$: אידיאל אחר הוא מהצורה $\mathcal{P}_F^l$ כאשר $l \geq 2$ ואז $\pi \cdot \pi^{l-1} \in \mathcal{P}_F^l$, אבל $\pi, \pi^{l-1} \notin \mathcal{P}_F^l$.
עד כדי כפל באיבר הפיך, π הוא האיבר האי־פריק היחיד ב$\mathcal{O}_F$.

משפט 3.15 באותם סימונים כמו קודם

$$[\mathcal{O}_F/\mathcal{P}_F : \mathbb{F}_p] = f$$

(תזכורת: $ef = n = [F:\mathbb{Q}_p]$, $\nu_p(F^*) = \frac{1}{e}\mathbb{Z}$)

הוכחה: נסמן $t = [\mathcal{O}_F/\mathcal{P}_F : \mathbb{F}_p]$. אז ראינו קודם כי $t \leq n$.
יהי $\{\varepsilon_i + \mathcal{P}_F\}_{i=1}^t$ בסיס ל$\mathcal{O}_F/\mathcal{P}_F$ מעל $\mathbb{F}_p$. (כאשר $|\varepsilon_i|_p = 1$)
נראה כי הקבוצה $\left\{\varepsilon_i\pi^j \mid 1 \leq i \leq t, 0 \leq j \leq e-1\right\}$ היא בסיס לF מעל $\mathbb{Q}_p$. מכאן ינבע כי

$$n = [F:\mathbb{Q}_p] = te$$

ומכיוון ש$n = ef$ נקבל $t = f$.
אי־תלות: נניח

$$\sum_{i=1}^{t}\sum_{j=0}^{l-1} c_{ij}\varepsilon_i\pi^j = 0$$

כאשר $c_{ij} \in \mathbb{Q}_p$ לא כולם אפסים. כמו קודם, ע"י הכפלה במכנה משותף (חזקה של p), אפשר להניח כי $c_{ij} \in \mathbb{Z}_p$. מתקיים מודולו $\mathcal{P}_F$:

$$\sum_{i=1}^{t} (c_{i0} + \mathcal{P}_F)(\varepsilon_i + \mathcal{P}_F) = \mathcal{P}_F$$

נסיק כי $c_{i0} \in \mathcal{P}_F$ לכל i ולכן $|c_{i0}|_p < 1$ לכל i.
כלומר, $c_{i0} \in p\mathbb{Z}_p$ לכל i. נכתוב

$$\begin{aligned} c_{i0} &= c'_{i0} \cdot p \\ &= \varepsilon_0 c'_{i0} \cdot \pi^e \end{aligned}$$

כאשר $c'_{i0} \in \mathbb{Z}_p$, $p = \varepsilon_0 \pi^e$. נקבל

$$\begin{aligned} \sum_{i=1}^{t} c_{i0}\varepsilon_i + \sum_{j=1}^{l-1}\sum_{i=1}^{t} c_{ij}\varepsilon_i \pi^j &= 0 \\ \varepsilon_0 \sum_{i=1}^{t} c'_{i0}\varepsilon_i \pi^e + \sum_{j=1}^{l-1}\sum_{i=1}^{t} c_{ij}\varepsilon_i \pi^j &= 0 \end{aligned}$$

נחלק בπ ונקבל

$$\varepsilon_0 \sum_{i=1}^{t} c'_{i0}\varepsilon_i \pi^{e-1} + \sum_{j=1}^{l-1}\sum_{i=1}^{t} c_{ij}\varepsilon_i \pi^{j-1} = 0$$

מודולו $\mathcal{P}_F$ נסיק כמו קודם כי $c_{i1} \in p\mathbb{Z}_p$ לכל i וכו'.
נסיק כי $c_{ij} \in p\mathbb{Z}_p$ לכל i, j. נחלק בp את התלות המקורית.

$$\sum_{i=1}^{t}\sum_{j=0}^{l-1} \frac{c_{ij}}{p}\varepsilon_i \pi^j = 0$$

ושוב נסיק כי $\frac{c_{ij}}{p} \in p\mathbb{Z}_p$. כלומר $c_{ij} \in p^2\mathbb{Z}_p$ לכל i, j וכו'. נקבל כי לכל l טבעי מתקיים $c_{ij} \in p^l\mathbb{Z}_p$ ולכן

$$|c_{ij}|_p \leq p^{-l} \underset{l\to\infty}{\to} 0$$

נסיק לכן כי $c_{ij} = 0$ לכל i, j.
פרישה: יהי $0 \neq x = \varepsilon\pi^r$ ($|\varepsilon|_p = 1$, r שלם). אפשר להניח כי $0 \leq r \leq e-1$ כי נחלק עם שארית:

$$r = ae + l$$

כאשר $0 \leq l \leq e-1$

$$\begin{aligned} x &= \varepsilon (\pi^e)^a \pi^l \\ &= \varepsilon \left(\varepsilon_0^{-1} p\right)^a \pi^l \\ &= \underbrace{p^a}_{\in \mathbb{Q}_p} \varepsilon' \pi^l \end{aligned}$$

כאשר $|\varepsilon'|_p = 1$.
נכתוב

$$\varepsilon + \mathcal{P}_F = \sum_{i=1}^{t} (c_i + \mathcal{P}_F)(\varepsilon_i + \mathcal{P}_F)$$

כאשר $c_i \in \mathbb{Z}_p$.

$$\varepsilon = \sum_{i=1}^{t} c_i \varepsilon_i + \alpha_1$$

כאשר $\alpha_1 \in \mathcal{P}_F = \mathcal{O}_F \pi$.
אם $\alpha_1 = 0$, אז סיימנו. אחרת נכתוב $\alpha_1 = \mu_1' \pi^l$, $|\mu_1'|_p = 1$, $l \geq 1$. כמו קודם, לאחר חלוקה של l עם שארית בe, אפשר לכתוב

$$\alpha_1 = p^{r_1} \mu_1 \pi^{l_1}$$

כאשר $|\mu_1|_p = 1$, $0 \leq l_1 \leq e-1$, $r_1 \geq 0$, $r_1 + l_1 \geq 1$.
כמו קודם, נציג

$$\mu_1 = \sum_{i=1}^{t} c_i' \varepsilon_i + \alpha_2$$

$\alpha_2 \in \mathcal{P}_F$

$$\alpha_1 = \sum_{i=1}^{t} p^{r_1} c_i' \varepsilon_i \pi^{l_1} + p^{r_1} \pi^{l_1} \alpha_2$$

וכך נמשיך (נכתוב $\alpha_2 = p^{r_2} \mu_2 \pi^{l_2}$ כמו קודם $0 \leq l_2 \leq e-1$, $r_2 \geq 0$, $r_2 + l_2 \geq 1$, $|\mu_2|_p = 1$ ונמשיך)
נקבל כי לכל s טבעי, קיים ייצוג

$$\varepsilon = \sum_{k=0}^{s} \sum_{i=1}^{t} \sum_{j=0}^{e-1} a_{ijk} p^k \varepsilon_i \pi^j + \alpha_{s+1}$$

כאשר $\alpha_{s+1} \in \mathcal{P}_F^{s+1} = \mathcal{O}_F \pi^{s+1}$ ו$a_{ijk} \in \mathbb{Z}_p$.
כיוון ש $|\alpha_{s+1}|_p \leq p^{-\frac{s+1}{e}} \underset{s\to\infty}{\to} 0$, נקבל כי

$$\begin{aligned}
\varepsilon &= \sum_{k=0}^{\infty} \sum_{i=1}^{t} \sum_{j=0}^{e-1} a_{ijk} p^k \varepsilon_i \pi^j \\
&= \sum_{i=1}^{t} \sum_{j=0}^{e-1} \underbrace{\left(\sum_{k=0}^{\infty} a_{ijk} p^k \right)}_{b_{ij} \in \mathbb{Z}_p} \varepsilon_i \pi^j \\
&= \sum_{i=1}^{t} \sum_{j=0}^{e-1} b_{ij} \varepsilon_i \pi^j
\end{aligned}$$

יהי $0 \le l \le e-1$

$$\varepsilon\pi^{l} = \sum_{i=1}^{t}\sum_{j=0}^{e-1} b_{ij}\pi^{j+l}$$

נתבונן במחוברים כך ש- $e \le j+l \le 2e-2$. נחזור על מה שהוכחנו בעבור $\varepsilon_i\pi^{j+l}$:
חלוקה עם שארית: $j+l = e+j'$ כאשר $0 \le j' \le e-2$.

$$\begin{aligned}\varepsilon_i \cdot \pi^{j+l} &= \varepsilon_i \cdot \pi^{e} \cdot \pi^{j'} \\ &= \underbrace{\frac{\varepsilon_i}{\varepsilon_0}}_{\varepsilon_i'} \cdot p \cdot \pi^{j'} \\ &= p \cdot \varepsilon_i' \cdot \pi^{j'}\end{aligned}$$

נציג

$$\begin{aligned}\varepsilon_i' &= \sum_{k=1}^{t}\sum_{s=0}^{e-1} b'_{ks}\varepsilon_k\pi^{s} \\ \varepsilon_i'\pi^{j'} &= \sum_{k=1}^{t}\sum_{s=0}^{e-1} b'_{ks}\varepsilon_k\pi^{s+j'}\end{aligned}$$

נתבונן שוב במחוברים כך ש- $e \le s+j' \le 2e-3$. חלוקה עם שארית:

$$s+j' = e+j''$$

כאשר $0 \le j'' \le e-3$ וכו'. התהליך יסתיים ונקבל

$$\varepsilon\pi^{l} = \sum_{i=0}^{t}\sum_{j=0}^{e-1} a_{ij}\varepsilon_i\pi^{j}$$

כאשר $a_{ij} \in \mathbb{Z}_p$. כלומר, הקבוצה פורשת, כנדרש. ■

e נקרא הסיעוף של F מעל $\mathbb{Q}_p$. (ramification)

הגדרה 3.16 נאמר כי ההרחבה $F/\mathbb{Q}_p$ אינה מסועפת (unramifieid) אם $e=1$.

במקרה כזה $p\mathcal{O}_F = \mathcal{P}_F$ (אפשר לבחור $\pi = p$),
$\mathcal{O}_F/\mathcal{P}_F \cong \mathbb{F}_{p^n}$, $\nu_p(F^*) = \mathbb{Z}$.

הגדרה 3.17 נאמר כי $F/\mathbb{Q}_p$ מסועפת לחלוטין (totaly ramified) אם $e=n$.

במקרה כזה

$$\begin{aligned}p\mathcal{O}_F &= \mathcal{P}_F^{n} \\ \nu_p(F^*) &= \frac{1}{n}\mathbb{Z} \\ \mathcal{O}_F/\mathcal{P}_F &\cong \mathbb{F}_p\end{aligned}$$

משפט 3.18 תהי $F/\mathbb{Q}_p$ הרחבה מסועפת לחלוטין ממעלה e. יהי π היוצר של האידיאל $\mathcal{P}_F = \mathcal{O}_F\pi$. אז $F = \mathbb{Q}_p(\pi)$ והפולינום האי־פריק $f(x)$ של π מעל $\mathbb{Q}_p$ הוא פולינום איזנשטיין מעל $\mathbb{Z}_p$, כלומר

$$f(x) = x^e + a_{l-1}x^{e-1} + \ldots + a_1x + a_0 \quad \in \quad \mathbb{Z}_p[x]$$

ו־$a_i \in p\mathbb{Z}_p$ לכל $0 \le i \le e-1$ וכן $a_0 \notin p^2\mathbb{Z}_p$.

להפך, כל שורש פולינום איזנשטיין ממעלה e מעל $\mathbb{Z}_p$ יוצר הרחבה מסועפת לחלוטין ממעלה e מעל $\mathbb{Q}_p$.

הוכחה: $\Longleftarrow$ אנו יודעים כי $\left\{\pi^j\right\}_{j=0}^{e-1}$ הוא בסיס ל־F מעל $\mathbb{Q}_p$. יהי $f(x) \in \mathbb{Q}_p[x]$ הפולינום האי־פריק של π מעל $\mathbb{Q}_p$. (מתוקן, ממעלה e)

כיוון ש־$\mathcal{O}_F$ הוא הסגור השלם של $\mathbb{Z}_p$ ב־F, π הוא שלם מעל $\mathbb{Z}_p$ (כי $\pi \in \mathcal{P}_F \subseteq \mathcal{O}_F$) וראינו $f(x) \in \mathbb{Z}_p[x]$.

$$\begin{aligned} p^{-1} &= |p|_p \\ &= |\pi^e|_p \\ &= \left|N_{F/\mathbb{Q}}(\pi)\right|_p \\ &= |a_0|_p \end{aligned}$$

לכן $a_0 \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$. שאר המקדמים a_i שייכים ל־$p\mathbb{Z}_p$ כי הם פולינומים סימטריים בצמודי גלואה של π שכולם בעלי ערך מוחלט $1 >$ ולכן גם $|a_i|_p < 1$ לכל i.

$\Longrightarrow$: יהי $f(x) \in \mathbb{Z}_p[x]$ פולינום איזנשטיין כנ"ל (מתוקן ממעלה e). יהי $\alpha \in \overline{\mathbb{Q}_p}$ שורש של $f(x)$. נסמן $F = \mathbb{Q}_p[\alpha]$. מתקיים $[F:\mathbb{Q}_p] = e$.

$$\begin{aligned} |\alpha|_p &= \left|N_{F/\mathbb{Q}_p}(\alpha)\right|_p^{\frac{1}{e}} \\ &= |a_0|_p^{\frac{1}{e}} \\ &= p^{-\frac{1}{e}} \end{aligned}$$

נסמן $\mathcal{P}_F = \mathcal{O}_F \cdot \pi$ וכן נסמן $\nu_p(F^*) = \frac{1}{e'}\mathbb{Z}$ אנו יודעים כי $e' \mid e$ (כי מימד ההרחבה הוא e ו־e' מחלק אותו).

מתקיים $\nu_p(\alpha) = \frac{1}{e} \in \frac{1}{e'}\mathbb{Z}$ (כי $|\alpha|_p = p^{-\frac{1}{e}}$) ולכן $e \mid e'$ (כי $\frac{1}{e} = \frac{l}{e'}$).

בסה"כ $e = e'$ ולכן $F/\mathbb{Q}_p$ הרחבה מסועפת לחלוטין ולכן יש $\varepsilon \in \mathcal{O}_F^*$ כך ש־$\alpha = \varepsilon\pi$ ולכן $\mathcal{P}_F = \mathcal{O}_F \cdot \alpha$. ■

נניח כי $\mathbb{Q}_p \subseteq F \subseteq K \subseteq \overline{\mathbb{Q}_p}$ שדות הרחבה ממעלה סופית. נסמן $[F:\mathbb{Q}_p] = n$, $[K:F] = m$, $[K:\mathbb{Q}_p] = m \cdot n$

נסמן גם $n = e_F \cdot f_F$ ו־$n \cdot m = e_K \cdot f_K$

מתקיים

$$\frac{1}{e_F}\mathbb{Z} = \nu_p(F^*) \quad \subseteq \quad \nu_p(K^*) = \frac{1}{e_K}\mathbb{Z}$$

ולכן

$$\frac{1}{e_F} \quad \in \quad \frac{1}{e_F}\mathbb{Z} \subseteq \frac{1}{e_K}\mathbb{Z}$$

ומכאן $e_K \mid e_F$. נסמן $e_{K/F} = \frac{e_K}{e_F}$. מתקיים $\mathcal{O}_F \subseteq \mathcal{O}_K$ ברור כי

$$\mathcal{P}_K \cap \mathcal{O}_F = \mathcal{P}_F$$

ולכן יש לנו שיכון של שדות מעל $\mathbb{F}_p$:

$$\mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p \hookrightarrow \begin{array}{c}\mathcal{O}_F/\mathcal{P}_F\\ \cong\\ \mathbb{F}_{p^{f_F}}\end{array} \underset{a+\mathcal{P}_F \mapsto a+\mathcal{P}_K}{\hookrightarrow} \begin{array}{c}\mathcal{O}_K/\mathcal{P}_K\\ \cong\\ \mathbb{F}_{p^{f_K}}\end{array}$$

לכן $f_F \mid f_K$.
נסמן $f_{K/F} = \frac{f_K}{f_F}$
נסמן

$$\begin{aligned}\mathcal{P}_F &= \mathcal{O}_F\pi_F\\ \mathcal{P}_K &= \mathcal{O}_K\pi_K\end{aligned}$$

נתבונן באידיאל $\mathcal{P}_F \cdot \mathcal{O}_K = \mathcal{O}_K\pi_F$ ולכן יש r טבעי כך ש

$$\begin{aligned}\mathcal{O}_K\pi_F &= \mathcal{O}_K \cdot \pi_K^r\\ \pi_F &= \varepsilon \cdot \pi_K^r\end{aligned}$$

כאשר $\varepsilon \in \mathcal{O}_K^*$. נקבל

$$\begin{aligned}-\frac{1}{e_F} &= \nu_p(\pi_F)\\ &= r \cdot \nu_p(\pi_K)\\ &= -\frac{r}{e_K}\end{aligned}$$

לכן $r = \frac{e_K}{e_F} = e_{K/F}$ ולכן $\mathcal{P}_F\mathcal{O}_K = \mathcal{P}_K^{e_{K/F}}$.
נסכם במשפט:

משפט 3.19 נניח $\mathbb{Q}_p \subseteq F \subseteq K \subseteq \overline{\mathbb{Q}_p}$. יש שיכון של שדות סופיים של $\mathbb{F}_p$

$$\mathcal{O}_F/\mathcal{P}_F \hookrightarrow \mathcal{O}_K/\mathcal{P}_K$$

נסמן $f_{K/F} = [\mathcal{O}_K/\mathcal{P}_K : \mathcal{O}_F/\mathcal{P}_F]$.
יהי $e_{K/F}$ המספר הטבעי המוגדר על ידי

$$\mathcal{P}_F\mathcal{O}_K = \mathcal{P}_K^{e_{K/F}}$$

אז $[K:F] = f_{K/F} \cdot e_{K/F}$
ואם $\mathbb{Q}_p \subseteq F \subseteq K \subseteq L \subseteq \overline{\mathbb{Q}_p}$ אז

$$\begin{aligned}e_{L/F} &= e_{L/K} \cdot e_{K/F}\\ f_{L/F} &= f_{L/K} \cdot f_{K/F}\end{aligned}$$

ובפרט

$$\begin{aligned} e_{F/\mathbb{Q}_p} &= e_F \\ f_{F/\mathbb{Q}_p} &= f_F \end{aligned}$$

הוכחה: את הרוב כבר ראינו. השלמות קטנות:

$$\begin{aligned} e_K \cdot f_K &= [K : \mathbb{Q}_p] \\ &= n \cdot m \\ &= [F : \mathbb{Q}_p] \cdot m \\ &= e_F \cdot f_F \cdot m \end{aligned}$$

ולכן

$$\begin{aligned} m &= \frac{e_K}{e_F} \cdot \frac{f_K}{f_F} \\ &= e_{K/F} \cdot f_{K/F} \end{aligned}$$

מתקיים

$$\begin{aligned} e_{L/F} &= \frac{e_L}{e_F} \\ &= \frac{e_L}{e_K} \cdot \frac{e_K}{e_F} \\ &= e_{L/K} \cdot e_{K/F} \end{aligned}$$

וכנ"ל ל-$f_{L/F}$. ■

הגדרה 3.20 אם $e_{K/F} = 1$, נאמר כי ההרחבה לא מסועפת. אם $e_{K/F} = [K : F]$ נאמר כי ההרחבה מסועפת לחלוטין.

3.4 הלמה של הנזל

יהי $F/\mathbb{Q}_p$ שדה הרחבה סופית.
נסמן ל-$f(x) \in \mathcal{O}_F[x]$ את $\overline{f}(x) \in (\mathcal{O}_F/\mathcal{P}_F)[x]$ - הפולינום המתקבל מרדוקציית מרדוקציית מקדמי $f(x)$ מודולו $\mathcal{P}_F$.

משפט 3.21 (הלמה של הנזל): יהי $f(x) \in \mathcal{O}_F[x]$ ונניח $\overline{f}(x) \neq 0$. נניח כי

$$\overline{f}(x) = a(x) \cdot b(x)$$

כאשר $a(x), b(x) \in (\mathcal{O}_F/\mathcal{P}_F)[x]$ פולינומים זרים.
אז קיימים $g(x), h(x) \in \mathcal{O}_F[x]$ כך ש-$\deg g(x) = \deg a(x)$ ו-$\deg h(x) = \deg b(x)$ ו $a(x) = \overline{g}(x)$, $b(x) = \overline{h}(x)$ וכן

$$f(x) = g(x) \cdot h(x)$$

הוכחה: נסמן $\deg f(x)=d$, $\deg a(x)=m$, $\deg b(x)\leq d-m$.
נבחר $g_0(x),h_0(x)\in\mathcal{O}_F[x]$ כך ש$\deg g_0(x)=m$, $\deg h_0(x)\leq d-m$
$\overline{g_0}(x)=a(x),\overline{h_0}(x)=b(x)$
מכאן $f(x)-g_0(x)h_0(x)\in\mathcal{P}_F[x]$. אם $f(x)=g_0(x)h_0(x)$, סיימנו.
אחרת, נניח $f(x)-g_0(x)h_0(x)\neq 0$ מהנתון, קיימים פולינומים $\alpha(x),\beta(x)\in\mathcal{O}_F[x]$
כך ש

$$\overline{\alpha}(x)\cdot\overline{g_0}(x)+\overline{\beta}(x)\cdot\overline{h_0}(x) = 1$$

כלומר

$$g_0(x)\alpha(x)+h_0(x)\beta(x)-1 \in \mathcal{P}_F[x]$$

יהי δ מקדם בעל ערך מוחלט מקסימלי מבין כל המקדמי הפולינומים

$$\begin{aligned}f(x)-g_0(x)h_0(x) &\in \mathcal{P}_F[x]\\ g_0(x)\alpha(x)+h_0(x)\beta(x)-1 &\in \mathcal{P}_F[x]\end{aligned}$$

כמובן, $|\delta|_p<1$ (כי $\delta\in\mathcal{P}_F$)
מטרתנו היא למצוא פולינומים $r_i(x),s_i(x)$ כך ש

$$\begin{aligned}g(x) &= g_0(x)+r_1(x)\delta+r_2(x)\delta^2+\ldots\\ h(x) &= h_0(x)+s_1(x)\delta+s_2(x)\delta^2+\ldots\end{aligned}$$

כך ש$\deg r_i(x)\leq m-1$ ו$\deg s_j(x)\leq d-m$
ביתר פירוט: מטרתנו למצוא, באינדוקציה לכל n טבעי, פולינומים

$$\begin{aligned}r_1(x),\ldots,r_{n-1}(x) &\in \mathcal{O}_F[x]\\ s_1(x),\ldots,s_{n-1}(x) &\in \mathcal{O}_F[x]\end{aligned}$$

כך ש

$$\begin{aligned}\deg r_i(x) &\leq m-1\\ \deg s_j(x) &\leq d-m\end{aligned}$$

וכשנגדיר

$$\begin{aligned}g_{n-1}(x) &= g_0(x)+r_1(x)\cdot\delta+\ldots+r_{n-1}(x)\cdot\delta^{n-1}\\ h_{n-1}(x) &= h_0(x)+s_1(x)\cdot\delta+\ldots+s_{n-1}(x)\cdot\delta^{n-1}\end{aligned}$$

מתקיים

$$f(x) \equiv g_{n-1}(x)h_{n-1}(x)\,(\bmod\ \mathcal{O}_F\delta^n)$$

ל$n=1$: נובע מהגדרת δ.

נניח כי מצאנו כנ"ל עד $n-1$. נראה איך למצוא $r_n(x), s_n(x)$. רוצים ש$r_n(x), s_n(x)$ יהיו כך שכשנגדיר

$$\begin{aligned}
g_n(x) &= g_{n-1}(x) + r_n(x)\delta^n \\
h_n(x) &= h_{n-1}(x) + s_n(x)\delta^n
\end{aligned}$$

יתקיים

$$\begin{aligned}
g_n(x)\cdot h_n(x) &= g_{n-1}(x)\cdot h_{n-1}(x) + \delta^n\left(g_{n-1}(x)\cdot s_n(x) + h_{n-1}(x)\cdot r_n(x)\right) + \delta^{2n}(\dots) \\
&\equiv g_{n-1}(x)\cdot h_{n-1}(x) + \delta^n\left(g_{n-1}(x)\cdot s_n(x) + h_{n-1}(x)\cdot r_n(x)\right) \pmod{\delta^{n+1}}
\end{aligned}$$

מתקיים

$$\begin{aligned}
f(x) - g_n(x)h_n(x) \equiv\ & f(x) - g_{n-1}(x)\cdot h_{n-1}(x) \\
& -\delta^n\left(g_{n-1}(x)\cdot s_n(x) + h_{n-1}(x)\cdot r_n(x)\right) \pmod{\delta^{n+1}}
\end{aligned}$$

רוצים לכן

$$f(x) - g_{n-1}(x)\cdot h_{n-1}(x) \equiv \delta^n\left(g_{n-1}(x)\cdot s_n(x) + h_{n-1}(x)\cdot r_n(x)\right) \pmod{\delta^{n+1}}$$

מהנחת האינדוקציה, $f(x) - g_{n-1}(x)\cdot h_{n-1}(x) \in \mathcal{O}_F\delta^n$ ולכן הקונגרואנציה הנ"ל מתקיימת $\iff$

$$\begin{aligned}
\delta^{-n}\left(f(x) - g_{n-1}(x)\cdot h_{n-1}(x)\right) &\equiv g_{n-1}(x)\cdot s_n(x) + h_{n-1}(x)\cdot r_n(x) \pmod{\delta} \\
&\equiv g_0(x)\cdot s_n(x) + h_0(x)\cdot r_n(x) \pmod{\delta}
\end{aligned}$$

כי

$$\begin{aligned}
g_0(x) &\equiv g_{n-1}(x) \pmod{\delta} \\
h_0(x) &\equiv h_{n-1}(x) \pmod{\delta}
\end{aligned}$$

נסמן

$$f_n(x) = \delta^{-n}\left(f(x) - g_{n-1}(x)\cdot h_{n-1}(x)\right)$$

כיוון ש

$$g_0(x)\alpha(x) + h_0(x)\beta(x) \equiv 1 \pmod{\delta}$$

נכפיל ב$f_n(x)$ ונקבל

$$g_0(x)\alpha(x)f_n(x) + h_0(x)\beta(x)f_n(x) \equiv f_n(x) \pmod{\delta}$$

נחלק עם שארית את $\beta(x)\cdot f_n(x)$ ב$g_0(x)$ ונקבל

$$\beta(x)f_n(x) = q(x)g_0(x) + r_n(x)$$

נזכר כי $g_0(x)$ הוא פולינום ממעלה m ב$\mathcal{O}_F[x]$ שהמקדם העליון שלו הוא ב$\mathcal{O}_F^*$ (כי בחרנו $\deg g_0(x) = \deg a(x)$), ולכן החלוקה בשארית מתבצעת ב$\mathcal{O}_F[x]$ ו$\deg r_n(x) < m$.

$$f_n(x) \equiv g_0(x)\left(\alpha(x)f_n(x) + h_0(x)q(x)\right) + h_0(x)r_n(x) \pmod{\delta}$$

נשים לב

$$\begin{aligned}\deg g_{m-1}(x) &= m\\ \deg h_{m-1}(x) &\leq d-m\end{aligned}$$

לכן $h_0(x)\,r_n(x)$ מדרגה $\geq d = d-m+m$.

נזרוק מ$\alpha(x)\,f_n(x)+h_0(x)\,q(x)$ את כל המקדמים המתחלקים בδ ונסמן את הפולינום הנותר $s_n(x)$.

$$f_n(x) \equiv g_0(x)\,s_n(x)+h_0(x)\,r_n(x) \pmod{\delta}$$

נשווה דרגות מודולו $\delta\mathcal{O}_F$ של שני האגפים.

דרגת $f_n(x)$ מודולו δ היא $\geq d$.

מאחר והמקדם העליון של$g_0(x)$ הפיך, מתקיים כי $\deg g_0(x)+\deg s_n(x) = \deg(g_0(x)\cdot s_n(x))$ גם כפולינומים מודולו δ. לכן דרגת $g_0(x)\,s_n(x)$ מודולו δ שווה ל$m+\deg(s_n(x)+\delta\mathcal{O}_F[x])$.

דרגת $h_0(x)\,r_n(x)$ מודולו $\delta \geq d$.

לכן נקבל

$$\deg(s_n(x)+\delta\mathcal{O}_F[x]) \leq d-m$$

ומתקיים $\deg(s_n(x)) = \deg(s_n(x)+\delta\mathcal{O}_F[x])$ מהגדרת $s_n(x)$.

נגדיר

$$\begin{aligned}g_n(x) &= g_{n-1}(x)+r_n(x)\cdot\delta^n\\ h_n(x) &= h_{n-1}(x)+s_n(x)\cdot\delta^n\end{aligned}$$

מתקיים

$$\begin{aligned}g_n(x)\cdot h_n(x) &\equiv g_{n-1}(x)\cdot h_{n-1}(x)+\delta^n\left(g_{n-1}(x)\cdot s_n(x)+h_{n-1}(x)\cdot r_n(x)\right) \pmod{\delta^{n+1}}\\ &\equiv g_{n-1}(x)\cdot h_{n-1}(x)+\delta^n\left(g_0(x)\cdot s_n(x)+h_0(x)\cdot r_n(x)\right) \pmod{\delta^{n+1}}\\ &\equiv g_{n-1}(x)\cdot h_{n-1}(x)+\delta^n f_n(x) \pmod{\delta^{n+1}}\\ &\equiv g_{n-1}(x)\cdot h_{n-1}(x)+\delta^n\left(\delta^{-n}\left(f(x)-g_{n-1}(x)\cdot h_{n-1}(x)\right)\right) \pmod{\delta^{n+1}}\\ &\equiv f(x) \pmod{\delta^{n+1}}\end{aligned}$$

כיוון ש

$$\begin{aligned}\deg s_j(x) &\leq d-m\\ \deg r_i(x) &\leq m-1\end{aligned}$$

הטורים

$$\begin{aligned}g(x) &= g_0(x)+\sum_{n=1}^{\infty}\delta^n r_n(x)\\ h(x) &= h_0(x)+\sum_{n=1}^{\infty}\delta^n s_n(x)\end{aligned}$$

מתכנסים לאיברים ב$\mathcal{O}_F[x]$.

$$\deg g(x) = \deg g_0(x) = m$$

לבסוף מתקיים

$$\begin{aligned} f(x) &= g(x) \cdot h(x) \\ \overline{g}(x) &= \overline{g_0}(x) = a(x) \\ \overline{h}(x) &= \overline{h_0}(x) = b(x) \end{aligned}$$

■

משפט 3.22 $\mathbb{Q}_p$ מכיל את שורשי היחידה מסדר $p-1$.

הוכחה: ידוע,

$$x^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (x-i) \pmod{p\mathbb{Z}}$$

ולכן גם

$$x^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (x-i) \pmod{p\mathbb{Z}_p}$$

מתקיים

$$\begin{aligned} \mathcal{O}_{\mathbb{Q}_p} &= \mathbb{Z}_p \\ \mathcal{P}_{\mathbb{Q}_p} &= p\mathbb{Z}_p \end{aligned}$$

ולכן

$$\begin{aligned} f(x) &= \frac{x^{p-1}-1}{x-1} \\ &= 1 + x + x^2 + \ldots + x^{p-2} \in \mathbb{Z}_p[x] \end{aligned}$$

מתקיים

$$\overline{f}(x) = (x-2)\, b(x) \pmod{p\mathbb{Z}_p}$$

כאשר

$$b(x) = \prod_{i=3}^{p-1} (x-i)$$

$x-2$ ו$b(x)$ פולינומים זרים, ולכן מהלמה של הנזל ישר פירוק

$$f(x) = (ux - v)\, h(x)$$

כך ש

$$\begin{aligned} u &\equiv 1 \left(\mod p\mathbb{Z}_p \right) \\ v &\equiv 2 \left(\mod p\mathbb{Z}_p \right) \end{aligned}$$

ו-$\overline{h}(x) = b(x)$.
כיוון ש-$u \in 1 + p\mathbb{Z}_p \subseteq \mathbb{Z}_p^*$ אפשר להניח כי $u = 1$.

$$(ux - v)\, h(x) = \left(x - \underbrace{\frac{v}{u}}_{\zeta_2} \right) (uh(x))$$

ומתקיים

$$\begin{aligned} \zeta_2^{p-1} &= 1 \\ \zeta_2 &\equiv 1 \left(\mod p\mathbb{Z}_p \right) \end{aligned}$$

וכך נמשיך: נתבונן בפולינום

$$\tilde{f}(x) = \frac{f(x)}{x - \zeta_2} \in \mathbb{Z}_p[x]$$

$$\tilde{f}(x) \equiv (x-3) \prod_{i=4}^{p-1} (x - i) \left(\mod p\mathbb{Z}_p \right)$$

כך נמצא $\zeta_3 \in \mathbb{Z}_p$ כך ש-$\zeta_3^{p-1} = 1$ ו-$\zeta_3 \equiv 3 \left(\mod p\mathbb{Z}_p \right)$.
וכו'. לכל $1 \leq i \leq p-1$ יש ζ_i (יחיד) כך ש-$\zeta_i^{p-1} = 1$ ו-$\zeta_i \equiv i \left(\mod p\mathbb{Z}_p \right)$.

$$x^{p-1} - 1 = \prod_{i=1}^{p-1} (x - \zeta_i)$$

■

נכליל: יהי $F/\mathbb{Q}_p$ שדה הרחבה סופית.

$$\mathcal{O}_F / \mathcal{P}_F \cong \mathbb{F}_{p^f}$$

כאשר $[F : \mathbb{Q}_p] = e \cdot f$. נסמן $q = p^f$. ידוע

$$x^{q-1} - 1 = \prod_{a \in F_q^*} (x - a)$$

נחזור על ההוכחה הנ"ל ונקבל כי $x^{q-1} - 1$ מתפצל ב-$F[x]$ (ב-$\mathcal{O}_F[x]$)

$$x^{q-1} - 1 = \prod_{a \in F_q^*} (x - \zeta_a)$$

כאשר

$$\begin{aligned} \zeta_a^{q-1} &= 1 \\ \zeta_a + \mathcal{P}_F &= a \in \mathcal{O}_F/\mathcal{P}_F = \mathbb{F}_q \end{aligned}$$

לכן F מכיל את חבורת כל שורשי היחידה מסדר $q-1 = p^f - 1$. ($f = f_{F/Q_p}$) נסמנה μ_{q-1}.

טענה 3.23 $\mathcal{O}_F^* = \mu_{q-1} \cdot (1+\mathcal{P}_F)$ וזאת מכפלה ישרה של חבורות.

הוכחה: $1+\mathcal{P}_F$ חבורה כפלית

$$(1+x)\cdot(1+y) = 1 + \underbrace{(x+y+xy)}_{\in \mathcal{P}_F} \in 1+\mathcal{P}_F$$

בנוסף

$$\begin{aligned} \frac{1}{1+x} &= \frac{1+x-x}{1+x} \\ &= 1 - \underbrace{\frac{x}{1+x}}_{\in \mathcal{P}_F} \end{aligned}$$

כי

$$\begin{aligned} \left|\frac{x}{1+x}\right|_p &= \frac{|x|_p}{|1+x|_p} \\ &= |x|_p \\ &< 1 \end{aligned}$$

כמובן, ההכלה $\mathcal{O}_F^* \supseteq \mu_{q-1}\cdot(1+\mathcal{P}_F)$ נכונה.
להפך, נניח $a \in \mathcal{O}_F^*$. אז

$$(0 \neq)\, a + \mathcal{P}_F \in \mathcal{O}_F/\mathcal{P}_F \cong \mathbb{F}_q$$

ולכן

$$\begin{aligned} (a+\mathcal{P}_F)^{q-1} &= a^{q-1} + \mathcal{P}_F \\ &= 1 + \mathcal{P}_F \end{aligned}$$

ולכן

$$a^{q-1} - 1 \equiv 0 \,(\mod \mathcal{P}_F)$$

ולכן a הוא שורש מודולו $\mathcal{P}_F$ של $x^{q-1}-1$. ממה שראינו קודם, יש $\omega_a \in \mathcal{O}_p^*$ יחיד כך ש

$$\begin{aligned} \omega_a^{q-1} &= 1 \\ \omega_a &\equiv a \,(\mod \mathcal{P}_F) \end{aligned}$$

אז

$$v = a-\omega_a \in \mathcal{P}_F$$

ומתקיים

$$\begin{aligned} a &= \omega_a + v \\ &= \omega_a\left(1+\frac{v}{\omega_a}\right) \\ &\in \mu_{q-1}\cdot(1+\mathcal{P}_F) \end{aligned}$$

נשים לב כי

$$\mu_{q-1}\cap(1+\mathcal{P}_F) = \{1\}$$

כי אם $\omega_a \in \mu_{q-1}\cap(1+\mathcal{P}_F)$ אז $\omega_a \equiv 1 \pmod{\mathcal{P}_F}$ ו-$\omega_a^{q-1}=1$ וראינו שיש רק איבר אחד כזה, ולכן $\omega_a = 1$. ■

משפט 3.24 $F^* = \langle\pi\rangle\cdot\mu_{q-1}\cdot(1+\mathcal{P}_F) \cong \mathbb{Z}\times\mu_{q-1}\times(1+\mathcal{P}_F)$ וזאת מכפלה ישרה. (כאשר כרגיל $\mathcal{P}_F = \mathcal{O}_F\pi$ ו-$\nu_p(\pi)=\frac{1}{e_F}$)

הוכחה: לכל $x \in F^*$ יש הצגה יחידה בצורה $x=\varepsilon\pi^r$ כאשר $r\in\mathbb{Z}$ ו-$\varepsilon\in\mathcal{O}_F^*$ ול-ε הצגה יחידה בצורה $\varepsilon=\zeta\cdot(1+v)$ כאשר $\zeta\in\mu_{q-1}$ ו-$v\in\mathcal{P}_F$. ■

את ההצגה הנ"ל נסמן כך

$$x = \pi^{e\nu_p(x)}\cdot\omega(x)\cdot\langle x\rangle$$

כאשר $\omega(x)\in\mu_{q-1}$ ו-$\langle x\rangle \in 1+\mathcal{P}_F$. $x\to\omega(x)$ הוא הומומורפיזם $F^*\to\mu_{q-1}\subseteq\overline{\mathbb{Q}}_p^*$.

3.4.1 הקרקטר של Teichmuller

משפט 3.25 יהי $x\in\mathcal{O}_F^*$ אז

$$\omega(x) = \lim_{n\to\infty} x^{q^n}$$

(כאשר $q=p^f$)

הוכחה: נראה ראשית כי $\left\{x^{q^n}\right\}_{n=0}^{\infty}$ היא סדרת קושי. נראה כי

$$x^{q^n}-x^{q^{n-1}} \underset{n\to\infty}{\longrightarrow} 0$$

ובכן

$$\begin{aligned} x^{q^n}-x^{q^{n-1}} &= x^{q^{n-1}}\left(x^{q^n-q^{n-1}}-1\right) \\ &= x^{q^{n-1}}\left(\left(x^{q-1}\right)^{q^{n-1}}-1\right) \end{aligned}$$

כיוון ש

$$\mathcal{O}_F/\mathcal{P}_F \cong \mathbb{F}_q$$

אז

$$x^{q-1} \equiv 1 \pmod{\mathcal{P}_F}$$

ולכן

$$x^{q-1} = 1+v$$

כאשר $v \in \mathcal{P}_F$.

$$(1+v)^{q^n-1}-1 = \sum_{i=1}^{q^n-1} \binom{q^{n-1}}{i} v^i$$

מתקיים

$$\binom{q^{n-1}}{i} = q^{n-1} \cdot \left(q^{n-1}-1\right) \cdot \frac{\left(q^{n-1}-2\right)}{2} \cdot \ldots \cdot \frac{\left(q^{n-1}-k\right)}{k} \cdot \ldots \cdot \frac{\left(q^{n-1}-(i-1)\right)}{i-1} \cdot \frac{1}{i}$$

(כזכור $q=p^f$)

נשים לב כי החזקות של p של המכנה ב$\frac{\left(q^{n-1}-k\right)}{k}$ מצטמצמות עם המונה ולכן ל$\binom{q^{n-1}}{i}$ חזקת p היא לפחות חזקת p של $\frac{q^{n-1}}{i}$.

נכתוב $i=lp^r$ כאשר $l,r \geq 0$ ‏$p \nmid l$. לכן

$$p^{f(n-1)-r} \mid \binom{q^{n-1}}{i}$$

ולכן

$$\left|\binom{q^{n-1}}{i}\right|_p \leq p^{-f(n-1)+r}$$

ולכן

$$\left|\binom{q^{n-1}}{i} v^i\right|_p \leq p^{-f(n-1)+r} \left|v\right|_p^i$$

מתקיים $v \in \mathcal{P}_F = \mathcal{O}_F\pi$ ולכן $\left|v\right|_p \leq \left|\pi\right|_p = p^{-\frac{1}{e}}$ כאשר $e = e_{F/\mathbb{Q}_p}$. לכן

$$\left|\binom{q^{n-1}}{i} v^i\right|_p \leq p^{-f(n-1)+r-\frac{lp^r}{e}}$$

נשים לב כי הסדרה $\left\{\frac{lp^r}{e}-r\right\}_{\substack{l\geq 1\\ r\geq 0}}$ חסומה מלרע: קיים x_0 כך ש

$$\frac{lp^r}{e}-r \geq \frac{p^r}{e}-r \geq x_0$$

לכל l ולכל r. לכן

$$\left|(1+v)^{q^{n-1}}-1\right|_p \leq \max_{i\geq1}\left|\binom{q^{n-1}}{i}v^i\right|_p \underset{n\to\infty}{\longrightarrow}0$$

ולכן מדובר בסדרת קושי. נסמן

$$a(x) = \lim_{n\to\infty}x^{q^n}$$

מתקיים

$$\begin{aligned} a(x)^{q-1} &= \lim_{n\to\infty}x^{q^n(q-1)} \\ &= \frac{\lim_{n\to\infty}x^{q^{n+1}}}{\lim_{n\to\infty}x^{q^n}} \\ &= \frac{a(x)}{a(x)} \\ &= 1 \end{aligned}$$

מתקיים

$$x^q \equiv x \pmod{\mathcal{P}_F}$$

ולכן לכל n

$$x^{q^n} \equiv x \pmod{\mathcal{P}_F}$$

כלומר

$$x^{q^n} \in x+\mathcal{P}_F$$

אבל $x+\mathcal{P}_F$ היא כזכור קבוצה סגורה ולכן $a(x)=\lim_{n\to\infty}x^{q^n}\in x+\mathcal{P}_F$.

כלומר $a(x)\equiv x \pmod{\mathcal{P}_F}$ ו־$a(x)^{q-1}=1$ אלה הן התכונות היחידות המגדירות את $\omega(x)$ ולכן $a(x)=\omega(x)$. ■

משפט 3.26 תהי $F/\mathbb{Q}_p$ הרחבה סופית $F\subseteq\overline{\mathbb{Q}_p}$ מדרגת סיעוף e ודרגת שארית f. נקבע π יוצר של $\mathcal{P}_F$ בחוג $\mathcal{O}_F$. ($\mathcal{P}_F=\mathcal{O}_F\pi$, $\nu_p(\pi)=\frac{1}{e}$)
אז לכל $x\in F^*$ יש ייצוג יחיד בצורה $x=\sum_{i=m}^{\infty}a_i\pi^i$ כאשר $m\in\mathbb{Z}$, $a_m\neq0$ ולכל $i\geq m$ מתקיים $a_i^{p^f}=a_i$.

הוכחה: יהי $x\in F^*$. נציג $x=\pi^m\cdot\omega(x)\cdot(1+u)$, כאשר $m\in\mathbb{Z}$ ו־$u\in\mathcal{P}_F$.

$$\begin{aligned} \nu_p(x) &= \nu_p(\pi^m)=\frac{m}{e} \\ m &= e\nu_p(x) \end{aligned}$$

נסמן $v=\omega(x)\cdot u\in\mathcal{P}_F$ אז מתקיים

$$\begin{aligned} x &= \pi^m\underbrace{\omega(x)}_{a_m}+\pi^m\cdot v \\ &= a_m\pi^m+\pi^m\cdot v \end{aligned}$$

נמשיך באותו אופן עם v:

$$v = \pi^{l}\omega(v)(1+u')$$

כאשר $l \geq 1$ (כי $v \in \mathcal{P}_F$), $u' \in \mathcal{P}_F$. נסמן $v' = \omega(v)u' \in \mathcal{P}_F$. אז

$$\begin{aligned} v &= \pi^{l}\omega(v)+\pi^{l}v' \\ x &= a_m\pi^m+\pi^{m+l}\cdot\underbrace{\omega(v)}_{a_{m+l}}+\pi^{m+l}v' \\ &= a_m\pi^m+a_{m+l}\pi^{m+l}+\pi^{m+l}v' \end{aligned}$$

יחידות: נניח כי $x=\sum_{i=n}^{\infty}b_i\pi^i$ הוא ייצוג נוסף כנ"ל, כאשר $b_n \neq 0$.

$$x = \pi^n\left(b_n+b_{n+1}\pi+b_{n+2}\pi^2+\ldots\right)$$

$b_n \in \mu_{q-1} \Longrightarrow |b_n|_p = 1$

הטור $b_{n+1}\pi+b_{n+2}\pi^2+\ldots$ מתכנס כי איברו הכללי שואף ל0 ושייך ל$\mathcal{P}_F$ ולכן

$$\begin{aligned} |b_n+b_{n+1}\pi+\ldots|_p &= |b_n|_p \\ &= 1 \end{aligned}$$

ולכן

$$\begin{aligned} |x|_p &= |\pi|_p^n \\ &= p^{-\frac{n}{e}} \end{aligned}$$

מצד שני $|x|_p = p^{-\frac{m}{e}}$ ולכן $p^{-\frac{m}{e}} = p^{-\frac{n}{e}}$ כלומר $m=n$.

$$\begin{aligned} \frac{x}{\pi^m} &= b_m+b_{m+1}\pi+\ldots \\ &\equiv b_m \pmod{\mathcal{P}_F} \end{aligned}$$

מצד שני

$$\begin{aligned} \frac{x}{\pi^m} &= a_m+a_{m+1}\pi+\ldots \\ &\equiv a_m \pmod{\mathcal{P}_F} \end{aligned}$$

ולכן $a_m \equiv b_m \pmod{\mathcal{P}_F}$. מאחר ו$a_m, b_m$ הם שורשי יחידה המסכימים מודולו $\mathcal{P}_F$, נקבל כי $a_m = b_m$.

נסיק כי

$$\sum_{i=m+1}^{\infty}a_i\pi^i = \sum_{i=m+1}^{\infty}b_i\pi^i$$

וכו'. נסיק כי $a_i = b_i$ לכל $i \geq m$. ■

3.5 הרחבות לא מסועפות של $\mathbb{Q}_p$

משפט 3.27

1. לכל f טבעי קיימת הרחבה לא מסועפת יחידה של $\mathbb{Q}_p$ ממעלה f, שתסומן K_f^{unr}. היא מתקבלת בצורה $K_f^{\mathrm{unr}}=\mathbb{Q}_p[\alpha]$, כאשר α הוא שורש פרימיטיבי של 1 מסדר p^f-1.

2. לכל שדה הרחבה $F/\mathbb{Q}_p$ מדרגת סיעוף e ודרגת שארית f, מתקיים

$$F = K_f^{\mathrm{unr}}(\pi)$$

כאשר $\mathcal{P}_F=\mathcal{O}_F\pi$ ו-π הוא שורש של פולינום איזנשטיין ממעלה e מעל השדה K_f^{unr}. (התמונה היא $F \subseteq K_f^{\mathrm{unr}} \subseteq F$, $\mathbb{Q}_p$, כאשר $K_f^{\mathrm{unr}}/\mathbb{Q}_p$ לא מסועפת ממעלה f, ו-F/K_f^{unr} מסועפת לחלוטין ממעלה e)

הוכחה:

1. יהי f מספר טבעי. החבורה $\mathbb{F}_{p^f}^*$ ציקלית מסדר p^f-1. נבחר לה יוצר ציקלי t. ברור כי

$$\mathbb{F}_{p^f} = \mathbb{F}_p[t]$$

כיוון ש $\left[\mathbb{F}_{p^f}:\mathbb{F}_p\right]=f$ ו-t אלגברי ממעלה f מעל $\mathbb{F}_p$.
יהי $p(x)=x^f+a_{f-1}x^{f-1}+\ldots+a_1x+a_0\in\mathbb{Z}_p[x]$ כך ש-$\bar{p}(x)\in\mathbb{F}_p[x]$ הוא הפולינום האי־פריק של t מעל $\mathbb{F}_p$. בפרט $p(x)$ אי־פריק ב-$\mathbb{Z}_p[x]$.
$p(x)$ אי־פריק גם כפולינום ב-$\mathbb{Q}_p[x]$ כי $\mathbb{Q}_p$ הוא שדה המנות של $\mathbb{Z}_p$, וכן $p(x)$ פולינום פרימיטיבי (כל המחלקים המשותפים המרביים של מקדמי $p(x)$ הם הפיכים, $p(x)$ מתוקן). נבחר $\alpha\in\mathbb{Q}_p$ שורש של $p(x)$. לכן $K=\mathbb{Q}_p[\alpha]$ ממעלה f מעל $\mathbb{Q}_p$.
α שלם מעל $\mathbb{Z}_p$ ולכן $\alpha\in\mathcal{O}_K$. מתקיים

$$\begin{aligned} p(\alpha+\mathcal{P}_K) &= p(\alpha)+\mathcal{P}_K \\ &= \mathcal{P}_K \end{aligned}$$

ולכן

$$\bar{p}(\alpha+\mathcal{P}_K) = 0$$

כלומר $\alpha+\mathcal{P}_K$ הוא שורש של $\bar{p}(x)$.
(תזכורת:

$$\begin{aligned} \mathbb{F}_p\cong\mathbb{Z}_p/p\mathbb{Z}_p &\hookrightarrow \mathcal{O}_K/\mathcal{P}_K \\ a+p\mathbb{Z}_p &\to a+\mathcal{P}_K \end{aligned}$$

)
נסיק כי $f_k=[\mathcal{O}_K/\mathcal{P}_K:\mathbb{F}_p]\geq f$ (כי $\bar{p}$ אי־פריק ממעלה f מעל $\mathbb{F}_p$ ו $a+\mathcal{P}_K\in\mathcal{O}_K/\mathcal{P}_K$ הוא שורש שלו) אבל $f=[K:\mathbb{Q}_p]=e_K\cdot f_K\geq f_K$ ומצד שני $f_K=[\mathcal{O}_K/\mathcal{P}_K:\mathbb{F}_p]\geq f$
בסה"כ $f_K=f=[K:\mathbb{Q}_p]$ ולכן $e_K=1$, כלומר $K/\mathbb{Q}_p$ הרחבה לא מסועפת

ממעלה f.
באופן כללי נניח כי $F/\mathbb{Q}_p$ מדרגת סיעוף e ודרגת שארית f. נסמן $q=p^f$. ראינו כי $F \supseteq \mu_{q-1}$ וכן μ_{q-1} מערכת נציגים ל $\mathcal{O}_F^*/\left(1+\mathcal{P}_F\right)$. יהי $\alpha\in\mu_{q-1}$ שורש פרימיטיבי של 1 מסדר $q-1$. זהו יוצר ציקלי של μ_{q-1} וכן $\alpha+\mathcal{P}_F$ יוצר ציקלי של $\mathbb{F}_q^*=\left(\mathcal{O}_F/\mathcal{P}_F\right)^*$. נתבונן ב$\mathbb{Q}_p\left[\alpha\right]\subseteq F$. יש שיכון מעל $\mathbb{F}_p$:

$$j:\mathcal{O}_{\mathbb{Q}_p[\alpha]}/\mathcal{P}_{\mathbb{Q}_p[\alpha]} \quad\hookrightarrow\quad \mathcal{O}_F/\mathcal{P}_F$$

כמובן $\alpha\in\mathcal{O}_{\mathbb{Q}_p[\alpha]}$ (כי $\left|\alpha\right|_p=1$).

$$\left\{\alpha^i+\mathcal{P}_f \mid 1\le i\le q-1\right\} \quad=\quad \left\{j\left(\alpha^i+\mathcal{P}_{\mathbb{Q}_p[\alpha]}\right)\mid 1\le i\le q-1\right\}$$

קבוצה בת $q-1$ איברים שונים, ובפרט בקבוצה $\left\{\alpha^i+\mathcal{P}_{\mathbb{Q}_p[\alpha]}\mid 1\le i\le q-1\right\}$ יש $q-1$ איברים שונים, לכן

$$\left|\mathcal{O}_{\mathbb{Q}_p[\alpha]}/\mathcal{P}_{\mathbb{Q}_p[\alpha]}\right| \quad\ge\quad q=p^f$$

(כי גם 0 בקבוצה זו)
ומצד שני

$$p^f \quad=\quad \left|\mathcal{O}_F/\mathcal{P}_F\right|\ge\left|\mathcal{O}_{\mathbb{Q}_p[\alpha]}/\mathcal{P}_{\mathbb{Q}_p[\alpha]}\right|$$

לכן $\mathcal{O}_F/\mathcal{P}_F\cong\mathbb{F}_q\cong\mathcal{O}_{\mathbb{Q}_p[\alpha]}/\mathcal{P}_{\mathbb{Q}_p[\alpha]}$. בפרט נסיק כי $\left[\mathbb{Q}_p\left[\alpha\right]:\mathbb{Q}_p\right]\ge f$ (כי $\left[\mathbb{Q}_p\left[\alpha\right]:\mathbb{Q}_p\right]\ge\left[\mathcal{O}_{\mathbb{Q}_p[\alpha]}/\mathcal{P}_{\mathbb{Q}_p[\alpha]}:\mathbb{F}_p\right]=f$).
במקרה הפרטי $e=1$ (כלומר $F/\mathbb{Q}_p$ הרחבה לא מסועפת)

$$f\le\left[\mathbb{Q}_p\left[\alpha\right]:\mathbb{Q}_p\right] \quad\le\quad \left[F:\mathbb{Q}_p\right]=f$$

מכאן $F=\mathbb{Q}_p\left[\alpha\right]$.
הוכחנו כי אם $F/\mathbb{Q}_p$ הרחבה לא מסועפת ממעלה f, אז $F=\mathbb{Q}_p\left[\alpha\right]$ כאשר α שורש פרימיטיבי של 1 מסדר p^f-1.
זה מראה גם את היחידות בחלק זה של המשפט.
לבסוף, יהי α שורש פרימיטיבי של 1 מסדר p^f-1. נסתכל בK_f^{unr}. יש β יוצר של μ_{q-1} כך ש$K_f^{\mathrm{unr}}=\mathbb{Q}_p\left[\beta\right]$. כיוון ש$\mathbb{Q}_p\left[\alpha\right]=\mathbb{Q}_p\left[\beta\right]$, קיבלנו כי $\mathbb{Q}_p\left[\alpha\right]=K_f^{\mathrm{unr}}$.

2. $F/\mathbb{Q}_p$ מדרגת סיעוף e ודרגת שארית f. נסמן $q=p^f$. אנו יודעים כי $\mu_{q-1}\subseteq F$ ולכן לכל יוצר ציקלי α של μ_{q-1} מתקיים $K_f^{\mathrm{unr}}=\mathbb{Q}_p\left[\alpha\right]\subseteq F$. יהי π כך ש$\mathcal{P}_F=\mathcal{O}_F\pi$. יהי $E\left(x\right)\in K_f^{\mathrm{unr}}\left[x\right]$ הפולינום האי־פריק של π מעל K_f^{unr} .

$$E\left(x\right) \quad=\quad \left(x-\pi_1\right)\cdot\left(x-\pi_2\right)\cdot\ldots\cdot\left(x-\pi_d\right)$$

כאשר $\pi_d, \ldots, \pi_1$ הם צמודי גלואה של π מעל K_f^{unr}.

$$\begin{aligned} d &= \left[K_f^{\mathrm{unr}}(\pi) : K_f^{\mathrm{unr}}\right] \\ &= \frac{\left[F : K_f^{\mathrm{unr}}\right]}{\left[F : K_f^{\mathrm{unr}}(\pi)\right]} \\ &= \frac{\frac{[F:\mathbb{Q}_p]}{\left[K_f^{\mathrm{unr}}(\pi):\mathbb{Q}_p\right]}}{\left[F : K_f^{\mathrm{unr}}(\pi)\right]} \\ &= \frac{\frac{ef}{f}}{\left[F : K_f^{\mathrm{unr}}(\pi)\right]} \\ &= \frac{e}{\left[F : K_f^{\mathrm{unr}}(\pi)\right]} \end{aligned}$$

לכן $d \mid e$.

$$\begin{aligned} |\pi|_p &= \left|N_{K_f^{\mathrm{unr}}(\pi)/\mathbb{Q}_p}(\pi)\right|_p^{\frac{1}{df}} \\ &= \left|N_{K_f^{\mathrm{unr}}/\mathbb{Q}_p}\left(\underbrace{N_{K_f^{\mathrm{unr}}(\pi)/K_f^{\mathrm{unr}}}}_{\pm c}\right)\right|_p^{\frac{1}{df}} \end{aligned}$$

כאשר $\pm c \in K_f^{\mathrm{unr}}$ האיבר החופשי של $E(x)$.

$$\begin{aligned} |\pi|_p &= \left|N_{K_f^{\mathrm{unr}}/\mathbb{Q}_p}(c)\right|_p^{\frac{1}{df}} \\ &= \left(\left|N_{K_f^{\mathrm{unr}}/\mathbb{Q}_p}(c)\right|_p^{\frac{1}{f}}\right)^{\frac{1}{d}} \\ &= |c|_p^{\frac{1}{d}} \end{aligned}$$

לכן $|\pi|_p = |c|_p^{\frac{1}{d}}$. לכן

$$\frac{1}{e} = \nu_p(\pi) = \frac{1}{d}\nu_p(c)$$

אבל

$$\nu_p(c) \in \nu_p\left(\left(K_f^{\mathrm{unr}}\right)^*\right) = \mathbb{Z}$$

(כי K_f^{unr} הרחבה לא מסועפת) ולכן $\nu_p(c) \in \mathbb{Z}$ ונסיק כי $e \mid d$. זה מראה כי $e = d$ וכי $\nu_p(c) = 1$. כלומר

$$c \in \mathcal{P}_{K_f^{\mathrm{unr}}} \setminus \mathcal{P}^2_{K_f^{\mathrm{unr}}}$$

(כזכור, $\mathcal{P}_{K_f^{\mathrm{unr}}} = \mathcal{O}_{K_f^{\mathrm{unr}}} p$)
כיוון ש$1 > |\pi|_p = |\pi_i|_p$ לכל $1 \le i \le d$, כל מקדמי $E(x)$ (פרט לעליון) שייכים ל$\mathcal{P}_{K_f^{\mathrm{unr}}}$, ולכן $E(x)$ פולינום איזנשטיין ממעלה e מעל K_f^{unr}.

■

מסקנה 3.28 יהי $\alpha \in \overline{\mathbb{Q}_p}$ שורש פרימיטיבי של 1 מסדר m זר לp. אז $\mathbb{Q}_p[\alpha]/\mathbb{Q}_p$ הרחבה לא מסועפת.

הוכחה: מכיוון שp וm זרים, p הפיך מודולו m. יהי f הסדר של p מודולו m ($p + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^*$). בפרט $p^f - 1 = 0 \pmod m$. נכתוב $p^f - 1 = m \cdot m'$.
יהי $\beta \in \overline{\mathbb{Q}_p}$ שורש פרימיטיבי של 1 מסדר $p^f - 1$. אז $\beta^{m'}$ הוא שורש פרימיטיבי של 1 מסדר m. מכאן, $\alpha = \beta^{m'r}$, כאשר r זר לm.
מכאן $\mathbb{Q}_p[\alpha] = \mathbb{Q}_p\left[\beta^{m'r}\right] \subseteq \mathbb{Q}_p[\beta]$. כיוון ש $\mathbb{Q}_p[\beta]/\mathbb{Q}_p$ הרחבה לא מסועפת, גם $\mathbb{Q}_p[\alpha]/\mathbb{Q}_p$ הרחבה לא מסועפת. ■

מסקנה 3.29 איחוד כל שדות ההרחבה ממימד סופי של $\mathbb{Q}_p$ אשר אינם מסועפים הוא שדה (החלקי ל$\overline{\mathbb{Q}_p}$).

הוכחה: נניח כי $\mathbb{Q}_p \subseteq F_1, F_2 \subseteq \overline{\mathbb{Q}_p}$ שדות הרחבה של $\mathbb{Q}_p$, לא מסועפים (מעל $\mathbb{Q}_p$) ממימדים f_1, f_2 בהתאמה. ראינו כי $F_i = \mathbb{Q}_p[\alpha_i]$ כאשר α_i הוא שורש יחידה פרימיטיבי מסדר $p^{f_i} - 1$.

$$\mathbb{Q}_p \quad \subseteq \quad F_1F_2 = \mathbb{Q}_p[\alpha_1, \alpha_2] \subseteq \mathbb{Q}_p[\beta]$$

כאשר β הוא שורש יחידה פרימיטיבי מסדר $m = \left(p^{f_1} - 1\right)\left(p^{f_2} - 1\right)$. כיוון ש$m$ זר לp, נובע מהמסקנה הקודמת כי $\mathbb{Q}_p(\beta)/\mathbb{Q}_p$ הרחבה לא מסועפת. לכן סכומים ומכפלות של איברים מF_1 וF_2 שייכים ל$\mathbb{Q}_p[\beta]$ ולכן לאיחוד הנ"ל. ■

נסמן את האיחוד במסקנה ב$\mathbb{Q}_p^{\mathrm{unr}}$. אומרים כי זהו השדה החלקי ל$\overline{\mathbb{Q}_p}$ שהוא ההרחבה הלא מסועפת המקסימלית של $\mathbb{Q}_p$.
נסמן

$$\mathcal{O}_{\mathbb{Q}_p^{\mathrm{unr}}} \quad = \quad \mathbb{Z}_p^{\mathrm{unr}} = \left\{x \in \mathbb{Q}_p^{\mathrm{unr}} \mid |x|_p \le 1\right\}$$

מתקיים

$$\mathcal{P}_{\mathbb{Q}_p^{\mathrm{unr}}} \quad = \quad \left\{x \in \mathbb{Q}_p^{\mathrm{unr}} \mid |x|_p < 1\right\} = p\mathbb{Z}_p^{\mathrm{unr}}$$

אכן: אם $x \in \mathbb{Q}_p^{\mathrm{unr}}$ כך ש$|x|_p < 1$, יש $F/\mathbb{Q}_p$ הרחבה לא מסועפת (ממימד f), כך ש$x \in F$. כמובן, $x \in \mathcal{P}_F = \mathcal{O}_F p$ (כי ההרחבה לא מסועפת ולכן $e_F = 1$) ולכן $\left|p^{-1}x\right|_p \le 1$ ולכן $p^{-1}x \in \mathbb{Z}_p^{\mathrm{unr}}$, כלומר $x \in p\mathbb{Z}_p^{\mathrm{unr}}$.

טענה 3.30 $\mathbb{Z}_p^{\mathrm{unr}}/p\mathbb{Z}_p^{\mathrm{unr}} \cong \overline{\mathbb{F}}_p$, כאשר $\overline{\mathbb{F}}_p$ הסגור האלגברי של $\mathbb{F}_p$.

הוכחה: ברור כי אגף שמאל הוא שדה (ראינו בעבר באופן כללי כי $\mathcal{P}_F$ הוא אידיאל מקסימלי של $\mathcal{O}_F$) ממציין p. יהי $x \in \left(\mathbb{Z}_p^{\mathrm{unr}}\right)^*$ ותהי $F/\mathbb{Q}_p$ הרחבה לא מסועפת ממימד f, המכילה את x.

$$\begin{array}{rcl}\mathbb{F}_{p^f} \cong \mathcal{O}_F/\mathcal{P}_F & \hookrightarrow & \mathbb{Z}_p^{\mathrm{unr}}/p\mathbb{Z}_p^{\mathrm{unr}} \\ t+\mathcal{P}_F & \mapsto & t+p\mathbb{Z}_p^{\mathrm{unr}}\end{array}$$

(מתקיים $p\mathbb{Z}_p^{\mathrm{unr}} \cap \mathcal{O}_F = \mathcal{P}_F$)

נסתכל על תמונת $x+\mathcal{P}_F$ תחת השיכון הנ"ל, כלומר על $x+p\mathbb{Z}_p^{\mathrm{unr}}$. מאחר ו$x+\mathcal{P}_F$ אלגברי מעל $\mathbb{F}_p$, נקבל כי גם $x+p\mathbb{Z}_p^{\mathrm{unr}}$ אלגברי מעל $\mathbb{F}_p$, ולכן $\mathbb{Z}_p^{\mathrm{unr}}/p\mathbb{Z}_p^{\mathrm{unr}}$ הוא שדה הרחבה אלגברית של $\mathbb{F}_p$, ולכן יש שיכון מעל $\mathbb{F}_p$:

$$\eta : \mathbb{Z}_p^{\mathrm{unr}}/p\mathbb{Z}_p^{\mathrm{unr}} \quad \hookrightarrow \quad \overline{\mathbb{F}}_p$$

אבל $\mathbb{Z}_p^{\mathrm{unr}}/p\mathbb{Z}_p^{\mathrm{unr}}$ מכיל את כל השדות הסופיים $\mathbb{F}_{p^f}$ לכל f טבעי. כזכור, יש לכל f תת־שדה יחיד בעל p^f איברים, וכן כל איבר של $\overline{\mathbb{F}}_p$ שייך לשדה סופי כזה. ולכן השיכון η הוא על. ■

3.6 השדה $\mathbb{C}_p$

משפט 3.31 השדה $\overline{\mathbb{Q}_p}$ אינו שלם.

הוכחה: לכל n טבעי זר לp, יהי $\zeta_n \in \overline{\mathbb{Q}_p}$ שורש פרימיטיבי מסדר n. אם $p \mid n$, נגדיר $\zeta_n = 1$.

נתבונן בטור $\sum_{n=1}^{\infty} \zeta_n p^n$, כלומר בסדרה

$$\overline{\mathbb{Q}_p} \quad \supseteq \quad \left\{S_n = \sum_{k=1}^{n} \zeta_k p^k\right\}_{n=1}^{\infty}$$

כיוון ש$\zeta_n p^n \underset{n\to\infty}{\longrightarrow} 0$, זאת סדרת קושי. נניח בשלילה כי הסדרה מתכנסת ל$\alpha \in \overline{\mathbb{Q}_p}$.

נסמן $F = \mathbb{Q}_p[\alpha]$. נראה כי $\zeta_n \in F$ לכל n טבעי.

$\zeta_1 = 1 \in F$ לפי ההגדרה.

נניח כי $\zeta_n \in F$ לכל $1 \le n < m$. נוכיח כי $\zeta_m \in F$. אפשר להניח $p \nmid m$.

נתבונן ב

$$\beta \quad = \quad p^{-m}\left(\alpha - \sum_{k=1}^{m-1} \zeta_k p^k\right)$$

לפי ההנחה $\beta \in F$

$$\beta \quad = \quad \zeta_m + \zeta_{m+1} p + \ldots$$

נשים לב כי ζ_m הוא בעל ערך מוחלט 1 ו $\zeta_{m+1} p + \ldots$ הוא בעל ערך מוחלט < 1.

לכן

$$|\beta - \zeta_m|_p \quad < \quad 1$$

כלומר, $\beta-\zeta_m\in\mathcal{P}_{F(\zeta_m)}$ ולכן $\beta+\mathcal{P}_{F(\zeta_m)}=\zeta_m+\mathcal{P}_{F(\zeta_m)}$.
נעלה בחזקת m ונקבל

$$\beta^m+\mathcal{P}_{F(\zeta_m)} = 1+\mathcal{P}_{F(\zeta_m)}$$

כלומר

$$\begin{aligned}\beta^m-1 &\in \mathcal{P}_{F(\zeta_m)}\\ \left|\beta^m-1\right|_p &< 1\end{aligned}$$

לכן $\beta+\mathcal{P}_F$ הוא שורש של $x^m-1\in\left(\mathcal{O}_F/\mathcal{P}_F\right)[x]$. כיוון ש־$p\nmid m$, מתקיים כי x^m-1 הוא פולינום ספרבילי מעל $\mathcal{O}_F/\mathcal{P}_F$. מהלמה של הנזל, יש פירוק ב־$\mathcal{O}_F[x]$

$$x^m-1 = (x-u)\,b(x)$$

כאשר $u\equiv\beta\ (\mod \mathcal{P}_F)$.
גם ζ_m הוא שורש x^m-1 ולכן $\zeta_m=u$ או ζ_m הוא שורש $b(x)$. במקרה שני,

$$b\left(\zeta_m+\mathcal{P}_{F(\zeta_m)}\right) = 0+\mathcal{P}_{F(\zeta_m)}$$

אבל אז $\beta+\mathcal{P}_{F(\zeta_m)}=\zeta_m+\mathcal{P}_{F(\zeta_m)}$ ולכן $b\left(\beta+\mathcal{P}_{F(\zeta_m)}\right)=\mathcal{P}_{F(\zeta_m)}$ ולכן נסיק כי $b(\beta+\mathcal{P}_F)=\mathcal{P}_F$ ומכאן נסיק כי $\beta+\mathcal{P}_F$ הוא שורש כפול של x^m-1 כפולינום מעל $\mathcal{O}_F/\mathcal{P}_F$ - סתירה כי פולינום זה ספרבילי.

מסקנה 3.32 לכל f טבעי, $\zeta_{p^f-1}\in F$, ומכאן $K_f^{\text{unr}}\subseteq F$ לכל f, ולכן $[F:\mathbb{Q}_p]\geq f$ לכל f טבעי. סתירה. (כי $F=\mathbb{Q}_p(\alpha)$ הרחבה סופית של $\mathbb{Q}_p$).

■

מסקנה 3.33 (מההוכחה) $\mathbb{Q}_p^{\text{unr}}$ אינו שלם.

יהי $\mathbb{C}_p$ שלמה ההשלמה של $\overline{\mathbb{Q}_p}$ ביחס ל־$|\cdot|_p$. נמשיך ונסמן ב־$|\cdot|_p$ את הערך המוחלט של $\mathbb{C}_p$.
אנו יודעים כי אם $0\neq x\in\mathbb{C}_p$, ו־$\{x_m\}_{m=1}^{\infty}\subseteq\overline{\mathbb{Q}_p}$ שואפת ל־x, אז

$$|x|_p = \lim_{n\to\infty}|x_n|_p$$

ולכן החל ממקום מסוים $|x|_p=|x_n|_p$ ולכן

$$|\mathbb{C}_p|_p = \left|\overline{\mathbb{Q}_p}\right|_p$$

נגדיר גם את $\nu_p(x)=-\log_p|x|_p$. מתקיים

$$\nu_p\left(\mathbb{C}_p^*\right) = \nu_p\left(\overline{\mathbb{Q}_p}\right)=\mathbb{Q}$$

תמונה:

$$\begin{aligned}\mathbb{F}_{p^r}\cong\mathcal{O}_F/\mathcal{P}_F\hookrightarrow\mathcal{O}_{\overline{\mathbb{Q}_p}}/\mathcal{P}_{\overline{\mathbb{Q}_p}} &\hookrightarrow \mathcal{O}_{\mathbb{C}_p}/\mathcal{P}_{\mathbb{C}_p}\\ x+\mathcal{P}_{\overline{\mathbb{Q}_p}} &\mapsto x+\mathcal{P}_{\mathbb{C}_p}\end{aligned}$$

שיכון שדות מעל $\mathbb{F}_p$.

טענה 3.34

$$\mathcal{O}_{\mathbb{C}_p}/\mathcal{P}_{\mathbb{C}_p} \cong \mathcal{O}_{\overline{\mathbb{Q}_p}}/\mathcal{P}_{\overline{\mathbb{Q}_p}} \cong \overline{\mathbb{F}}_p$$

הוכחה: יהי $x \in \mathcal{O}^*_{\mathbb{C}_p}$. נראה כי מודולו $\mathcal{P}_{\mathbb{C}_p}$, x אלגברי מעל $\mathbb{F}_p$. מאחר ו$\overline{\mathbb{Q}_p}$ צפוף ב$\mathbb{C}_p$, יש $x' \in \overline{\mathbb{Q}_p}$ כך ש$|x - x'|_p < 1$, ולכן $|x'|_p = 1$.

יהי $\mathbb{Q}_p \subseteq F \subseteq \overline{\mathbb{Q}_p}$ שדה הרחבה סופית כך ש$x' \in F$. נסתכל על השיכון

$$\begin{aligned} \mathcal{O}_F/\mathcal{P}_F &\hookrightarrow \mathcal{O}_{\mathbb{C}_p}/\mathcal{P}_{\mathbb{C}_p} \\ x' + \mathcal{P}_F &\mapsto x' + \mathcal{P}_{\mathbb{C}_p} \end{aligned}$$

מאחר ו$|x - x'|_p < 1$ אז $x - x' \in \mathcal{P}_{\mathbb{C}_p}$ ולכן $x + \mathcal{P}_{\mathbb{C}_p} = x' + \mathcal{P}_{\mathbb{C}_p}$, כלומר $x + \mathcal{P}_{\mathbb{C}_p}$ הוא תמונה של $x' + \mathcal{P}_F$ תחת השיכון הנ"ל ולכן $x + \mathcal{P}_{\mathbb{C}_p}$ אלגברי מעל $\mathbb{F}_p$.

(אנו חושבים על $\mathbb{F}_p$ בתור $\left\{i + \mathcal{P}_{\mathbb{C}_p} \mid 0 \le i \le p-1\right\}$) ■

טענה 3.35 לכל $0 \neq x \in \mathbb{C}_p$ יש הצגה בצורה

$$x = p^r \cdot \zeta \cdot (1+u)$$

כאשר $u \in \mathcal{P}_{\mathbb{C}_p}$, ζ הוא שורש יחידה מסדר מהצורה $p^f - 1$ (כאשר f טבעי) ו$r \in \mathbb{Q}$, כאשר p^r מסמן איבר מהצורה הבאה $r = \frac{a}{b}$, כאשר b טבעי וa שלם, וp^r מסמן שורש ב$\overline{\mathbb{Q}_p}$ של הפולינום $t^b - p^a$.

הוכחה: $|x|_p = p^{-r}$ כאשר $r = \frac{a}{b} \in \mathbb{Q}$ כאשר b טבעי וa שלם. קל לבדוק כי $|p^r|_p = p^{-r}$ כאשר $p^r \in \overline{\mathbb{Q}_p}$ כנ"ל.

נסמן $y = xp^{-r} \in \mathbb{C}_p$, אז $|y|_p = 1$.

כמו קודם, ניקח $y' \in \overline{\mathbb{Q}_p}$ כך ש$|y - y'|_p < 1$ ויהי $\mathbb{Q}_p \subseteq F \subseteq \overline{\mathbb{Q}_p}$, כך ש$y' \in F$. (מתקיים שוב $|y'|_p = 1$). אז

$$y = \left(y \cdot (y')^{-1}\right) \cdot y'$$

כעת $\left(y \cdot (y')^{-1}\right) \in 1 + \mathcal{P}_{\mathbb{C}_p}$ כי $\left|y \cdot (y')^{-1} - 1\right|_p = |y - y'|_p \cdot |y'|_p^{-1} = |y - y'|_p < 1$.

בנוסף בF מתקיים כי בF ניתן להציג את y' בצורה $\pi_F^0 \cdot \omega(y') \cdot (1+v)$ כאשר $v \in \mathcal{P}_F$. נקבל לכן

$$y = \zeta(1+u)$$

ולכן

$$x = p^r \cdot \zeta \cdot (1+u)$$

כנדרש. ■

למה 3.36 נתונים שני פולינומים ממעלה n

$$f(x), g(x) \quad \in \quad \mathbb{C}_p[x]$$

נניח כי $g(x) = \sum_{i=0}^{n} a_i x^i$ ($a_n \neq 0$).
נניח כי $\beta \in \mathbb{C}_p$ שורש של הפולינום $g(x)$, אז

$$|f(\beta)|_p \quad \leq \quad |f-g|_p \left(\max_{0 \leq i \leq n} \left| \frac{a_i}{a_n} \right|_p \right)^n$$

כאשר אם $f(x) = \sum_{i=0}^{n} b_i x^i$ אז

$$|f-g|_p \quad = \quad \max_{0 \leq i \leq n} |a_i - b_i|_p$$

הוכחה:

$$\begin{aligned} |f(\beta)|_p &= |f(\beta) - g(\beta)|_p \\ &= \left| \sum_{i=0}^{n} (b_i - a_i) \beta^i \right|_p \\ &\leq \max_{0 \leq i \leq n} |b_i - a_i|_p \cdot |\beta|_p^i \\ &\leq |f-g|_p \cdot \max_{0 \leq i \leq n} |\beta|_p^i \end{aligned}$$

מתקיים

$$-\sum_{i=0}^{n-1} a_i \beta^i \quad = \quad a_n \beta^n$$

ולכן

$$\begin{aligned} |a_n|_p \cdot |\beta|_p^n &\leq \max_{0 \leq i \leq n-1} |a_i|_p \, |\beta|_p^i \\ &\leq \max_{0 \leq i \leq n-1} |a_i|_p \cdot \max \left\{ 1, |\beta|_p^{n-1} \right\} \end{aligned}$$

אם $|\beta|_p > 1$ נקבל

$$|a_n|_p \cdot |\beta|_p^n \quad \leq \quad \max_{0 \leq i \leq n-1} |a_i|_p \cdot |\beta|_p^{n-1}$$

כלומר

$$|\beta|_p \quad \leq \quad \max_{0 \leq i \leq n-1} \left| \frac{a_i}{a_n} \right|_p$$

לכן בכל מקרה

$$\begin{aligned} |\beta|_p &\le \max\left\{1, \max_{0\le i\le n-1}\left|\frac{a_i}{a_n}\right|_p\right\} \\ &= \max_{0\le i\le n}\left\{\left|\frac{a_i}{a_n}\right|_p\right\} \end{aligned}$$

לכן

$$\begin{aligned} |f(\beta)|_p &\le \max_{0\le i\le n}|b_i-a_i|_p\cdot|\beta|_p^n \\ &\le \max_{0\le i\le n}|b_i-a_i|_p\cdot\left(\max_{0\le i\le n}\left|\frac{a_i}{a_n}\right|_p\right)^n \end{aligned}$$

כנדרש. ■

משפט 3.37 $\mathbb{C}_p$ סגור אלגברית.

הוכחה: יהי

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$$

פולינום ב-$\mathbb{C}_p[x]$. נראה כי יש לו שורש ב-$\mathbb{C}_p$.

נבחר סדרות מ-$\overline{\mathbb{Q}}_p$ $\{a_{ij}\}_{i=1}^{\infty}$ השואפות ל-a_j (ל-$0\le j\le n-1$). נגדיר

$$\begin{aligned} g_i(x) &= x^n + a_{i,n-1}x^{n-1} + \ldots + a_{i,1}x + a_{i,0} \\ g_i(x) &\in \overline{\mathbb{Q}}_p[x] \end{aligned}$$

נפרק את $g_i(x)$ מעל $\overline{\mathbb{Q}}_p$:

$$g_i(x) = (x-r_{1i})\cdot(x-r_{2i})\cdot\ldots\cdot(x-r_{ni})$$

נראה שאפשר לבחור לכל $1\le i$, שורש $r_{k_i,i}$ של $g_i(x)$, כך שהסדרה $\{r_{k_i,i}\}$ היא סדרת קושי.

מתקיים מהלמה

$$|g_{i+1}(r_{k,i})|_p \le |g_{i+1}-g_i|_p\cdot\max_{0\le j\le n-1}\left\{1,|a_{i,j}|_p\right\}^n$$

כיוון ש-$a_{ij}\underset{i\to\infty}{\longrightarrow}a_j$ ל-$0\le j\le n-1$, אז $\{a_{ij}\}_{i=1}^{\infty}$ חסומה, ולכן יש $1\le C$ כך ש-$|a_{i,j}|_p\le C$ לכל $i\ge 1$ ולכל $0\le j\le n-1$.

$$|g_{i+1}(r_{k,i})|_p \le |g_{i+1}-g_i|_p\cdot C^n$$

אבל

$$g_{i+1}(r_{k,i}) = (r_{k,i}-r_{1,i+1})\cdot(r_{k,i}-r_{2,i+1})\cdot\ldots\cdot(r_{k,i}-r_{n,i+1})$$

ולכן

$$\prod_{l=1}^{n}\left|r_{k,i}-r_{l,i+1}\right|_p \leq \left|g_{i+1}-g_i\right|_p\cdot C^n$$

לכן יש $1\leq l\left(k\right)\leq n$ כך ש

$$\left|r_{k,i}-r_{l(k),i+1}\right|_p \leq \sqrt[n]{\left|g_{i+1}-g_i\right|_p}\cdot C$$

נבחר את הסדרה הבאה: ל$i=1$ נבחר $r_{1,1}$ (כלומר $k_1=1$). אם בחרנו לאינדקס i את k_i, אז לאינדקס $i+1$ נבחר את $k_{i+1}=l\left(k_i\right)$.
מתקיים

$$\begin{aligned}\left|r_{k_i,i}-r_{k_{i+1},i+1}\right|_p &= \left|r_{k_i,i}-r_{l(k_{i+1}),i+1}\right|_p\\ &\leq \sqrt[n]{\left|g_{i+1}-g_i\right|_p}\cdot C\end{aligned}$$

אבל מאחר וg_i סדרת קושי, נקבל כי

$$\lim_{i\to\infty}\sqrt[n]{\left|g_{i+1}-g_i\right|_p}\cdot C = 0$$

ולכן

$$\left|r_{k_i,i}-r_{k_{i+1},i+1}\right|_p \underset{i\to\infty}{\longrightarrow} 0$$

כלומר, $r_{k_i,i}$ סדרת קושי.
נסמן

$$r = \lim_{i\to\infty} r_{k_i,i}$$

נזכר כי

$$\begin{aligned}g_i\left(x\right) &= x^n+a_{i,n-1}x^{n-1}+\ldots+a_{i,1}x+a_{i,0}\\ g_i\left(x\right) &\in \overline{\mathbb{Q}}_p\left[x\right]\end{aligned}$$

מרציפות

$$f\left(r\right) = \lim_{i\to\infty} f\left(r_{k_i,i}\right)$$

שוב, מהלמה

$$\begin{aligned}\left|f\left(r_{k_i,i}\right)\right|_p &\leq \left|f-g_i\right|_p\cdot\max_{0\leq j\leq n-1}\left\{1,\left|a_{i,j}\right|\right\}^n\\ &\leq \left|f-g_i\right|_p\cdot C^n\underset{i\to\infty}{\longrightarrow}0\end{aligned}$$

לכן $\lim_{i\longrightarrow\infty} f\left(r_{k_i,i}\right)=0$, ולכן $f\left(r\right)=0$, כנדרש. ■

משפט 3.38 $\mathbb{C}_p$ אינו קומפקטי מקומית.

הוכחה: בשלילה, נניח כי יש סביבה של 0 בעלת סגור קומפקטי. לכן הסגור הקומפקטי מכיל כדור פתוח, המכיל כדור סגור כלשהו, ולכן כדור סגור זה הוא קומפקטי כתת קבוצה סגורה של קבוצה קומפקטית. כלומר, יש N טבעי כך ש $\left\{x \in \mathbb{C}_p \mid |x|_p \le p^{-N}\right\}$ קומפקטי. ע"י הכפלה בp^{-N}, נסיק כי

$$\mathcal{O}_{\mathbb{C}_p} = \left\{x \in \mathbb{C}_p \mid |x|_p \le 1\right\}$$

הוא קומפקטי.

נבנה סדרה ב $\mathcal{O}_{\mathbb{C}_p}$ שאין לה תת־סדרה מתכנסת.

לכל n טבעי יהי $\eta_n \in \overline{\mathbb{Q}}_p \subseteq \mathbb{C}_p$ שורש יחידה פרימיטיבי מסדר $p^n - 1$.

בשלילה, נניח כי יש ל$\{\eta_n\}$ יש תת־סדרה המתכנסת לα. אז $|\alpha|_p = 1$ (כי $|\eta_n|_p = 1$).

ראינו (בהוכחה כי $\overline{\mathbb{F}}_p \cong \mathcal{O}_{\mathbb{C}_p}/\mathcal{P}_{\mathbb{C}_p}$) כי $\alpha + \mathcal{P}_{\mathbb{C}_p}$ אלגברי מעל

$$\begin{aligned} \mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p &\hookrightarrow \mathcal{O}_{\mathbb{C}_p}/\mathcal{P}_{\mathbb{C}_p} \\ a + p\mathbb{Z}_p &\to a + \mathcal{P}_{\mathbb{C}_p} \end{aligned}$$

ולכן יוצר תת־חבורה ציקלית סופית של $\left(\mathcal{O}_{\mathbb{C}_p}/\mathcal{P}_{\mathbb{C}_p}\right)^*$ מסדר המחלק את $p^f - 1$ לf טבעי מסוים.

יהי k_0 טבעי כך שלכל $k \ge k_0$ מתקיים

$$|\eta_{n_k} - \alpha|_p < 1$$

כלומר

$$\eta_{n_k} + \mathcal{P}_{\mathbb{C}_p} = \alpha + \mathcal{P}_{\mathbb{C}_p}$$

מכאן

$$\left(\eta_{n_k} + \mathcal{P}_{\mathbb{C}_p}\right)^{p^f - 1} = 1 + \mathcal{P}_{\mathbb{C}_p}$$

כלומר

$$|\eta_{n_k} - 1|_p < 1$$

נסמן

$$F_n = \mathbb{Q}_p(\eta_n) \subseteq \overline{\mathbb{Q}}_p$$

ראינו כי זאת ההרחבה הלא מסועפת של $\mathbb{Q}_p$ ממעלה n.

כמו כן, ראינו כי $\eta_n + \mathcal{P}_{F_n}$ הוא יוצר ציקלי של

$$\mathbb{F}_{p^n}^* \cong \left(\mathcal{O}_{F_n}/\mathcal{P}_{F_n}\right)^*$$

ולכן מסדר $p^n - 1$.

מאחר ו$|\eta_{n_k} - 1|_p < 1$, נובע כי

$$\left(\eta_{n_k} + \mathcal{P}_{F_{n_k}}\right)^{p^f - 1} = 1 + \mathcal{P}_{F_{n_k}}$$

ולכן $p^{n_k} - 1 \mid p^f - 1$ לכל $k \ge 1$. סתירה. ■

4 טורי חזקות p־אדיים

4.1 טורים (מתכנסים) מעל $\mathbb{C}_p$

טענה 4.1 נניח כי $\sum_{n=1}^{\infty} a_n$ טור מתכנס ב־$\mathbb{C}_p$, אז לכל פונקציה חד־חד־ערכית ועל $\sigma : \mathbb{N} \to \mathbb{N}$ גם $\sum_{n=1}^{\infty} a_{\sigma(n)}$ מתכנס, ולאותו הסכום.

הוכחה: הטור מתכנס אם ורק אם $a_n \underset{n\to\infty}{\longrightarrow} 0$. יהי $\varepsilon > 0$. קיים N_ε טבעי כך שלכל $n \geq N_\varepsilon$ מתקיים $|a_n|_p < \varepsilon$.
יש $M_\varepsilon \geq N_\varepsilon$ כך ש

$$\{1, 2, \ldots, N_\varepsilon\} \subseteq \{\sigma(1), \sigma(2), \ldots, \sigma(M_\varepsilon)\}$$

נניח כי $n > M_\varepsilon$, אז

$$\sigma(n) \notin \{\sigma(1), \sigma(2), \ldots, \sigma(M_\varepsilon)\}$$

ולכן $\sigma(n) \notin \{1, 2, \ldots, N_\varepsilon\}$, כלומר $\sigma(n) > N_\varepsilon$. לכן $\left|a_{\sigma(n)}\right| < \varepsilon$.
לכן הטור $\sum_{n=1}^{\infty} a_{\sigma(n)}$ מתכנס. נסמן $\alpha = \sum_{n=1}^{\infty} a_n$ אז

$$\begin{aligned}\left|\alpha - \sum_{n=1}^{l} a_{\sigma(n)}\right|_p &= \left|\sum_{\substack{n=1 \\ n\notin\{\sigma(1),\ldots,\sigma(l)\}}}^{\infty} a_n\right|_p \\ &\leq \max_{n\notin\{\sigma(1),\ldots,\sigma(l)\}} |a_n|_p\end{aligned}$$

נניח כי $l > M_\varepsilon$ אז

$$\begin{aligned}\left|\alpha - \sum_{n=1}^{l} a_{\sigma(n)}\right|_p &\leq \max_{n\notin\{\sigma(1),\ldots,\sigma(l)\}} |a_n|_p \\ &\leq \max_{n>N_\varepsilon} |a_n|_p \\ &< \varepsilon\end{aligned}$$

ולכן

$$\sum_{n=1}^{\infty} a_{\sigma(n)} = \alpha$$

■

טענה 4.2 נתונה סדרה $\{a_{m,n}\}_{m,n\geq 1}$ ב־$\mathbb{C}_p$. נניח כי לכל m טבעי $\lim_{n\to\infty} a_{m,n} = 0$ וכן נניח כי $\lim_{m\to\infty} a_{m,n} = 0$ במידה שווה ב־n. אז הטורים $\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} a_{mn}$ ו־$\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} a_{mn}$ מתכנסים, ולאותו הסכום.

הוכחה: יהי $\varepsilon > 0$. קיים N טבעי כך שלכל $m \geq N$ ולכל n טבעי מתקיים $|a_{m,n}|_p < \varepsilon$.
הטור $\sum_{n=1}^{\infty} a_{m,n}$ מתכנס (כי $\lim_{n\to\infty} a_{m,n} = 0$) ולכן לכל $N \geq m$ מתקיים

$$\begin{aligned}\left|\sum_{n=1}^{\infty} a_{m,n}\right|_p &\leq \max_{n\geq 1} |a_{m,n}| \\ &< \varepsilon\end{aligned}$$

מכאן $\lim_{m\to\infty} \sum_{n=1}^{\infty} a_{m,n} = 0$ ולכן הטור $\sum_{m=1}^{\infty}\left(\sum_{n=1}^{\infty} a_{m,n}\right)$ מתכנס.
קיים N_1 טבעי כך שלכל $1 \leq m \leq N-1$ ולכל $n \geq N_1$, $|a_{m,n}|_p < \varepsilon$.
לכן, כאשר $n \geq N_1$

$$\begin{aligned}\left|\sum_{m=1}^{\infty} a_{m,n}\right|_p &= \left|\sum_{m=1}^{N-1} a_{m,n} + \sum_{m=N}^{\infty} a_{m,n}\right|_p \\ &\leq \max\left\{\left|\sum_{m=1}^{N-1} a_{m,n}\right|_p, \left|\sum_{m=N}^{\infty} a_{m,n}\right|_p\right\}\end{aligned}$$

אבל

$$\begin{aligned}\left|\sum_{m=1}^{N-1} a_{m,n}\right|_p &\leq \max_{1\leq m<N} |a_{m,n}|_p \\ &< \varepsilon\end{aligned}$$

ו

$$\begin{aligned}\left|\sum_{m=N}^{\infty} a_{m,n}\right|_p &\leq \max_{m\geq N} |a_{m,n}|_p \\ &< \varepsilon\end{aligned}$$

מכאן

$$\lim_{n\to\infty}\left(\sum_{m=1}^{\infty} a_{m,n}\right) = 0$$

ולכן קיים $\sum_{m=1}^{\infty}\left(\sum_{n=1}^{\infty} a_{m,n}\right)$.
נראה כעת כי הטורים שווים.
מתקיים

$$\begin{aligned}\left|\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} a_{m,n} - \sum_{m=1}^{N-1}\sum_{n=1}^{N_1-1} a_{m,n}\right|_p &= \left|\sum_{m=1}^{N-1}\sum_{n=N_1}^{\infty} a_{m,n} + \sum_{m=N}^{\infty}\sum_{n=1}^{\infty} a_{m,n}\right|_p \\ &< \varepsilon\end{aligned}$$

באופן דומה

$$\left|\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}a_{m,n}-\sum_{n=1}^{N_1-1}\sum_{m=1}^{N-1}a_{m,n}\right|_p \quad < \quad \varepsilon$$

כיוון ש

$$\sum_{n=1}^{N_1-1}\sum_{m=1}^{N-1}a_{m,n} \quad = \quad \sum_{m=1}^{N-1}\sum_{n=1}^{N_1-1}a_{m,n}$$

נסיק כי

$$\left|\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}a_{m,n}-\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}a_{m,n}\right|_p \quad < \quad \varepsilon$$

לכל $\varepsilon > 0$ ולכן השוויון המבוקש מתקיים. ■

טענה 4.3 נניח כי הטורים $\sum_{i=0}^{\infty}a_i$, $\sum_{j=0}^{\infty}b_j$ מתכנסים ב$\mathbb{C}_p$. אז הטורים הבאים מתכנסים ולאותו הסכום:

$$\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}a_ib_j$$

$$\sum_{j=0}^{\infty}\sum_{i=0}^{\infty}a_ib_j$$

$$\sum_{k=0}^{\infty}\left(\sum_{\substack{i+j=k\\ i,j\geq 0}}a_ib_j\right)$$

לסכום $\left(\sum_{j=0}^{\infty}b_j\right)\left(\sum_{i=0}^{\infty}a_i\right)$.

הוכחה: כיוון ש$a_i \longrightarrow 0$, $b_j \longrightarrow 0$, סדרות אלה חסומות, ולכן לכל $\varepsilon > 0$ קיים N טבעי, כך שלכל $i \geq N$ ולכל j, $|a_ib_j|_p < \varepsilon$ וכן לכל $j \geq N$ ולכל i, $|a_ib_j|_p < \varepsilon$. לכן

$$\lim_{i\to 0}(a_ib_j) \quad = \quad 0$$

במידה שווה בj וגם להפך:

$$\lim_{j\to 0}(a_ib_j) \quad = \quad 0$$

במידה שווה בi.

נניח כי N2 $\geq k = i + j$, אז $N \geq i$ או $N \geq j$ ואז $\varepsilon > |a_i b_j|_p$ לכל $0 \geq i,j$ כך ש$i + j = k$.
מכאן

$$\left|\sum_{i+j=k} a_i b_j\right|_p \leq \max_{i+j=k} |a_i b_j|_p < \varepsilon$$

זה מראה ש

$$\lim_{k\to\infty}\left(\sum_{i+j=k} a_i b_j\right) = 0$$

ולכן $\sum_{k=0}^{\infty}\left(\sum_{\substack{i+j=k\\ i,j\geq 0}} a_i b_j\right)$ מתכנס.
מתקיים

$$\left|\sum_{i=0}^{n}\sum_{j=0}^{\infty} a_i b_j - \sum_{k=0}^{2n}\sum_{\substack{i+j=k\\ i,j\geq 0}} a_i b_j\right|_p =$$

$$\left|a_0\sum_{j=2n+1}^{\infty} b_j + a_1\sum_{j=2n}^{\infty} b_j + \ldots + a_n\sum_{j=n+1}^{\infty} b_j\right|_p \leq \max_{\substack{1\leq i\leq n\\ 0\leq j\\ i+j>2n}} |a_i b_j|_p$$

לכן ל$N \geq n$, נקבל כי הביטוי האחרון $> \varepsilon$. ולכן

$$\left|\sum_{i=0}^{n}\sum_{j=0}^{\infty} a_i b_j - \sum_{k=0}^{2n}\sum_{\substack{i+j=k\\ i,j\geq 0}} a_i b_j\right|_p < \varepsilon$$

נשאיף $\infty \longrightarrow n$ ונקבל

$$\left|\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_i b_j - \sum_{k=0}^{\infty}\sum_{\substack{i+j=k\\ i,j\geq 0}} a_i b_j\right|_p < \varepsilon$$

לכל $0 < \varepsilon$ ולכן מתקיים השוויון המבוקש. ■

טענה 4.4 נתונה סדרה $\{a_{i_1,\dots,i_n}\}_{i_1,\dots,i_n\geq 1}$ ב-$\mathbb{C}_p$ כך שלכל $\varepsilon>0$ קיים N טבעי כך שאם $\max\{i_1,\dots,i_n\}\geq N$ אז $|a_{i_1,\dots,i_n}|_p<\varepsilon$. אז הטורים

$$\sum_{i_{\sigma(n)}=1}^{\infty}\cdots\sum_{i_{\sigma(2)}=1}^{\infty}\sum_{i_{\sigma(1)}=1}^{\infty}a_{i_1\dots i_n}$$

מתכנסים לכל תמורה $\sigma\in S_n$, ולאותו סכום.

4.2 טורי חזקות ב-$\mathbb{C}_p$ כפונקציות בעיגול ההתכנסות

יהי $\sum_{n=0}^{\infty}a_nx^n$ טור חזקות ($a_n\in\mathbb{C}_p$).

משפט 4.5 לטור החזקות הנ"ל נגדיר את המספר r לפי

$$\frac{1}{r}=\overline{\lim_{n\to\infty}}|a_n|_p^{\frac{1}{n}}$$

(כאשר הגבול הוא ב-$\mathbb{R}$, ואם אגף ימין שווה ל-0, אז $r=\infty$, ואם אגף ימין שווה ל-∞ אז $r=0$)

אז הטור מתכנס כאשר $|x|_p<r$ ומתבדר כאשר $|x|_p>r$.

הוכחה: הטור מתכנס $\iff$ $\lim_{n\to\infty}|a_nx^n|_p=0$.

נתבונן בטור הממשי $\sum_{n=0}^{\infty}|a_n|_p|x|_p^n$. מטורי חזקות מעל $\mathbb{R}$, אם $|x|_p<r$ הטור מתכנס, ובפרט $\lim_{n\to\infty}|a_n|\cdot|x|_p^n=0$. לכן הטור $\sum_{n=0}^{\infty}a_nx^n$ מתכנס ב-$\mathbb{C}_p$.

כמו כן, אנו יודעים כי כאשר $|x|_p>r$ אז הטור הממשי $\sum_{n=0}^{\infty}|a_n|_p\cdot|x|_p^n$ מתבדר מהסיבה כי $\lim_{n\to\infty}|a_n|_p\cdot|x|_p^n\neq 0$ ולכן $\sum_{n=0}^{\infty}a_nx^n$ אינו מתכנס ב-$\mathbb{C}_p$. ■

הערה 4.6 (דוגמא): כל טור ב-$\mathcal{O}_{\mathbb{C}_p}[[x]]$ מתכנס בעיגול $\mathcal{P}_{\mathbb{C}_p}$.

הערה 4.7 (דוגמא): נסתכל על הטור $\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}x^n$. אז

$$|a_n|_p^{\frac{1}{n}}=\left(\frac{1}{|n|_p}\right)^{\frac{1}{n}}$$

נכתוב $n=p^k\cdot v$ כאשר $p\nmid v$.

$$\begin{aligned}|a_n|_p^{\frac{1}{n}}&=p^{\frac{k}{n}}\\&\leq p^{\frac{\log_p n}{n}}\\&=n^{\frac{1}{n}}\underset{n\to\infty}{\longrightarrow}1\end{aligned}$$

וכיוון ש-$p^{\frac{k}{n}}\geq 1$ לכל $k\geq 0$ אז $\lim_{n\to\infty}\left(\frac{1}{|n|_p}\right)^{\frac{1}{n}}=1$

הערה 4.8 (דוגמא): נסתכל על הטור $\sum_{n=0}^{\infty}\frac{x^n}{n!}$, $a_n=\frac{1}{n!}$

$$|a_n|_p^{\frac{1}{n}} = \left(\frac{1}{|n!|_p}\right)^{\frac{1}{n}}$$

החזקה של p המחלקת את $n!$ היא $p^{\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]}$.

$$\begin{aligned} |a_n|_p^{\frac{1}{n}} &= \left(\frac{1}{|n!|_p}\right)^{\frac{1}{n}} \\ &= p^{\frac{1}{n}\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]} \\ &\leq p^{\frac{1}{n}\sum_{k=1}^{\infty}\frac{n}{p^k}} \\ &= p^{\frac{1}{p}\cdot\frac{1}{1-\frac{1}{p}}} \\ &= p^{\frac{1}{p-1}} \end{aligned}$$

נראה כי זהו אכן הגבול.
לכיוון השני: נניח כי $p^{N_n}\leq n<p^{N_n+1}$, כאשר $0\leq N_n$ שלם ($N_n=\left[\log_p n\right]$).

$$\begin{aligned} |a_n|_p^{\frac{1}{n}} &= p^{\frac{1}{n}\sum_{k=1}^{N_n}\left[\frac{n}{p^k}\right]} \\ &\geq p^{\frac{1}{n}\sum_{k=1}^{N_n}\left(\frac{n}{p^k}-1\right)} \\ &= p^{\frac{1}{n}\sum_{k=1}^{\left[\log_p n\right]}\left(\frac{n}{p^k}-1\right)} \\ &= p^{\sum_{k=1}^{\left[\log_p n\right]}\frac{1}{p^k}}\cdot p^{-\frac{\left[\log_p n\right]}{n}} \\ &\geq p^{\sum_{k=1}^{\left[\log_p n\right]}\frac{1}{p^k}}\cdot p^{-\frac{\log_p n}{n}} \end{aligned}$$

כעת $\lim_{n\to\infty}p^{-\frac{\log_p n}{n}}=1$ ו$\lim_{n\to\infty}p^{\sum_{k=1}^{\left[\log_p n\right]}\frac{1}{p^k}}=p^{\frac{1}{p-1}}$ ולכן נקבל כי

$$\lim_{n\to\infty}|a_n|_p^{\frac{1}{n}} \geq p^{\frac{1}{p-1}}$$

לכן קיים הגבול $\lim_{n\to\infty}\left(\frac{1}{|n!|_p}\right)^{\frac{1}{n}}=p^{\frac{1}{p-1}}$, ולכן רדיוס ההתכנסות של הטור הוא $r=p^{-\frac{1}{p-1}}$.

נסמן ל$a\in\mathbb{C}_p$ ו$r>0$

$$D(a,r) = \left\{x\in\mathbb{C}_p\mid |x-a|_p<r\right\}$$

טענה 4.9 נתון $f(x)=\sum_{n=0}^{\infty}a_nx^n$ בעל רדיוס התכנסות $r>0$. אז $f(x)$ מגדיר פונקציה רציפה מ$D(0,r)$ ל$\mathbb{C}_p$.

הוכחה: רציפות ב־$x=0$: נקבע $0 \neq x_0 \in D(0,r)$ ונניח כי $|x|_p \le |x_0|_p < r$. אז

$$\begin{aligned}
|f(x)-f(0)|_p &= \left|\sum_{n=1}^{\infty} a_n x^n\right|_p \\
&\le \max_{n\ge 1} |a_n x^n|_p \\
&= |x|_p \cdot \max_{n\ge 1} \left|a_n x^{n-1}\right|_p \\
&\le |x|_p \cdot \max_{n\ge 1} \left|a_n x_0^{n-1}\right|_p \underset{x\to 0}{\longrightarrow} 0
\end{aligned}$$

נניח כעת כי $0 \neq b \in D(0,r)$, נניח כי

$$|x-b|_p < |b|_p$$

אז מאי־שוויון המשולש הלא־ארכימדי

$$|x|_p \le \max\left\{|x-b|_p, |b|_p\right\} = |b|_p$$

ומאחר ו־$|b|_p, |x-b|_p$ שונים, $|x|_p = |b|_p$. לכן $|x|_p = |b|_p < r$, ולכן $x \in D(0,r)$.

$$\begin{aligned}
|f(x)-f(b)|_p &= \left|\sum_{n=1}^{\infty} a_n (x^n - b^n)\right|_p \\
&\le \max_{n\ge 1} |a_n (x^n - b^n)|_p \\
&= \max_{n\ge 1} \left(|a_n|_p \cdot |x-b|_p \cdot \left|x^{n-1} + x^{n-2}\cdot b + \ldots + b^{n-1}\right|_p\right)
\end{aligned}$$

נשים לב כי

$$\begin{aligned}
\left|\sum_{i=0}^{n-1} x^{n-i-1} b^i\right|_p &\le \max_{0\le i\le n-1} \left|x^{n-i-1}\right|_p \cdot \left|b^i\right|_p \\
&= |b|_p^{n-1}
\end{aligned}$$

לכן

$$\begin{aligned}
|f(x)-f(b)|_p &\le \max_{n\ge 1} \left(|a_n|_p \cdot |x-b|_p \cdot |b|_p^{n-1}\right) \\
&= \max_{n\ge 1} \left(|a_n|_p \cdot |b|_p^{n-1}\right) \cdot |x-b|_p \underset{x\to b}{\longrightarrow} 0
\end{aligned}$$

■

טענה 4.10

1. בסימונים הקודמים, $f(x)$ גזירה במובן שלכל $b \in D(0,R)$ קיים

$$\lim_{x\to b}\frac{f(x)-f(b)}{x-b} = f'(b)$$

2. רדיוס ההתכנסות של $\sum_{n=1}^{\infty} na_n x^{n-1}$ הוא r ומתקיים $f'(x)=\sum_{n=1}^{\infty} na_n x^{n-1}$ לכל $x \in D(0,r)$.

הוכחה: נניח כי $0 \neq b \in D(0,r)$ ונניח כי $|b|_p < |x-b|_p$ (ולכן $|x|_p = |b|_p < r$). אז

$$f(x)-f(b) = (x-b)\left(\sum_{n=1}^{\infty} a_n\left(\sum_{i=0}^{n-1} b^{n-i-1}x^i\right)\right)$$

נגדיר

$$a_{n,i}(x) = \begin{cases} a_n b^{n-1-i}x^i & 0\le i\le n-1\\ 0 & i\ge n\end{cases}$$

אז

$$f(x)-f(b) = (x-b)\sum_{n=1}^{\infty}\sum_{i=0}^{\infty} a_{n,i}(x)$$

מתקיים

$$|a_{n,i}(x)|_p = \begin{cases} |a_n|_p\,|b|_p^{n-1} & 0\le i\le n-1\\ 0 & i\ge n\end{cases}$$

ולכן לכל $\varepsilon > 0$, כשניקח N טבעי כל שלכל $n \ge N$

$$\begin{aligned}\frac{1}{|b|_p}\cdot|a_nb^n|_p &= \left|a_nb^{n-1}\right|_p\\ &< \varepsilon\end{aligned}$$

(מאחר והטור מתכנס, $|a_nb^n|_p \underset{n\to\infty}{\longrightarrow} 0$)
ולכן לכל $n \ge N$ ולכל $i \ge 0$

$$|a_{n,i}(x)| < \varepsilon$$

לכן $\lim_{n\to\infty} a_{n,i}(x) = 0$ במידה שווה ב-i.
כמובן, כאשר n קבוע, $\lim_{i\to\infty} a_{n,i}(x) = 0$ שהרי $a_{n,i}(x)=0$ לכל $i \ge n$.

מכאן

$$\begin{aligned}\sum_{n=1}^{\infty}\sum_{i=0}^{\infty}a_{n,i}(x) &= \sum_{i=0}^{\infty}\sum_{n=1}^{\infty}a_{n,i}(x)\\ &= \sum_{i=0}^{\infty}\left(\sum_{n=i+1}^{\infty}a_nb^{n-1-i}\right)x^i\\ &= \sum_{i=0}^{\infty}\left(\underbrace{\sum_{n=0}^{\infty}a_{n+i+1}b^n}_{c_i}\right)x^i\\ &= \sum_{i=0}^{\infty}c_ix^i\underset{x\to b}{\longrightarrow}\sum_{i=0}^{\infty}c_ib^i\end{aligned}$$

זה מוכיח קיום הגבול. נחשב $\sum_{i=0}^{\infty}c_ib^i$:

$$\begin{aligned}\sum_{i=0}^{\infty}c_ib^i &= \sum_{i=0}^{\infty}\sum_{n=1}^{\infty}a_{n,i}(b)\\ &= \sum_{n=1}^{\infty}\sum_{i=0}^{\infty}a_{n,i}(b)\\ &= \sum_{n=1}^{\infty}\sum_{i=0}^{n-1}a_nb^{n-1-i}b^i\\ &= \sum_{n=1}^{\infty}\sum_{i=0}^{n-1}a_nb^{n-1}\\ &= \sum_{n=1}^{\infty}na_nb^{n-1}\end{aligned}$$

נחשב את רדיוס ההתכנסות של $\sum_{n=1}^{\infty}na_nx^{n-1}=\sum_{n=0}^{\infty}(n+1)a_{n+1}x^n$

$$\begin{aligned}|(n+1)\cdot a_{n+1}|_p^{\frac{1}{n}} &= |(n+1)\cdot a_{n+1}|_p^{\frac{1}{n+1}\cdot\frac{n+1}{n}}\\ &= \left(|n+1|_p^{\frac{1}{n+1}}\cdot|a_{n+1}|_p^{\frac{1}{n+1}}\right)^{\frac{n+1}{n}}\end{aligned}$$

ראינו קודם כי $|n+1|_p^{\frac{1}{n+1}}\underset{n\to\infty}{\longrightarrow}1$. בנוסף, $\overline{\lim}_{n\to\infty}|a_{n+1}|_p^{\frac{1}{n+1}}=\frac{1}{r}$ ו $\frac{n+1}{n}\underset{n\to 1}{\longrightarrow}1$ ולכן

$$\begin{aligned}\overline{\lim}_{n\to\infty}|(n+1)\cdot a_{n+1}|_p^{\frac{1}{n}} &= \overline{\lim}_{n\to\infty}|a_n|_p^{\frac{1}{n}}\\ &= \frac{1}{r}\end{aligned}$$

■

משפט 4.11 (שטרסמן): נתון

$$0 \neq f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}_p[[x]]$$

נניח כי $a_n \xrightarrow[n\to\infty]{} 0$. לכן הטור מתכנס ב-$\mathcal{O}_{\mathbb{C}_p}$. נגדיר N טבעי לפי $\max_{n\geq 0}|a_n|_p = |a_N|_p$ ו-$|a_N|_p > |a_n|_p$ לכל $n > N$. אז ל-$f(x)$, כפונקציה על $\mathcal{O}_{\mathbb{C}_p}$, יש לכל היותר N אפסים (ב-$\mathcal{O}_{\mathbb{C}_p}$).

הוכחה: באינדוקציה על N. נניח כי $N = 0$. לכן $|a_0|_p > |a_n|_p$ לכל $n \geq 1$. נניח כי $\alpha \in \mathcal{O}_{\mathbb{C}_p}$ הוא אפס של $f(x)$. אז

$$\begin{aligned} f(\alpha) &= 0 \\ a_0 &= -\sum_{n=1}^{\infty} a_n \alpha^n \end{aligned}$$

ולכן

$$\begin{aligned} |a_0|_p &\leq \max_{n\geq 1}|a_n\alpha^n|_p \\ &\underbrace{\leq}_{|\alpha|_p<1} \max_{n\geq 1}|a_n|_p \\ &< |a_0|_p \end{aligned}$$

סתירה.

נניח כי $N \geq 1$. יהי $\alpha \in \mathcal{O}_{\mathbb{C}_p}$ אפס של $f(x)$.

$$\begin{aligned} f(x) &= f(x) - f(\alpha) \\ &= \sum_{n=1}^{\infty} a_n (x^n - \alpha^n) \\ &= (x-\alpha)\sum_{n=1}^{\infty} c_i x^i \end{aligned}$$

כאשר המעבר האחרון הוא כמו בהוכחה הקודמת, ו-$c_i = \sum_{i=0}^{\infty} a_{n+i+1}\alpha^n$.
נראה כי $\sum_{i=0}^{\infty} c_i x^i$ מקיים את תנאי המשפט עם $N-1$ במקום N.

$$\begin{aligned} |c_i|_p &\leq \max_{n\geq 0}|a_{n+i+1}\alpha^n|_p \\ &\leq \max_{n\geq 0}|a_{n+i+1}|_p \\ &= \max_{n>i}|a_n|_p \xrightarrow[i\to\infty]{} 0 \end{aligned}$$

כמו כן

$$\begin{aligned} |c_i|_p &\leq \max_{n\geq 0}|a_{n+1+i}|_p \\ &\leq |a_N|_p \end{aligned}$$

בנוסף

$$\begin{aligned} \left|c_{N-1}\right|_p &= \left|\sum_{n=0}^{\infty} a_{n+N}\alpha^n\right|_p \\ &= \left|a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 \ldots +\right|_p \\ &= \left|a_N\right|_p \end{aligned}$$

כי לכל $j \geq 1$

$$\begin{aligned} \left|a_{N+j}\alpha^j\right|_p &\leq \left|a_{N+j}\right|_p \\ &< \left|a_N\right|_p \end{aligned}$$

נניח כי $N' > N - 1$ אז $N' \geq N$ ומתקיים

$$\left|C_{N'}\right|_p = \left|a_{N'+1} + a_{N'+2}\alpha + \ldots\right|_p$$

לכל המחוברים יש ערך מוחלט $< \left|a_N\right|_p$.

מהנחת האינדוקציה, יש ל$\sum_{i=0}^{\infty} c_i x^i$ לכל היותר $N-1$ אפסים ב$\mathcal{O}_{\mathbb{C}_p}$. ■

מסקנה 4.12 (מההוכחה): יהי

$$0 \neq f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}_p[[x]]$$

כך ש$a_n \underset{n\to\infty}{\longrightarrow} 0$. אז ל$f(x)$, כפונקציה על $\mathcal{O}_{\mathbb{C}_p}$, יש מספר סופי של אפסים. נניח כי אלה הם (כולל הריבוי) $\alpha_1, \ldots, \alpha_m$. אז יש פירוק

$$f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_m)\, g(x)$$

כאשר $g(x) \in \mathbb{C}_p[[x]]$ מתכנס ב$\mathcal{O}_{\mathbb{C}_p}$ ואינו מתאפס שם.

4.3 הפונקציה המעריכית והפונקציה הלוגריתמית

ל$x \in D\left(0, p^{-\frac{1}{p=1}}\right)$ נגדיר $\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$

ל$x \in D(0,1)$ נגדיר $\mathrm{Log}_p(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} x^n}{n}$

טענה 4.13 לכל $x, y \in \mathbb{C}_p$ כך ש $|x|_p, |y|_p < 1$ מתקיים $\exp_p(x+y) = \exp_p(x) \cdot \exp_p(y)$.

הוכחה:

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

כאשר המעבר האחד לפני האחרון הוא מהלמה על מכפלת טורים. ■

משפט 4.14 לכל $x,y\in\mathbb{C}_p$ כך ש $|x|_p\,,|y|_p<1$ מתקיים

$$\operatorname{Log}_p((1+x)(1+y)) = \operatorname{Log}_p(1+x)+\operatorname{Log}_p(1+y)$$

הוכחה:

$$\begin{aligned}
\operatorname{Log}_p((1+x)(1+y)) &= \operatorname{Log}_p(1+x+y+xy)\\
&= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}(x+y+xy)^n\\
&= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\sum_{k_1=0}^{n}\binom{n}{k_1}(x+y)^{n-k_1}(xy)^{k_1}\\
&= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\sum_{k_1=0}^{n}\binom{n}{k_1}\sum_{k_2=0}^{n}\binom{n-k_1}{k_2}\underbrace{x^{k_2}y^{n-k_1-k_2}(xy)^{k_1}}_{x^{k_1+k_2}y^{n-k_1}}
\end{aligned}$$

נסמן $k_1+k_2=i$,$n-k_2=j$ אז $k_2=n-j$,$n+k_1=i+j$ ו$k_1=i+j-n$.

$$\begin{aligned}
\operatorname{Log}_p((1+x)(1+y)) &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\sum_{\substack{0\le i,j\le n\\ n\le i+j}}\binom{n}{i+j-n}\binom{2n-i-j}{n-j}x^i y^j\\
&= \sum_{n=1}^{\infty}\sum_{i=0}^{n}\sum_{j=0}^{n}a_{i,j,n}
\end{aligned}$$

כאשר

$$a_{i,j,n} = \begin{cases}\frac{(-1)^{n+1}}{n}\binom{n}{i+j-n}\binom{2n-i-j}{n-j}x^i y^j & \begin{cases}0\le i,j\le n\\ i+j\ge n\end{cases}\\ 0 & \text{otherwise}\end{cases}$$

נניח כי $1 > |y|_p \leq |x|_p$. לכל $\varepsilon > 0$ קיים N כך שלכל $n \geq N$ מתקיים $\left|\frac{y^n}{n}\right|_p < \varepsilon$. נראה כי

$$\max\{i,j,n\} \geq N \quad \Longrightarrow \quad |a_{i,j,n}|_p < \varepsilon$$

אם $i > n$ או $j > n$ אז $a_{i,j,n} = 0$. נניח $i,j \leq n$. אם $i + j < n$ אז $a_{i,j,n} = 0$. נניח $i + j \geq n$, אז

$$\max\{i,j,n\} = n$$

$$\begin{aligned}
|a_{i,j,n}|_p &\leq \left|\frac{x^i y^j}{n}\right|_p \\
&\leq \frac{|y|_p^{i+j}}{|n|_p} \\
&\underbrace{\leq}_{\substack{i+j\geq n \\ |y|_p<1}} \frac{|y|_p^n}{|n|_p} \\
&= \left|\frac{y^n}{n}\right|_p \\
&< \varepsilon
\end{aligned}$$

לכן אפשר להחליף סדר סכום

$$\begin{aligned}
\mathrm{Log}_p\left((1+x)(1+y)\right) &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\underbrace{\sum_{n=\max\{i,j\}}^{i+j}\frac{(-1)^{n+1}}{n}\binom{n}{i+j-n}\binom{2n-i-j}{n-j}}_{b_{ij}\in\mathbb{Q}} x^i y^j \\
&= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} b_{ij} x^i y^j
\end{aligned}$$

כאשר $b_{ij} \in \mathbb{Q}$.

במספרים הממשיים מתקיים

$$\ln\left((1+u)(1+v)\right) = \ln(1+u) + \ln(1+v)$$

וניתן להראות שגם בממשיים

$$\ln\left((1+u)(1+v)\right) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} b_{ij} u^i v^j$$

לכן בממשיים מתקיים כי

$$\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} b_{ij} x^i y^j = \sum_{i=1}^{\infty}\frac{(-1)^{i+1}}{i}u^i + \sum_{i=1}^{\infty}\frac{(-1)^{i+1}}{i}v^i$$

ע"י השוואת מקדמים נסיק כי $b_{ij}=0$ כאשר $i,j\geq 1$ וכי $b_{i0}=\frac{(-1)^{i+1}}{i}$ ו $b_{0j}=\frac{(-1)^{j+1}}{j}$.
לכן

$$\begin{aligned}\mathrm{Log}_p\left((1+x)(1+y)\right) &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} b_{ij}x^i y^j \\ &= \sum_{i=0}^{\infty} b_{i0}x^i + \sum_{j=0}^{\infty} b_{0j}y^j \\ &= \mathrm{Log}_p(1+x) + \mathrm{Log}_p(1+y)\end{aligned}$$

■

למה 4.15 יהי $\zeta\in\overline{\mathbb{Q}}_p$ שורש יחידה מסדר p^m. אז

$$|\zeta-1|_p < 1$$

הוכחה:

$$(\zeta-1)^{p^m} = \zeta^{p^m}+(-1)^{p^m}+\sum_{k=1}^{p^m-1}(-1)^{p^m-k}\cdot\binom{p^m}{k}\cdot\zeta^k$$

אנו יודעים כי $p\mid\binom{p^m}{k}$ לכל $1\leq k\leq m$. אם $p\geq 3$ קיבלנו,

$$(\zeta-1)^{p^m} = \sum_{k=1}^{p^m-1}(-1)^{p^m-k}\cdot\binom{p^m}{k}\cdot\zeta^k$$

ואז

$$\begin{aligned}|\zeta-1|_p^{p^m} &\leq \max_{1\leq k<p^m}\left|\binom{p^m}{k}\right|_p \\ &< 1\end{aligned}$$

ולכן

$$|\zeta-1|_p < 1$$

אם $p=2$:

$$(\zeta-1)^{2^m} = 2+\sum_{k=1}^{2^m-1}(-1)^k\cdot\binom{2^m}{k}\cdot\zeta^k$$

ואז

$$\begin{aligned}|\zeta-1|_2^{2^m} &\leq \max\left\{|2|_2\,,\max_{1\leq k<2^m}\left|\binom{2^m}{k}\right|_2\right\} \\ &< 1\end{aligned}$$

ולכן

$$|\zeta-1|_2 \quad < \quad 1$$

■

מסקנה 4.16 יהי $\zeta\in\overline{\mathbb{Q}}_p$ שורש יחידה מסדר p^m, אז $\mathrm{Log}_p\zeta$ מוגדר ומתקיים $\mathrm{Log}_p\zeta=0$.

הוכחה: $|\zeta-1|_p<1$ ולכן $\mathrm{Log}_p\left(1+(\zeta-1)\right)$ מוגדר

$$\begin{aligned}\mathrm{Log}_p 1 &= \mathrm{Log}_p\left(\zeta^{p^m}\right)\\ &= p^m\mathrm{Log}\left(\zeta\right)\end{aligned}$$

אבל

$$\begin{aligned}\mathrm{Log}_p 1 &= \mathrm{Log}_p\left(1+0\right)\\ &= \sum_{n=1}^{\infty}\frac{(-1)^n}{n}x^n\mid_{x=0}\\ &= 0\end{aligned}$$

ולכן

$$p^m\mathrm{Log}\left(\zeta\right) \quad = \quad 0$$

כלומר $\mathrm{Log}\left(\zeta\right)=0$. ■

הערה 4.17 (דוגמא): $p=2$, $\zeta=-1$ לכן

$$\mathrm{Log}_p\left(\zeta\right) \quad = \quad 0$$

לכן $0=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}(-2)^n}{n}$ ב-$\mathbb{C}_2$ (וגם ב-$\mathbb{Q}_2$). לכן $\sum_{n=1}^{\infty}\frac{2^n}{n}=0$ ב-$\mathbb{Q}_2$.
לכן לכל m טבעי קיים N טבעי כך שלכל $n\geq N$,

$$\left|\sum_{k=1}^{n}\frac{2^k}{k}\right|_2 \quad \leq \quad 2^{-m}$$

זה אומר שכאשר מסתכלים בסכום $2+2+\frac{2^3}{3}+\frac{2^4}{4}+\ldots+\frac{2^n}{n}$ ורושמים אותו כמנה מצומצמת של טבעיים, אז המונה מתחלק ב-2^m.

למה 4.18 נניח כי $|x|_p<p^{-\frac{1}{p-1}}$ אז

$$\begin{aligned}\left|\exp_p\left(x\right)-1\right|_p &< p^{-\frac{1}{p-1}}\\ \left|\mathrm{Log}\left(1+x\right)\right|_p &< p^{-\frac{1}{p-1}}\end{aligned}$$

הוכחה:

$$\begin{aligned}\left|\exp_p(x)-1\right|_p &= \left|\sum_{n=1}^{\infty}\frac{x^n}{n!}\right|_p\\ &\le \max_{n\ge 1}\left|\frac{x^n}{n!}\right|_p\\ &\le \max_{n\ge 1}\frac{|x^n|_p}{|n!|_p}\end{aligned}$$

חישבנו קודם

$$\left|\frac{1}{n!}\right|_p = p^{\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]}$$

נרשום $n=p^l\cdot v$ כאשר $p\nmid v$ ונניח כי $p^N\le v<p^{N+1}$. אז מתקיים

$$\begin{aligned}\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] &= \sum_{k=1}^{l}\left[\frac{p^l\cdot v}{p^k}\right]+\sum_{k=1}^{N}\left[\frac{p^l\cdot v}{p^{l+k}}\right]\\ &= \sum_{k=1}^{l}p^{l-k}\cdot v+\left[\frac{v}{p}\right]+\left[\frac{v}{p^2}\right]+\ldots+\left[\frac{v}{p^N}\right]\\ &\le v\cdot\frac{p^l-1}{p-1}+\frac{v}{p}\cdot\left(1+\frac{1}{p}+\ldots+\frac{1}{p^{N-1}}\right)\\ &= v\cdot\frac{p^l-1}{p-1}+\frac{v}{p}\cdot\frac{1-\frac{1}{p^N}}{1-\frac{1}{p}}\\ &= v\cdot\frac{p^l-1}{p-1}+v\cdot\frac{1-\frac{1}{p^N}}{p-1}\\ &= \frac{v}{p-1}\left(p^l-1+1-\frac{1}{p^N}\right)\\ &= \frac{v}{p-1}\left(p^l-\frac{1}{p^N}\right)\\ &= \frac{n-\frac{v}{p^N}}{p-1}\\ &\le \frac{n-1}{p-1}\end{aligned}$$

ולכן $\left|\frac{1}{n!}\right|_p\le p^{\frac{n-1}{p-1}}$. נקבל לכן כי

$$\begin{aligned}\left|\frac{x^n}{n!}\right|_p &< p^{-\frac{n}{n-1}+\frac{n-1}{p-1}}\\ &= p^{-\frac{1}{p-1}}\end{aligned}$$

באשר ללוגריתם:

$$\begin{aligned}\left|\mathrm{Log}_p(1+x)\right|_p &= \left|\sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}\right|_p \\ &\le \max_{n\ge 1}\left|\frac{x^n}{n}\right|_p\end{aligned}$$

נרשום, כמו קודם, $n=p^l\cdot v$.

$$\begin{aligned}\left|\frac{x^n}{n}\right|_p &= |x|_p^n\cdot p^l \\ &< p^{-\frac{n}{p-1}+l} \\ &\le p^{\log_p n-\frac{n}{p-1}}\end{aligned}$$

נגדיר את הפונקציה

$$g(t) = \log_p t-\frac{t-1}{p-1}$$

לו $t\ge 1$.
נגזור ונחפש נקודות קיצון:

$$g'(t) = \frac{1}{t\ln p}-\frac{1}{p-1}$$

נקבל כי יש נקודת מקסימום יחידה כאשר $1<t=\frac{p-1}{\ln p}<p$.
לכן לכל $n\ge p$ מתקיים

$$g(n) \le g(p)=0$$

כלומר $\log_p n-\frac{n}{p-1}<-\frac{1}{p-1}$ ולכן

$$\left|\frac{x^n}{n}\right|_p < p^{-\frac{1}{p-1}}$$

לכל $n\ge p$.
כאשר $1\le n<p$, n זר ל-p ולכן

$$\begin{aligned}\left|\frac{x^n}{n}\right|_p &= |x|_p^n \\ &< p^{-\frac{n}{p-1}} \\ &\le p^{-\frac{1}{p-1}}\end{aligned}$$

לכן

$$\begin{aligned}\left|\mathrm{Log}_p(1+x)\right|_p &\le \max_{n\ge 1}\left|\frac{x^n}{n}\right|_p \\ &< p^{-\frac{1}{p-1}}\end{aligned}$$

■

טענה 4.19 נניח כי $|x|_p < p^{-\frac{1}{p-1}}$, אז

$$\mathrm{Log}_p\left(\exp_p(x)\right) = x$$

הוכחה:

$$\exp_p(x) = 1 + \left(\exp_p(x) - 1\right)$$

ומהלמה הקודמת, הLog_p מוגדר, כלומר $\mathrm{Log}_p\left(\exp_p(x)\right)$ מוגדר.

$$\begin{aligned}\mathrm{Log}_p\left(\exp_p(x)\right) &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\left(\exp_p(x)-1\right)^n\\ &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\left(\sum_{k=1}^{\infty}\frac{x^k}{k!}\right)^n\\ &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\sum_{k=1}^{\infty}\left(\sum_{\substack{m_1+\ldots+m_n=k\\ m_i\geq 1}}\frac{x^k}{m_1!\cdot\ldots\cdot m_n!}\right)\end{aligned}$$

נגדיר

$$c_{k,n} = \begin{cases}\frac{(-1)^{n+1}}{n}\sum_{\substack{m_1+\ldots+m_n=k\\ m_i\geq 1}}\frac{1}{m_1!\cdot\ldots\cdot m_n!} & k\geq n\\ 0 & k<n\end{cases}$$

לכן

$$\mathrm{Log}_p\left(\exp_p(x)\right) = \sum_{n=1}^{\infty}\sum_{k=1}^{\infty}c_{k,n}x^k$$

$$\left|\sum_{\substack{m_1+\ldots+m_n=k\\ m_i\geq 1}}\frac{1}{m_1!\cdot\ldots\cdot m_n!}\right|_p \leq \max_{\substack{m_1+\ldots+m_n=k\\ m_i\geq 1}}\prod_{i=1}^{n}\left|\frac{1}{m_i!}\right|_p$$

נשים לב כי

$$\begin{aligned}\prod_{i=1}^{n}\left|\frac{1}{m_i!}\right|_p &\leq \prod_{i=1}^{n}p^{\frac{m_i-1}{p-1}}\\ &= p^{\frac{k-n}{p-1}}\end{aligned}$$

כי ראינו קודם כי $\left|\frac{1}{n}\right|_p \le p^{\frac{n-1}{p-1}}$ (באמצעות הפונקציה $g(t)$)
ואז

$$\begin{aligned}\left|c_{k,n}x^k\right| &< \left|\frac{1}{n}\right|_p \cdot p^{\frac{k-n}{p-1}} \cdot \left|x^k\right|_p \\ &\le p^{\frac{n-1}{p-1}} \cdot p^{\frac{k-n}{p-1}} \cdot \left|x^k\right|_p \\ &= p^{\frac{n-1}{p-1}+\frac{k-n}{p-1}} \cdot \left|x^k\right|_p \\ &= p^{\frac{k-1}{p-1}} \cdot |x|_p^k \\ &= \left(p^{\frac{1}{p-1}} \cdot |x|_p\right)^k \cdot p^{-\frac{1}{p-1}} \underset{k\to\infty}{\longrightarrow} 0\end{aligned}$$

כי $|x|_p < p^{-\frac{1}{p-1}}$. זו, כמובן, שאיפה במידה שווה בn. כעת מתנאי הלמה, ניתן להחליף את סדר הסכימה:

$$\begin{aligned}\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} c_{k,n}x^k &= \sum_{k=1}^{\infty}\sum_{n=1}^{\infty} c_{k,n}x^k \\ &= \sum_{k=1}^{\infty}\underbrace{\left(\sum_{n=1}^{k}\frac{(-1)^{n+1}}{n}\sum_{\substack{m_1+\ldots+m_n=k\\ m_i\ge 1}}\frac{1}{m_1!\cdot\ldots\cdot m_n!}\right)}_{c_k\in\mathbb{Q}}x^k\end{aligned}$$

בממשיים מתקיים $\ln(e^u) = u$ בתחום בו $|e^u - 1| < 1$. ואז $\sum_{k=1}^{\infty} c_k u^k = u$ ולכן $c_k = 0$ לכל $k \ge 2$ ו$c_1 = 1$. ולכן

$$\mathrm{Log}_p\left(\exp_p(x)\right) = x$$

■

טענה 4.20 (תרגיל) גם $\exp_p\left(\mathrm{Log}_p(1+x)\right) = 1+x$.

מסקנה 4.21 למשוואה $\mathrm{Log}_p(1+x) = 0$ יש פתרון יחיד עבור $|x|_p < p^{-\frac{1}{p-1}}$ והוא $x = 0$.

הוכחה: ההעתקות $\mathrm{Log}_p(y) : D\left(1, p^{-\frac{1}{p-1}}\right) \to D\left(0, p^{-\frac{1}{p-1}}\right)$
ו$\exp_p(x) : D\left(0, p^{-\frac{1}{p-1}}\right) \to D\left(1, p^{-\frac{1}{p-1}}\right)$ הפוכות זו לזו (בתחומים המצוינים). לכן יש מקור יחיד ל$0 \in D\left(0, p^{-\frac{1}{p-1}}\right)$. ■

טענה 4.22 נסמן $f(x) = \mathrm{Log}_p(1-px)$ ל$|x|_p \le 1$. אז

1. כאשר $p \ne 2$ יש ל$f(x)$ אפס יחיד ב$\mathcal{O}_{\mathbb{C}_p}$ והוא $x = 0$.
2. כאשר $p = 2$ יש ל$f(x)$ בדיוק שני אפסים ב$\mathcal{O}_{\mathbb{C}_p}$.

הוכחה: אם $p\neq 2$, אז נשים לב כי $|px|_p=p^{-1}|x|_p\leq p^{-1}<p^{-\frac{1}{p-1}}$ (כי $p\geq 3$) ולכן הטענה נובעת מהמסקנה הקודמת.
אם $p=2$ אז

$$\begin{aligned}|px|_p &= |2x|_2\\ &= \frac{1}{2}|x|_2\\ &\leq \frac{1}{2}\end{aligned}$$

מתקיים

$$\begin{aligned}\mathrm{Log}_2(1-2x) &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}(-2x)^n\\ &= -\sum_{n=1}^{\infty}\frac{2^n}{n}x^n\end{aligned}$$

נעריך

$$\begin{aligned}\left|\frac{2^n}{n}\right|_2 &= \frac{2^{-n}}{|n|_2}\\ &\leq 2^{-n+\log_2 n}\underset{n\to\infty}{\longrightarrow}0\end{aligned}$$

מתקיים $\log_2(n)\leq n-1$ לכל n טבעי (ראינו זאת ע"י חקירת $g(t)=\log_2 t-(t-1)$).
לכן

$$\left|\frac{2^n}{n}\right|_2 \leq 2^{-n+n-1}=2^{-1}$$

מתקיים $\log_2(n)<n-1$ לכל $n\geq 3$ טבעי וכאשר $n=1,2$ מקבלים שוויון:

$$\begin{aligned}\left|\frac{2}{1}\right|_2 &= \left|\frac{2^2}{2}\right|_2\\ &= \frac{1}{2}\end{aligned}$$

לכן

$$\max_{n\geq 1}\left|\frac{2^n}{n}\right| = \frac{1}{2}$$

ולכן $N=2$ (כאשר N האינדקס במשפט שטרסמן)
ממשפט שטרסמן, יש ל $\sum_{n=1}^{\infty}\frac{2^n}{n}x^n$ ב$\mathcal{O}_{\mathbb{C}_2}$ לכל היותר $N=2$ אפסים. כיוון ש$x=0,1$ הם אפסים, ל$f(x)$ יש בדיוק שני אפסים ב$\mathcal{O}_{\mathbb{C}_2}$. ■

מסקנה 4.23 אם ζ שורש יחידה מסדר p^m אז $p^{-\frac{1}{p-1}}\leq|\zeta-1|_p<1$

הוכחה: ראינו כי $\left|\zeta-1\right|_p<1$. ראינו גם $\mathrm{Log}_p\left(\zeta\right)=0$ ולכן מאחר ויש שורש יחיד ל$\mathrm{Log}_p\left(1+x\right)$ עבור $\left|x\right|_p<p^{-\frac{1}{p-1}}$ והוא $x=0$, נסיק כי $\left|\zeta-1\right|_p\leq p^{-\frac{1}{p-1}}$. ■

טענה 4.24 נניח כי ζ שורש יחידה פרימיטיבי מסדר m, שאינו חזקת p. אז $\left|\zeta-1\right|_p=1$.

הוכחה: בשלילה, נניח כי $\left|\zeta-1\right|_p<1$. כלומר, $\zeta\in1+\mathcal{P}_{\mathbb{C}_p}$ ולכן $\zeta^i\in1+\mathcal{P}_{\mathbb{C}_p}$ לכל i טבעי, כלומר $\left|\zeta^i-1\right|_p<1$ לכל i טבעי.

יהי $l\geq2$ טבעי הזר לp כך ש$l\mid m$. נסמן $\xi=\zeta^{\frac{m}{l}}$. אז ξ שורש יחידה פרימיטיבי מסדר l (זר לp) ומתקיים $\left|\xi-1\right|_p<1$.

$$\begin{aligned}0&=\xi^l-1\\&=\left(1+\left(\xi-1\right)\right)^l-1\\&=\sum_{j=1}^{l}\binom{l}{j}\left(\xi-1\right)^j\end{aligned}$$

נחלק ב$\xi-1$ ונקבל

$$l=-\sum_{j=2}^{l}\binom{l}{j}\left(\xi-1\right)^{j-1}$$

נקבל

$$\begin{aligned}1&=\left|l\right|_p\\&\leq\max_{2\leq j\leq l}\left(\underbrace{\left|\binom{l}{j}\right|_p}_{\leq1}\cdot\left|\xi-1\right|_p^{j-1}\right)\\&\leq\max_{1\leq j\leq l-1}\left|\xi-1\right|_p^j\\&<1\end{aligned}$$

סתירה. ■

משפט 4.25 קיימת הרחבה יחידה לLog_px מ$D\left(1,1\right)$ לכל $\mathbb{C}_p^*$ כך ש

$$\mathrm{Log}_p\left(xy\right)=\mathrm{Log}_p\left(x\right)+\mathrm{Log}_p\left(y\right)$$

לכל $x,y\in\mathbb{C}_p^*$ ו

$$\mathrm{Log}_p\left(p\right)=0$$

כמו כן $\mathrm{Log}_p\left(x\right)$ היא אנליטית מקומית, במובן שלכל $x_0\in\mathbb{C}_p$ יש עיגול פתוח סביב x_0, שם Log_px שווה לטור חזקות מתכנס. מתקיים $\left(\mathrm{Log}_px\right)'=\frac{1}{x}$ לכל $x\in\mathbb{C}_p$.

הוכחה: נניח כי יש הרחבה כזאת. יהי $0 \neq x \in \mathbb{C}_p$. ראינו כי אפשר להציג

$$x = p^r \cdot \zeta \cdot (1+u)$$

כאשר $r = \nu_p(x) \in \mathbb{Q}$, $r = \frac{a}{b}$, a שלם, b טבעי, וp^r הוא שורש של הפולינום $t^b - p^a$, כלומר

$$(p^r)^b = p^a$$

וζ הוא שורש יחידה מסדר $p^f - 1$ כאשר $f \geq 0$, ו$|u|_p < 1$.
מתקיים

$$\begin{aligned}(p^r)^b &= p^a \\ b\text{Log}_p(p^r) &= a\text{Log}_p p \\ &= 0\end{aligned}$$

ולכן

$$\text{Log}_p(p^r) = 0$$

בנוסף

$$\begin{aligned}0 &= \text{Log}_p(1) \\ &= \text{Log}_p\left(\zeta^{p^f-1}\right) \\ &= \left(p^f-1\right)\text{Log}_p(\zeta)\end{aligned}$$

ולכן

$$\text{Log}_p(\zeta) = 0$$

ואז נקבל

$$\begin{aligned}\text{Log}_p(x) &= \text{Log}_p(1+u) \\ &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}u^n}{n}\end{aligned}$$

נראה כעת כי אין תלות בייצוג שבחרנו: יהי

$$x = (p^r)' \cdot \zeta' \cdot (1+v)$$

ייצוג נוסף (כאשר $(p^r)'$ הוא שורש אחר של הפולינום $t^b - p^a = 0$)
מתקיים

$$\left((p^r)'\right)^b = p^a$$

ולכן יש שורש יחידה מסדר b, ω, כך ש

$$(p^r)' = \omega \cdot p^r$$

ומתקיים

$$\omega\cdot\zeta'\cdot(1+v) \quad=\quad \zeta\cdot(1+u)$$

ולכן

$$\begin{aligned}\frac{1+u}{1+v} &= \omega\cdot\zeta'\cdot\zeta^{-1}\\ &= \zeta''\end{aligned}$$

כאשר ζ'' שורש יחידה.

$$\begin{aligned}\left|\frac{1+u}{1+v}-1\right|_p &= \left|\frac{u-v}{1+v}\right|_p\\ &= |u-v|_p\\ &< 1\end{aligned}$$

מהטענה הקודמת, ζ'' הוא שורש יחידה מסדר שהוא חזקת p (לא ברור למה ζ'' הוא שורש פרימיטיבי. ציינו בכיתה שהטענה נכונה גם לשורש שאינו פרימיטיבי אם הוא מסדר שאינו חזקה של p, אבל נראה לי שלא צריך את העובדה הזאת בהמשך).
כאן כבר ראינו כי $\mathrm{Log}_p\left(\zeta''\right)=0$ (נתון ע"י הטור המתכנס). כלומר,

$$\begin{aligned}\mathrm{Log}_p\left(1+u\right) &= \mathrm{Log}_p\left(\zeta''\left(1+v\right)\right)\\ &= \underbrace{\mathrm{Log}_p\left(\zeta''\right)}_{0}+\mathrm{Log}_p\left(1+v\right)\\ &= \mathrm{Log}_p\left(1+v\right)\end{aligned}$$

כי הוכחנו כי השוויון הנ"ל נכון בתחום ההתכנסות.
לכן ההגדרה

$$\mathrm{Log}_p x \quad=\quad \mathrm{Log}_p\left(1+u\right)$$

כאשר $x=p^r\zeta\left(1+u\right)$ היא טובה (ובפרט מקיימת $\mathrm{Log}_p p=0$).
נניח כי $x,y\in\mathbb{C}_p^*$ ו

$$\begin{aligned}x &= p^r\zeta\left(1+u\right)\\ y &= p^s\xi\left(1+v\right)\end{aligned}$$

פירוקים כנ"ל. נכתוב $r=\frac{a}{b}$, $s=\frac{c}{d}$ כאשר a,c שלמים, b,d טבעיים.

$$\begin{aligned}\left(p^r\cdot p^s\right)^{bd} &= \left(\left(p^r\right)^b\right)^d\cdot\left(\left(p^s\right)^d\right)^b\\ &= p^{ad}\cdot p^{cb}\\ &= p^{ad+bc}\end{aligned}$$

לכן אפשר לבחור p^{r+s} כ־$p^r\cdot p^s$ כי

$$\begin{aligned}r+s &= \frac{a}{b}+\frac{c}{d}\\ &= \frac{ad+bc}{bd}\end{aligned}$$

נניח כי ζ שורש יחידה מסדר p^f-1 ו־ξ שורש יחידה מסדר p^t-1. כיוון ש־$p^f-1, p^t-1 \mid p^{ft}-1$ מתקיים כי $\zeta\cdot\xi$ שורש יחידה מסדר $p^{ft}-1$.

$$xy = \left(p^r p^s\right)\cdot(\zeta\cdot\xi)\cdot(1+u)(1+v)$$

ואז

$$\begin{aligned}\mathrm{Log}_p(xy) &= \mathrm{Log}_p((1+u)(1+v))\\ &= \mathrm{Log}_p(1+u)+\mathrm{Log}_p(1+v)\\ &= \mathrm{Log}_p(x)+\mathrm{Log}_p(y)\end{aligned}$$

נניח כי $0\neq x_0\in\mathbb{C}_p$. נתבונן בעיגול

$$D\left(x_0,|x_0|_p\right) = \left\{x \mid |x-x_0|_p<|x_0|_p\right\}$$

מתקיים כי $\left|\frac{x}{x_0}-1\right|_p<1 \iff x$ בעיגול. בנוסף $0\notin D\left(x_0,|x_0|_p\right)$.

$$\begin{aligned}\mathrm{Log}_p x &= \mathrm{Log}_p\left(x_0\cdot\frac{x}{x_0}\right)\\ &= \mathrm{Log}_p(x_0)+\mathrm{Log}_p\left(\frac{x}{x_0}\right)\\ &= \mathrm{Log}_p(x_0)+\mathrm{Log}_p\left(1+\left(\frac{x}{x_0}-1\right)\right)\\ &= \mathrm{Log}_p(x_0)+\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\left(\frac{x}{x_0}-1\right)^n\\ &= \mathrm{Log}_p(x_0)+\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{nx_0^n}(x-x_0)^n\end{aligned}$$

נחשב את הנגזרת:

$$\begin{aligned}\left(\mathrm{Log}_p x\right)' &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{nx_0^n}n(x-x_0)^{n-1}\\ &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{x_0^n}(x-x_0)^{n-1}\\ &= \frac{1}{x_0}\sum_{n=1}^{\infty}(-1)^{n-1}\left(\frac{x}{x_0}-1\right)^{n-1}\\ &= \frac{1}{x_0}\sum_{n=1}^{\infty}\left(1-\frac{x}{x_0}\right)^{n-1}\\ &= \frac{1}{x_0}\cdot\frac{1}{1-\left(1-\frac{x}{x_0}\right)}\\ &= \frac{1}{x}\end{aligned}$$

■

4.4 הטור הבינומי

ל-$a \in \mathbb{C}_p$ ו-$n \geq 0$ שלם נגדיר

$$\binom{a}{0} = 1$$
$$\binom{a}{n} = \frac{a \cdot (a-1) \cdot \ldots \cdot (a-n+1)}{n!}$$

נגדיר

$$B_{a,p}(x) = \sum_{n=0}^{\infty} \binom{a}{n} x^n$$

טענה 4.26 נניח כי $|a|_p > 1$. אז רדיוס ההתכנסות של $B_{a,p}(x)$ הוא $\frac{p^{-\frac{1}{p-1}}}{|a|_p}$.

הוכחה: כיוון שלכל i שלם מתקיים $|i|_p \leq 1$,

$$|a-i|_p = |a|_p$$

ולכן

$$\left| \binom{a}{n} x^n \right|_p = \left| \frac{(ax)^n}{n!} \right|_p$$

ולכן תחום ההתכנסות שווה לתחום ההתכנסות של $\exp_p(ax)$, שהוא בדיוק $|ax|_p < p^{-\frac{1}{p-1}}$.
■

טענה 4.27 אם $|a|_p \leq 1$ אז $B_{a,p}(x)$ מתכנס כאשר $|x|_p < p^{-\frac{1}{p-1}}$.

הוכחה: כאן, לו i שלם, $|a-i|_p \leq 1$ ולכן

$$\left| \binom{a}{n} \right|_p \leq \left| \frac{1}{n!} \right|_p$$

ולכן

$$\left| \binom{a}{n} x^n \right|_p \leq \left| \frac{x^n}{n!} \right|_p$$

ולכן הטור מתכנס בכל נקודה x שם הטור של $\exp_p(x)$ מתכנס. ■

טענה 4.28 לכל $a \in \mathbb{Z}_p$ גם $\binom{a}{n} \in \mathbb{Z}_p$ לכל $n \geq 0$ ולכן $B_{a,p}(x)$ מתכנס כאשר $|x|_p < 1$.

הוכחה: נתבונן ב $f\left(x\right)=\frac{x(x-1)\cdot\ldots\cdot(x-n+1)}{n!}$. זהו פולינום ממעלה n ולכן רציף כפונקציה מ$\mathbb{Q}_p$ ל$\mathbb{Q}_p$. בפרט לכל k טבעי, קיים N טבעי כך ש

$$\left|x-a\right|_p\le p^{-N}\quad\Longrightarrow\quad\left|f\left(x\right)-f\left(a\right)\right|_p\le p^{-k}$$

נקח $k=0$. כיוון ש$\mathbb{N}$ צפוף ב$\mathbb{Z}_p$, אפשר לבחור $x=a_0$ טבעי כך ש$\left|a_0-a\right|_p\le p^{-N}$ ואז $\left|f\left(a_0\right)-f\left(a\right)\right|\le1$ ואז

$$f\left(a\right)-f\left(a_0\right)\;=\;f\left(a\right)-\binom{a_0}{n}\in\mathbb{Z}_p$$

ומאחר ו$\binom{a_0}{n}\in\mathbb{Z}$ מתקיים $\binom{a_0}{n}\in\mathbb{Z}_p$ ולכן $f\left(a\right)\in\mathbb{Z}_p$. ■

הערה 4.29 (דוגמא): יהי m טבעי. נסתכל ב

$$B_{\frac{1}{m},p}\left(x\right)\;=\;\sum_{n=0}^{\infty}\binom{\frac{1}{m}}{n}x^n$$

אם $p\nmid m$ אז $\frac{1}{m}\in\mathbb{Z}_p$ והטור מתכנס כאשר $\left|x\right|_p<1$.

אם $p\mid m$ אז $\left|\frac{1}{m}\right|_p>1$ וכאן כבר ראינו כי רדיוס ההתכנסות הוא $\frac{p^{-\frac{1}{p-1}}}{\left|\frac{1}{m}\right|_p}=\left|m\right|_p\cdot p^{-\frac{1}{p-1}}$.

בכל מקרה, ברדיוס ההתכנסות

$$\left(B_{\frac{1}{m},p}\left(x\right)\right)^m\;=\;1+x$$

כי

$$\begin{aligned}\left(B_{\frac{1}{m},p}\left(x\right)\right)^m &= \left(\sum_{n=0}^{\infty}\binom{\frac{1}{m}}{n}x^n\right)^m\\ &= \sum_{k=0}^{\infty}\left(\sum_{\substack{n_1+\ldots+n_m=k\\ n_i\ge0}}\binom{\frac{1}{m}}{n_1}\binom{\frac{1}{m}}{n_2}\cdot\ldots\cdot\binom{\frac{1}{m}}{n_m}\right)x^k\end{aligned}$$

ו$\sum_{\substack{n_1+\ldots+n_m=k\\ n_i\ge0}}\binom{\frac{1}{m}}{n_1}\binom{\frac{1}{m}}{n_2}\cdot\ldots\cdot\binom{\frac{1}{m}}{n_m}$ הם מקדמים רציונליים.

מעל $\mathbb{R}$ מתקיים כי $\sum_{n=0}^{\infty}\binom{\frac{1}{m}}{n}x^n$ מתכנס בהחלט ל$\left|x\right|<1$ והוא שווה ל$\sqrt[m]{1+x}$ ולכן

$$\left(\sum_{n=0}^{\infty}\binom{\frac{1}{m}}{n}x^n\right)^m\;=\;1+x$$

וכשנכפיל כמו קודם, נקבל

$$\sum_{\substack{n_1+\ldots+n_m=k\\ n_i\ge0}}\binom{\frac{1}{m}}{n_1}\binom{\frac{1}{m}}{n_2}\cdot\ldots\cdot\binom{\frac{1}{m}}{n_m}\;=\;\begin{cases}0 & k\ge2\\ 1 & k=0,1\end{cases}$$

נשים לב כי מאחר ומקדמי הטור רציונליים, הוא מתכנס בתחום קטן יותר, למשל ב$\mathbb{Q}_p$.

הערה 4.30 (דוגמה): מקרה פרטי: $m=2, p=7$

$$B_{\frac{1}{2},7}(x) = \sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}x^n$$

מתקיים $\left|\frac{1}{2}\right|_7 = 1$ ולכן הטור מתכנס ל$|x|_7 < 1$.

$$\begin{aligned} B_{\frac{1}{2},7}(x) &= \sum_{n=0}^{\infty}\frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\cdot\ldots\cdot\left(\frac{1}{2}-n+1\right)}{n!}x^n \\ &= 1+\frac{1}{2}x+\sum_{n=2}^{\infty}\frac{(-1)^{n-1}\cdot 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-3)}{2^n\cdot n!}\cdot x^n \end{aligned}$$

נציב $x=\frac{7}{9}$ (זה אפשרי כי $\left|\frac{7}{9}\right|_7 = \frac{1}{7} < 1$)

$$\begin{aligned} \left(B_{\frac{1}{2},7}\left(\frac{7}{9}\right)\right)^2 &= 1+\frac{7}{9} \\ &= \frac{16}{9} \end{aligned}$$

לכן

$$B_{\frac{1}{2},7}\left(\frac{7}{9}\right) = \pm\frac{4}{3}$$

(ב$\mathbb{Q}_7$)

$$B_{\frac{1}{2},7}\left(\frac{7}{9}\right) = 1+\frac{1}{2}\left(\frac{7}{9}\right)+\sum_{n=2}^{\infty}\frac{(-1)^{n-1}\cdot 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-3)}{2^n\cdot n!}\cdot\left(\frac{7}{9}\right)^n$$

נשים לב כי $\left|B_{\frac{1}{2},7}\left(\frac{7}{9}\right)-1\right|_7 < 1$ ולכן

$$B_{\frac{1}{2},7}\left(\frac{7}{9}\right) \equiv 1 \pmod 7$$

נשים לב כי $\frac{4}{3}-1=\frac{1}{3}$ ולכן $\frac{4}{3}\not\equiv 1 \pmod 7$. לעומת זאת $-\frac{4}{3}-1=-\frac{7}{3}$ ולכן $-\frac{4}{3}\equiv 1 \pmod 7$. לכן קיבלנו

$$1+\frac{1}{2}\left(\frac{7}{9}\right)+\sum_{n=2}^{\infty}\frac{(-1)^{n-1}\cdot 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-3)}{2^n\cdot n!}\cdot\left(\frac{7}{9}\right)^n = \begin{cases}-\frac{4}{3} & (\mathbb{Q}_7)\\ \frac{4}{3} & (\mathbb{R})\end{cases}$$

הערה 4.31 ב־$\mathbb{R}$: אם $0 < x < 1$ מתקיים

$$(1+x)^a \cdot (1+x)^b = (1+x)^{a+b}$$

בפרט, זה נכון ל־$a, b \in \mathbb{Q}$.
נקבל

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}$$

זוהי זהות של מספרים רציונליים, לכן נכונה ב־$\mathbb{C}_p$. לכן נקבל כי ל־$a, b \in \mathbb{Q}$ מתקיים

$$B_{a,p}(x) \cdot B_{b,p}(x) = B_{a+b,p}(x)$$

5 אינטרפולציה p־אדית

5.1 אינטרפולציה של סדרת מספרים שלמים ע"י פונקציה רציפה $f : \mathbb{Z}_p \to \mathbb{Z}_p$

תהי $\{a_k\}_{k=1}^{\infty} \subseteq \mathbb{Z}$. מטרתנו היא לראות האם יש $f : \mathbb{Z}_p \to \mathbb{Z}_p$ רציפה כך ש $f(k) = a_k$ לכל k טבעי.
זה מחייב, מאחר ו־$\mathbb{Z}_p$ קומפקטי, כי f רציפה במידה שווה על $\mathbb{Z}_p$, ולכן צריך לדרוש את התנאי ההכרחי: לכל m טבעי, קיים $N = N_m$ טבעי כך שלכל k, k' טבעיים מתקיים

$$(*)\, k \equiv k' \pmod{p^N} \implies a_k \equiv a_{k'} \pmod{p^m}$$

שקול לנוסח לכל $\varepsilon > 0$ קיים $\delta > 0$ כך שלכל k, k' המקיימים $|k-k'|_p < \delta$ מתקיים $|a_k - a_{k'}|_p < \varepsilon$.
נחשוב על הסדרה כעל פונקציה רציפה במידה שווה לפי $|\cdot|_p$. כיוון שהסגור של $\mathbb{N}$ ב־$\mathbb{Q}_p$ הוא $\mathbb{Z}_p$, יש לפונקציה הרחבה יחידה לפונקציה $f : \mathbb{Z}_p \to \mathbb{Z}_p$
(ל־$x \in \mathbb{Z}_p$, בוחרים סדרת טבעיים $\{n_i\}_{i=1}^{\infty}$ כך ש־$n_i \xrightarrow[i\to\infty]{} x$. מוכיחים שקיים $\lim_{i\to\infty} a_{n_i}$ וכי הוא תלוי רק ב־x. מגדירים $f(x) = \lim_{i\to\infty} a_{n_i}$, f רציפה).
כנ"ל אם $\{a_k\}_{k=1}^{\infty} \subseteq \mathbb{C}_p$ ומקיימת את התנאי $(*)$ אז יש הרחבה יחידה לפונקציה $f : \mathbb{Z}_p \to \mathbb{C}_p$, $f(k) = a_k$ לכל k טבעי.

הערה 5.1 (דוגמה): יהי n טבעי כך ש־$n \equiv 1 \pmod p$, $n = 1 + pu$, $u > 0$ שלם.
נתבונן בסדרה $\{n^k\}_{k=1}^{\infty}$. נראה כי היא מקיימת $(*)$. נניח כי k, k' כך ש־$0 < k - k' = r \cdot p^l$ ו־$p \nmid r$. אז

$$\begin{aligned} n^{k-k'} - 1 &= (1+pu)^{k-k'} - 1 \\ &= \sum_{j=1}^{k-k'} \binom{k-k'}{j} p^j u^j \\ &= \sum_{j=1}^{k-k'} \binom{r \cdot p^l}{j} p^j u^j \end{aligned}$$

אם $j\geq l$ אז

$$\begin{aligned}\left|\binom{r\cdot p^{l}}{j}p^{j}u^{j}\right|_{p} & \leq \left|p^{j}\right|_{p}\\ & = p^{-j}\\ & \leq p^{-l}\end{aligned}$$

נניח כי $1\leq j\leq l$

$$\binom{r\cdot p^{l}}{j} = \frac{r\cdot p^{l}}{j}\cdot\frac{\left(r\cdot p^{l}-1\right)}{1}\cdot\ldots\cdot\frac{\left(r\cdot p^{l}-(j-1)\right)}{j-1}$$

אם $1\leq i<j$ אז $i<l<p^{l}$ ומכאן

$$\left|\frac{rp^{l}-i}{i}\right|_{p} = 1$$

(כי מתקיים $\left|rp^{l}\right|_{p}=\frac{1}{p^{l}}$ ו־$\left|i\right|_{p}>\frac{1}{p^{l}}$, מאחר ו־$p^{l}\nmid i$, ואז מאי־ארכימדיות $\left|\cdot\right|_{p}$ נובע כי $\left|rp^{l}-i\right|_{p}=\left|i\right|_{p}$)
לכן

$$\left|\binom{r\cdot p^{l}}{j}\right|_{p} = \left|\frac{rp^{l}}{j}\right|_{p}$$

ולכן

$$\begin{aligned}\left|\binom{r\cdot p^{l}}{j}\cdot u^{j}\cdot p^{j}\right|_{p} & \leq p^{-j-l+\log_{p}(j)}\\ & = p^{-l-\left(j-\log_{p}(j)\right)}\\ & \leq p^{-l}\end{aligned}$$

מתקיים $n\equiv1\left(\mod p\right)$ ולכן $\left|n\right|_{p}=1$.

$$\left|k-k'\right|_{p}=p^{-l}\quad\Longrightarrow\quad\left|n^{k-k'}-1\right|_{p}\underbrace{=}_{\left|n\right|_{p}=1}\left|n^{k}-n^{k'}\right|_{p}\leq p^{-l}$$

לכן מתקיימת התכונה $(*)$ ולכן יש $f:\mathbb{Z}_{p}\to\mathbb{Z}_{p}$ רציפה יחידה כך ש־$f\left(k\right)=n^{k}$ לכל k טבעי.

מסמנים $f\left(x\right)=n^{x}$ ל־$x\in\mathbb{Z}_{p}$. מתקיים $n^{x+y}=n^{x}\cdot n^{y}$ לכל $x,y\in\mathbb{Z}_{p}$.

הערה 5.2 (דוגמה): פונקציית גאמא: ל־$s\in\mathbb{C}$ עם $\Re\left(s\right)>-1$ מגדירים

$$\Gamma\left(s+1\right) = \int_{0}^{\infty}e^{-x}x^{s}dx$$

מתקיים לכל $n\geq 0$ שלם כי

$$\Gamma(n+1) = n!$$

אם יש $f:\mathbb{Z}_p\to\mathbb{Q}_p$ רציפה כך ש-$f(n)=(n-1)!$ לכל n טבעי אז מאחר ו $|n!|_p \underset{n\to\infty}{\longrightarrow} 0$, זה יחייב כי $f(x)=0$ לכל $x\in\mathbb{Z}_p$. לכן אין הרחבה כזאת.

תיקון: נניח כי $p\neq 2$. נגדיר $a_k=\prod_{\substack{j=1\\ p\nmid j}}^{k-1} j$. ננסה להראות כי $\{a_k\}_{k=1}^{\infty}$ מקיימת $(*)$.

$$\begin{aligned} a_{k+p^s} &= \prod_{\substack{j=1\\ p\nmid j}}^{k+p^s-1} j \\ &= \prod_{\substack{j=1\\ p\nmid j}}^{p^s} j\cdot \prod_{\substack{j=p^s+1\\ p\nmid j}}^{k+p^s-1} j \end{aligned}$$

מתקיים כי

$$\begin{aligned} \prod_{\substack{j=1\\ p\nmid j}}^{p^s} j &\equiv \prod_{j\in(\mathbb{Z}/p^s\mathbb{Z})^*} j \pmod{p^s} \\ &\equiv \prod_{j^2\equiv 1 \pmod{p^s}} j \pmod{p^s} \\ &\equiv -1 \pmod{p^s} \end{aligned}$$

ולכן

$$\begin{aligned} a_{k+p^s} &\equiv -\prod_{\substack{j=p^s+1\\ p\nmid j}}^{k+p^s-1} j \pmod{p^s} \\ &\equiv -a_k \pmod{p^s} \end{aligned}$$

כי הסדרה $\{j+p^s\}_{j=1}^{k-1}$ מודולו p^s שקולה לסדרה $\{j\}_{j=1}^{k-1}$.
נגדיר לכן

$$b_k = (-1)^k a_k$$

מתקיים

$$\begin{aligned} b_{k+p^s} &= (-1)^{k+p^s} a_{k+p^s} \\ &\equiv (-1)^{k+p^s+1}\cdot a_k \pmod{p^s} \\ &\underbrace{\equiv}_{p\neq 2} (-1)^k a_k \pmod{p^s} \\ &\equiv b_k \pmod{p^s} \end{aligned}$$

לכן קיימת פונקציה רציפה $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p$ כך שלכל k טבעי מתקיים

$$\Gamma_p\left(k\right) = \left(-1\right)^k \cdot \prod_{\substack{j=1 \\ p \nmid j}}^{k-1} j$$

(מגדירים $\Gamma_p\left(0\right) = 1, \Gamma_p\left(1\right) = -1$)
כמו כן, ראינו

$$\Gamma_p\left(x + p^s\right) \equiv \Gamma\left(x\right)\left(\mod p^s\mathbb{Z}_p\right)$$

זוהי פונקציית גאמא ה־p־אדית.

5.2 משפט Mahler

טענה 5.3 נתונה סדרת איברים $\{a_k\}_{k=1}^{\infty}$ (ב־$\mathbb{C}_p$).
נגדיר $b_n = \sum_{k=0}^{n} \binom{n}{k} a_k$. אז

$$a_n = \sum_{k=0}^{n} \left(-1\right)^{n-k} \binom{n}{k} b_k$$

הוכחה: נתחיל מאגף ימין

$$\sum_{k=0}^{n} \left(-1\right)^{n-k} \binom{n}{k} b_k = \sum_{k=0}^{n} \left(-1\right)^{n-k} \binom{n}{k} \sum_{j=0}^{k} \binom{k}{j} a_j$$

(נגדיר $\binom{k}{j} = 0$ ל־$j > k$)

$$\begin{aligned} \sum_{k=0}^{n} \left(-1\right)^{n-k} \binom{n}{k} \sum_{j=0}^{k} \binom{k}{j} a_j &= \sum_{k=0}^{n} \left(-1\right)^{n-k} \binom{n}{k} \sum_{j=0}^{n} \binom{k}{j} a_j \\ &= \sum_{j=0}^{n} \left(\sum_{k=0}^{n} \left(-1\right)^{n-k} \binom{n}{k} \binom{k}{j} \right) a_j \end{aligned}$$

נחשב

$$\begin{aligned}
\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\binom{k}{j} &= \sum_{k=j}^{n}(-1)^{n-k}\binom{n}{k}\binom{k}{j} \\
&= (-1)^{n}\frac{n!}{j!}\sum_{k=j}^{n}\frac{(-1)^{k}}{(n-k)!\,(k-j)!} \\
&= (-1)^{n}\binom{n}{j}\sum_{k=j}^{n}\frac{(-1)^{k}(n-j)!}{(n-k)!\,(k-j)!} \\
&= (-1)^{n}\binom{n}{j}\sum_{k=j}^{n}(-1)^{k}\binom{n-j}{k-j} \\
&= (-1)^{n}\binom{n}{j}\sum_{k=0}^{n-j}(-1)^{k+j}\binom{n-j}{k} \\
&= (-1)^{n+j}\binom{n}{j}\sum_{k=0}^{n-j}(-1)^{k}\binom{n-j}{k} \\
&= (-1)^{n+j}\binom{n}{j}(1+(-1))^{n-j} \\
&= \begin{cases} 0 & j<n \\ 1 & j=n \end{cases} \\
&= \delta_{jn}
\end{aligned}$$

■

הערה 5.4 הטענה מראה גם את הכיוון ההפוך: אם נתונה הסדרה $\{b_k\}_{k=1}^{\infty}$ ומגדירים $a_n=\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}b_k$ אז

$$\underbrace{(-1)^{n}a_n}_{\beta_n} = \sum_{k=0}^{n}\binom{n}{k}\left(\underbrace{(-1)^{k}b_k}_{\alpha_k}\right)$$

אז מהטענה

$$\begin{aligned}
\alpha_n &= \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\beta_k \\
(-1)^{n}b_n &= \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}(-1)^{k}a_k \\
&= (-1)^{n}\sum_{k=0}^{n}\binom{n}{k}a_k
\end{aligned}$$

כלומר

$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_k$$

נתונה $f:\mathbb{Z}_p \to \mathbb{C}_p$ רציפה.
נגדיר

$$a_n(f) = \sum_{k=0}^{n} (-1)^n \binom{n}{k} f(k)$$

מהטענה הקודמת מתקיים

$$\begin{aligned} f(n) &= \sum_{k=0}^{n} \binom{n}{k} a_k(f) \\ &= \sum_{k=0}^{\infty} \binom{n}{k} a_k(f) \end{aligned}$$

הרעיון: להציב $x \in \mathbb{Z}_p$ במקום n ולהראות כי

$$f(x) = \sum_{k=0}^{\infty} \binom{x}{k} a_k(f)$$

(לאחר שנראה כי הטור הנ"ל אכן מגדיר מספר)

הגדרה 5.5 נגדיר

$$\Delta^n f(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(x+k)$$

לכל $n \geq 0$ שלם.

הערה 5.6 (דוגמאות):

$$\begin{aligned} \Delta^n f(0) &= a_n(f) \\ \Delta^1 f(x) &= f(x+1) - f(x) \\ \Delta^2 f(x) &= f(x+2) - 2f(x+1) + f(x) \end{aligned}$$

וכו'.

למה 5.7

$$\Delta^n f(x) = \sum_{j=0}^{m} \binom{m}{j} \Delta^{n+j} f(x-m)$$

לכל $m \geq 0$.

הוכחה: מספיק להוכיח כי

$$f(x) = \sum_{j=0}^{m}\binom{m}{j}\Delta^{j}f(x-m)$$

(ואח"כ נציב $\Delta^{n}f$ במקום f)

$$\begin{aligned}\sum_{j=0}^{m}\binom{m}{j}\Delta^{j}f(x-m) &= \sum_{j=0}^{m}\binom{m}{j}\sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k}f(x-m+k)\\ &= \sum_{j=0}^{m}\binom{m}{j}\sum_{k=0}^{m}(-1)^{j-k}\binom{j}{k}f(x-m+k)\end{aligned}$$

כי $\binom{j}{k}=0$ לכל $j<k$.

$$\begin{aligned}\sum_{j=0}^{m}\binom{m}{j}\Delta^{j}f(x-m) &= \sum_{j=0}^{m}\binom{m}{j}\sum_{k=0}^{m}(-1)^{j-k}\binom{j}{k}f(x-m+k)\\ &= \sum_{k=0}^{m}f(x-m+k)(-1)^{k}\sum_{j=0}^{m}(-1)^{j}\binom{m}{j}\binom{j}{k}\\ &= \sum_{k=0}^{m}f(x-m+k)(-1)^{k}\underbrace{\sum_{j=0}^{m}(-1)^{j}\binom{m}{j}\binom{j}{k}}_{(-1)^{m}\delta_{mk}}\\ &= f(x-m+m)(-1)^{m}(-1)^{m}\\ &= f(x)\end{aligned}$$

■

נציב $x=m$ ונקבל:

$$\begin{aligned}\sum_{j=0}^{m}\binom{m}{j}\Delta^{n+j}f(m-m) &= \Delta^{n}f(m)\\ \sum_{j=0}^{m}\binom{m}{j}\Delta^{n+j}f(0) &= \Delta^{n}f(m)\\ \sum_{j=0}^{m}\binom{m}{j}a_{n+j}(f) &= \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(m+k)\end{aligned}$$

למה 5.8

$$\sum_{j=0}^{m}\binom{m}{j}a_{n+j}(f) = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(m+k)$$

הערה 5.9 אם נתונה סדרה $\mathbb{C}_p \supseteq \{\varphi(k)\}_{k=0}^{\infty}$, אז גם מתקיים

$$\sum_{j=0}^{m} \binom{m}{j} a_{n+j}(\varphi) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \varphi(m+k)$$

לכל $m, n \geq 0$, כי אותה הוכחה תעבוד.

משפט 5.10 (Mahler): תהי

$$f : \mathbb{Z}_p \to \mathbb{C}_p$$

רציפה. נגדיר לכל $n \geq 0$

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$$

אז $\lim_{n\to\infty} a_n(f) = 0$ ומתקיים

$$f(x) = \sum_{k=0}^{n} \binom{x}{k} a_k(f)$$

לכל $x \in \mathbb{Z}_p$. בפרט, אפשר לקרב מידה שווה את f ע"י פולינום על $\mathbb{Z}_p$.

הערה 5.11 ריאנו כי ל$x \in \mathbb{Z}_p$ מתקיים כי $\binom{x}{k} \in \mathbb{Z}_p$ ולכן הטור מתכנס במידה שווה, במידה והוא מתכנס.

הוכחה: f רציפה, ומאחר ו$\mathbb{Z}_p$ קבוצה קומפקטית, f רציפה במ"ש על $\mathbb{Z}_p$. לכן לכל s טבעי קיים t טבעי, כך שלכל $x, y \in \mathbb{Z}_p$, אם $|x-y|_p \leq p^{-t}$, מתקיים $|f(x) - f(y)|_p \leq p^{-s}$. בפרט

$$\left|f\left(x+p^t\right) - f(x)\right|_p \leq p^{-s}$$

לכל $x \in \mathbb{Z}_p$.
f חסומה: $|f(z)|_p \leq A$ לכל $z \in \mathbb{Z}_p$, מכאן:

$$\begin{aligned} |a_n(f)|_p &\leq \max_{0\leq k\leq n} \left(\left|\binom{n}{k}\right|_p \cdot |f(k)|_p \right) \\ &\leq A \end{aligned}$$

נציב $m = p^t$ בלמה האחרונה ונקבל

$$\sum_{j=0}^{p^t} \binom{p^t}{j} a_{n+j}(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f\left(k+p^t\right)$$

נעביר אגף את כל הגורמים פרט לאחרון ונקבל

$$\begin{aligned} a_{n+p^t}(f) &= -\sum_{j=1}^{p^t-1}\binom{p^t}{j}a_{n+j}(f)-a_n(f)+\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f\left(k+p^t\right) \\ &= -\sum_{j=1}^{p^t-1}\binom{p^t}{j}a_{n+j}(f)-\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(k)+\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f\left(k+p^t\right) \\ &= -\sum_{j=1}^{p^t-1}\binom{p^t}{j}a_{n+j}(f)+\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\left(f\left(k+p^t\right)-f(k)\right) \end{aligned}$$

לכן

$$\begin{aligned} \left|a_{n+p^t}(f)\right|_p &\le \max\left\{\max_{1\le j\le p^t-1}\underbrace{\left|\binom{p^t}{j}\right|_p}_{\le p^{-1}}\underbrace{\left|a_{n+j}(f)\right|_p}_{\le A},p^{-s}\right\} \\ &\le \max\left\{p^{-1}\cdot A,p^{-s}\right\} \\ &= A\cdot p^{-1} \end{aligned}$$

כאשר נדרוש $p^{-s}<p^{-1}\cdot A$, כלומר $1-\log_p(A)<s$.
נציב בסדרת האי־שוויונות האחרונה $n+p^t$ במקום n ונקבל

$$\begin{aligned} \left|a_{n+2p^t}(f)\right|_p &\le \max\left\{\max_{1\le j\le p^t-1}\underbrace{\left|\binom{p^t}{j}\right|_p}_{\le p^{-1}}\underbrace{\left|a_{n+p^t+j}(f)\right|_p}_{\le A\cdot p^{-1}},p^{-s}\right\} \\ &\le A\cdot p^{-2} \end{aligned}$$

כאשר נדרוש $p^{-2}\cdot A>p^{-s}$ כלומר $s>2-\log_p A$.
כללית, יהי s' השלם כך ש

$$A\cdot p^{s-1}<p^{s'}\quad\le\quad A\cdot p^{s}$$

כלומר

$$0<s-1+\log_p A\quad<\quad s'<s+\log_p A$$

נחזור על התהליך ונקבל

$$\left|a_{n+s'\cdot p^t}(f)\right|_p\quad\le\quad p^{-s'}\cdot A$$

זה מוכיח שלכל $k\ge s'\cdot p^t$

$$\left|a_k(f)\right|_p\quad\le\quad p^{-s'}\cdot A$$

זה מראה ש

$$a_k(f) \underset{k\to\infty}{\longrightarrow} 0$$

ראינו כי $\binom{x}{p} \in \mathbb{Z}_p$ לכל $x \in \mathbb{Z}_p$. מכאן, $\sum_{k=0}^{\infty}\binom{x}{k}a_k(f)$ מתכנס במ"ש ב-$\mathbb{Z}_p$ ולכן מגדיר שם פונקציה רציפה $g(x)$.
כיוון שלכל $n \geq 0$ מתקיים

$$\begin{aligned} g(n) &= \sum_{k=0}^{\infty}\binom{n}{k}a_k(f) \\ &= \sum_{k=0}^{n}\binom{n}{k}a_k(f) \\ &= f(n) \end{aligned}$$

יוצא כי הפונקציה הרציפה $f(x) - g(x)$ על $\mathbb{Z}_p$ מתאפסת על הקבוצה הצפופה $\mathbb{Z}_p^+$ ולכן $f(x) = g(x)$ לכל $x \in \mathbb{Z}_p$. ■

מסקנה 5.12 תהי $\{a_n\}_{n=0}^{\infty}$ סדרה. נגדיר

$$b_n = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}a_k$$

אז קיימת $f : \mathbb{Z}_p \to \mathbb{C}_p$ רציפה כך ש-$f(n) = a_n$ לכל $n \geq 0$ שלם אם ורק אם $b_n \underset{n\to\infty}{\longrightarrow} 0$.

הוכחה: אם קיימת f רציפה כנ"ל, אז כיוון ש-$a_n(f) = b_n$, אז ממשפט מאהלר, $b_n = a_n(f) \underset{n\to\infty}{\longrightarrow} 0$. להפך, נניח כי $b_n \underset{n\to\infty}{\longrightarrow} 0$ אז נגדיר

$$f(x) = \sum_{n=0}^{\infty}\binom{x}{n}b_n$$

($x \in \mathbb{Z}_p$)
הטור מתכנס במידה שווה ב-$\mathbb{Z}_p$ ומגדיר שם פונקציה רציפה $f(x)$.

$$\begin{aligned} f(n) &= \sum_{k=0}^{\infty}\binom{n}{k}b_k \\ &= \sum_{k=0}^{n}\binom{n}{k}b_k \\ &= a_n \end{aligned}$$

■

מסקנה 5.13 תהי $\{a_n\}_{n=0}^{\infty} \subseteq \mathbb{C}_p$. אז התכונות הבאות שקולות:

1. לכל $\varepsilon > 0$ קיים $\delta > 0$ כך שלכל $m, n \geq 0$

$$|m-n|_p < \delta \implies |a_n - a_m|_p < \varepsilon$$

2. נגדיר

$$b_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} a_k$$

אז $b_n \underset{n\to\infty}{\longrightarrow} 0$.

5.3 המשכה אנליטית של פונקציות רציפות על $\mathbb{Z}_p$

למה 5.14 תהי $\{g_i(x) = \sum_{n=0}^{\infty} a_{n,i}x^n\}$ סדרה של טורי חזקות ב-$\mathbb{C}_p[[x]]$, המתכנסים בקבוצה $D \subseteq \mathbb{C}_p$. נניח כי קיימים $\lim_{i\to\infty} a_{n,i} = a_n$ לכל $n \geq 0$.
יהי $x \in D$ ונניח כי לכל $\varepsilon > 0$ קיים $n_0 = n_0(x, \varepsilon)$ כך שלכל $n \geq n_0$

$$\left| \sum_{m=n}^{\infty} a_{m,i}x^n \right|_p < \varepsilon$$

לכל $i \geq 1$.
(כלומר, $\sum_{n=0}^{\infty} a_{n,i}x^n$, מתכנס במ"ש ב-$i$)
אז הטור $g(x) = \sum_{n=0}^{\infty} a_n x^n$ מתכנס, לכל $x \in D$ ומתקיים $\lim_{i\to\infty} g_i(x) = g(x)$.

הוכחה: יהי $\varepsilon > 0$ ויהי $n_0 = n_0(x, \varepsilon)$ כנ"ל. לכל $n > n_0$ ו-$i \geq 1$ מתקיים

$$\begin{aligned} |a_{n,i}x^n|_p &= \left| \sum_{m=n}^{\infty} a_{m,i}x^m - \sum_{m=n+1}^{\infty} a_{m,i}x^m \right|_p \\ &\leq \max\left\{ \left| \sum_{m=n}^{\infty} a_{m,i}x^m \right|_p, \left| \sum_{m=n+1}^{\infty} a_{m,i}x^m \right|_p \right\} \\ &< \varepsilon \end{aligned}$$

לכן לכל $n > n_0$ ולכל $i \geq 1$ מתקיים

$$|a_{n,i}x^n|_p < \varepsilon$$

נשאיף את i לאינסוף. לכן

$$|a_n x^n|_p \leq \varepsilon$$

לכל $n > n_0$. מכאן

$$a_n x^n \underset{n\to\infty}{\longrightarrow} 0$$

ולכן

$$g(x) = \sum_{n=0}^{\infty} a_n x^n$$

מתכנס.

$$g_i(x) - g(x) = \sum_{n=0}^{\infty} (a_{n,i} - a_n) x^n$$

$$|g_i(x) - g(x)|_p \leq \max\left\{ \left| \sum_{n=0}^{n_0} (a_{n,i} - a_n) x^n \right|_p, \left| \sum_{n=n_0}^{\infty} a_{n,i} x^n \right|_p, \left| \sum_{n=n_0}^{\infty} a_n x^n \right|_p \right\}$$

ונקח n_0 די גדול כך שגם

$$\left| \sum_{n=n_0}^{\infty} a_n x^n \right|_p < \varepsilon$$

וניקח i_0 כך שלכל $i \geq i_0$ מתקיים $|(a_{n,i} - a_n) x^n|_p < \varepsilon$ לכל $0 \leq n \leq n_0 - 1$.
לכן

$$|g_i(x) - g(x)|_p < \varepsilon$$

זה מראה ש $g_i(x) \underset{i\to\infty}{\longrightarrow} g(x)$. ■

משפט 5.15 נתונה סדרה $\{a_n\}_{n=0}^{\infty} \subseteq \mathbb{C}_p$ ונניח כי קיימים $0 < r < p^{-\frac{1}{p-1}}$ ו$M > 0$ כך ש$|a_n|_p \leq M r^n$ לכל $0 \leq n$.
נתבונן בפונקציה על $\mathbb{Z}_p$

$$f(x) = \sum_{n=0}^{\infty} \binom{x}{n} a_n$$

זאת פונקציה רציפה על $\mathbb{Z}_p$.
$f(x)$ היא צמצום של טור חזקות ב$\mathbb{C}_p[[x]]$ המתכנס בעיגול

$$D(0,R) = \left\{ x \in \mathbb{C}_p \mid |x|_p < R \right\}$$

כאשר $R = \left(r p^{\frac{1}{p-1}} \right)^{-1}$ ($R > 1$).

הוכחה: לכל $i \geq 0$ נגדיר

$$g_i(x) = \sum_{n=0}^{i} \binom{x}{n} a_n$$

$$= \sum_{n=0}^{i} \frac{a_n}{n!} \underbrace{x(\cdot x - 1) \cdot \ldots \cdot (x - n + 1)}_{(x)_n}$$

$$= \sum_{n=0}^{i} \frac{a_n}{n!} \sum_{k=0}^{n} (-1)^{n-k} S_{n-k}(0, 1, \ldots, n-1) x^k$$

כאשר $S_{n-k}\left(0,1,\ldots,n-1\right)$ הוא הפולינום הסימטרי האלמנטרי ממעלה $n-k$ במשתנים $x_0,\ldots,x_{n-1}$ כאשר מציבים $x_j=j$. נגדיר ל־$n<k$ $S_{n-k}=0$. אז

$$\begin{aligned} g_i\left(x\right) &= \sum_{n=0}^{i}\sum_{k=0}^{n}\frac{a_n}{n!}\left(-1\right)^{n-k}S_{n-k}\left(0,1,\ldots,n-1\right)x^k \\ &= \sum_{n=0}^{i}\sum_{k=0}^{i}\frac{a_n}{n!}\left(-1\right)^{n-k}S_{n-k}\left(0,1,\ldots,n-1\right)x^k \\ &= \sum_{k=0}^{i}\sum_{n=0}^{i}\frac{a_n}{n!}\left(-1\right)^{n-k}S_{n-k}\left(0,1,\ldots,n-1\right)x^k \\ &= \sum_{k=0}^{i}\underbrace{\sum_{n=k}^{i}\frac{a_n}{n!}\left(-1\right)^{n-k}S_{n-k}\left(0,1,\ldots,n-1\right)x^k}_{a_{k,i}} \end{aligned}$$

מתקיים

$$g_i\left(x\right) = \sum_{k=0}^{i}a_{k,i}x^k$$

$$\begin{aligned} \left|a_{k,i}\right|_p &\le \max_{k\le n\le i}\left|a_n\right|_p\cdot\left|\frac{1}{n!}\right|_p \\ &\le M\cdot\max_{k\le n\le i}r^n\cdot\underbrace{\left|\frac{1}{n!}\right|_p}_{\le p^{\frac{n-1}{p-1}}<p^{\frac{n}{p-1}}} \\ &\le M\cdot\max_{k\le n\le i}\left(rp^{\frac{1}{o-1}}\right)^n \\ &= M\cdot R^{-k} \end{aligned}$$

כעת

$$\begin{aligned} \left|a_{k,i+1}-a_{k,i}\right|_p &= \left|\frac{a_{i+1}}{\left(i+1\right)!}\left(-1\right)^{i+1-k}\cdot S_{I+1-k}\left(0,1,\ldots,i\right)\right|_p \\ &\le \left|\frac{a_{i+1}}{\left(i+1\right)!}\right|_p \\ &< MR^{-(i+1)}\underset{i\to\infty}{\longrightarrow}0 \end{aligned}$$

ולכן $\left\{a_{k,i}\right\}$ סדרת קושי. נסמן

$$\alpha_k = \lim_{i\to\infty}a_{k,i}$$

אז

$$\left|a_{k,i}\right|_p < MR^{-k}$$

ולכן

$$|\alpha_k|_p \leq MR^{-k}$$

ולכן הטור $\sum_{k=0}^{\infty}\alpha_k x^k$ מתכנס ב$D(0,R)$.

$$\begin{aligned}\left|\sum_{k=N}^{\infty}a_{k,i}x^k\right|_p &\leq \max_{N\leq k}|a_{k,i}|_p\cdot|x|_p^k\\ &\leq M\cdot\max_{N\leq k}\left(\frac{|x|_p}{R}\right)^k \underset{N\to\infty}{\longrightarrow}0\end{aligned}$$

והשאיפה היא במידה שווה בi, כאשר $R<|x|_p$. לכן מהלמה האחרונה קיים

$$\begin{aligned}\lim_{i\to\infty}g_i(x) &= g(x)\\ \sum_{k=0}^{\infty}\binom{x}{k}a_k &= \lim_{i\to\infty}\sum_{k=0}^{i}\binom{x}{k}a_k=\sum_{k=0}^{\infty}\alpha_k x^k\end{aligned}$$

■

משפט 5.16 תהי $f:\mathbb{Z}_p\to\mathbb{C}_p$ פונקציה רציפה, בעלת טור מאהלר

$$f(x) = \sum_{n=0}^{\infty}\binom{x}{n}c_n$$

(כאשר $c_n=a_n(f)$).

אז f היא צמצום מ$\mathcal{O}_{\mathbb{C}_p}$ של טור חזקות ב$\mathbb{C}_p[[x]]$, $\sum_{n=0}^{\infty}a_nx^n$ כאשר $a_n\underset{n\to\infty}{\longrightarrow}0$ (ולכן הטור מתכנס ב$\mathcal{O}_{\mathbb{C}_p}$) אם ורק אם $\frac{c_n}{n!}\underset{n\to\infty}{\longrightarrow}0$.

הוכחה: נניח כי $\frac{c_n}{n!}\underset{n\to\infty}{\longrightarrow}0$. ל$x\in\mathbb{Z}_p$ מתקיים

$$\begin{aligned}f(x) &= \sum_{n=0}^{\infty}\frac{c_n}{n!}(x)_n\\ &= \sum_{n=0}^{\infty}\frac{c_n}{n!}\sum_{k=0}^{n}(-1)^{n-k}S_{n-k}(0,\ldots,n-1)x^k\\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{c_n}{n!}(-1)^{n-k}S_{n-k}(0,\ldots,n-1)x^k\end{aligned}$$

מתקיים

$$\left|\frac{c_n}{n!}(-1)^{n-k}S_{n-k}(0,\ldots,n-1)x^k\right|_p \underbrace{\leq}_{|x|_p\leq 1} \left|\frac{c_n}{n!}\right|_p\underset{n\to\infty}{\longrightarrow}0$$

במידה שווה ב-k.

כיוון ש-$S_{n-k}=0$ ל-$k>n$, מתקיים

$$\lim_{k\to\infty}\frac{c_n}{n!}\left(-1\right)^{n-k}S_{n-k}\left(0,\ldots,n-1\right)x^k = 0$$

ולכן אפשר להחליף את סדר הסיכומים ולקבל

$$\begin{aligned} f\left(x\right) &= \sum_{k=0}^{\infty}\sum_{n=0}^{\infty}\frac{c_n}{n!}\left(-1\right)^{n-k}S_{n-k}\left(0,\ldots,n-1\right)x^k \\ &= \sum_{k=0}^{\infty}\underbrace{\sum_{n=k}^{\infty}\frac{c_n}{n!}\left(-1\right)^{n-k}S_{n-k}\left(0,\ldots,n-1\right)}_{a_k}x^k \\ &= \sum_{k=0}^{\infty}a_kx^k \end{aligned}$$

מתקיים

$$\left|a_k\right|_p \leq \max_{n\geq k}\left|\frac{c_n}{n!}\right|_p\underset{k\to\infty}{\longrightarrow}0$$

כנדרש.

להפך, נניח כי $f\left(x\right)=\sum_{k=0}^{\infty}a_kx^k$ ל-$x\in\mathbb{Z}_p$ כאשר $a_k\underset{k\to\infty}{\longrightarrow}0$.

נכתוב

$$\left(x\right)_n = \sum_{k=0}^{n}\left(-1\right)^{n-k}S_{n-k}\left(0,1,\ldots,n-1\right)x^k$$

אז המטריצה
$$\begin{pmatrix} 1 & 0 & 0 & \ldots & * \\ 0 & 1 & -1 & \vdots & \vdots \\ 0 & 0 & 1 & \vdots & -S_2\left(0,\ldots,n-1\right) \\ 0 & 0 & 0 & \ddots & -S_1\left(0,\ldots,n-1\right) \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
היא מטריצה יוניפוטנטית עליונה מעל $\mathbb{Z}$. לכן המטריצה ההפוכה היא גם כן מטריצה יוניפוטנטית מעל $\mathbb{Z}$.

לכן אפשר להציג

$$x^n = \sum_{k=0}^{n}S\left(n,k\right)\left(x\right)_k$$

כאשר $S\left(n,k\right)\in\mathbb{Z}$ ונגדיר $S\left(n,k\right)=0$ כאשר $n<k$.

$$\begin{aligned} f\left(x\right) &= \sum_{k=0}^{\infty}a_k\sum_{l=0}^{k}S\left(k,l\right)\left(x\right)_l \\ &= \sum_{k=0}^{\infty}\sum_{l=0}^{\infty}a_kS\left(k,l\right)\left(x\right)_l \end{aligned}$$

מתקיים

$$\left|a_k S(k,l)(x)_l\right|_p \underbrace{\leq}_{|S(k,l)|_p, \left|(x)_l\right|_p \leq 1} |a_k|_p \underset{k\to\infty}{\longrightarrow} 0$$

במידה שווה ב-l.
$a_k S(k,l)(x)_l = 0$ לכל $k < l$ ולכן שואף ל-0 כאשר $l \to \infty$.
לכן אפשר להחליף את סדר הסיכום

$$\begin{aligned} f(x) &= \sum_{k=0}^{\infty}\sum_{l=0}^{\infty} a_k S(k,l)(x)_l \\ &= \sum_{l=0}^{\infty}\sum_{k=0}^{\infty} a_k S(k,l)(x)_l \\ &= \sum_{l=0}^{\infty}\underbrace{\sum_{k=l}^{\infty} a_k S(k,l)(x)_l}_{b_l} \end{aligned}$$

מתקיים

$$|b_l|_p \leq \max_{k\geq l} |a_k|_p \underset{l\to\infty}{\longrightarrow} 0$$

כעת

$$f(x) = \sum_{l=0}^{\infty}\binom{x}{l}\cdot(b_l\cdot l!)$$

מתקיים כי $c_l = b_l \cdot l!$ ולכן

$$\frac{c_l}{l!} = b_l \underset{l\to\infty}{\longrightarrow} 0$$

■

הערה 5.17 (דוגמאות):

1.

$$f(x) = n^x$$

נניח $p \neq 2$. דרשנו $n \equiv 1 \pmod p$. טור מאהלר:

$$\begin{aligned} a_m(f) &= \sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k} f(k) \\ &= \sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k} n^k \\ &= (n-1)^m \end{aligned}$$

ולכן

$$
\begin{aligned}
n^x &= \sum_{k=0}^{\infty} \binom{x}{k} a_k(f) \\
&= \sum_{k=0}^{\infty} \binom{x}{k} (n-1)^k \\
&= B_{x,p}(n-1)
\end{aligned}
$$

מתקיים

$$
\begin{aligned}
|n-1|_p &\le p^{-1} \\
|a_k(f)|_p &\le p^{-k}
\end{aligned}
$$

$r = p^{-1} < p^{-\frac{1}{p=1}}$, $M = 1$ ומתקיים

$$
|a_k(f)|_p \le Mr^k
$$

ואז ראינו כי $f(x)$ צמצום של טור חזקות מתכנס ב$|x|_p < R$ (ב$\mathbb{C}_p$) כאשר

$$
\begin{aligned}
R &= \left(rp^{\frac{1}{p-1}}\right)^{-1} \\
&= p^{1-\frac{1}{p-1}} \\
&= p^{\frac{p-2}{p-1}}
\end{aligned}
$$

.2 $p = 2$. כאן נניח $n \equiv 1 \pmod 4$ ונתבונן ב

$$
f(x) = n^x
$$

נוכל לחזור על הדוגמא הקודמת, אבל הפעם $|n-1|_2 \le \frac{1}{4}$ ולכן נוכל לקבל $r = \frac{1}{4} \le 2^{-\frac{1}{2-1}}$

$$
\begin{aligned}
R &= \left(\frac{1}{4} \cdot 2\right)^{-1} \\
&= 2
\end{aligned}
$$

הערה 5.18 נסתכל על הפונקציה הרציפה $\exp_p\left(x \cdot \mathrm{Log}_p n\right)$. לפונקציה זו טור חזקות

$$
\exp_p\left(x \cdot \mathrm{Log}_p n\right) = \sum_{k=0}^{\infty} \frac{x^k}{k!} \left(\mathrm{Log}_p n\right)^k
$$

המתכנס ל$|x|_p \leq 1$. מתקיים מתכונות האקספוננט כי

$$\begin{aligned}\exp_p\left(m\cdot \mathrm{Log}_p n\right) &= \underbrace{\exp_p\left(\mathrm{Log}_p n\right)\cdot \ldots \cdot \exp_p\left(\mathrm{Log}_p n\right)}_{m}\\ &= \underbrace{n\cdot n\cdot \ldots \cdot n}_{m}\\ &= n^m\end{aligned}$$

לכל $m \geq 0$ שלם. לכן משיקולי רציפות מתקיים

$$\exp_p\left(x\cdot \mathrm{Log}_p n\right) = n^x$$

6 פונקציות־L p־אדיות

6.1 טורי L של דיריכלה

הגדרה 6.1 יהי f מספר טבעי. כרקטר פרימיטיבי מודולו f הוא הומומורפיזם של חבורות

$$\chi : (\mathbb{Z}/f\mathbb{Z})^* \to \mathbb{C}^*$$

יש תנאי מינימליות על f במובן הבא: נניח כי $f' \mid f$. אז יש לנו

$$\nu : (\mathbb{Z}/f\mathbb{Z})^* \to (\mathbb{Z}/f'\mathbb{Z})^*$$

הומומורפיזם של חבורת ההפיכים של החוגים. דורשים כי לא קיים הומומורפיזם

$$\xi : (\mathbb{Z}/f'\mathbb{Z})^* \to \mathbb{C}^*$$

כך ש

$$\chi = \xi\circ\nu$$

בפרט, אם $f > 1$ אז $\chi \not\equiv 1$.

כאשר $f = 1$ נסמן את הכרקטר ב$\chi = 1$.

נרחיב את χ לפונקציה על המספרים הטבעיים:

$$\chi(n) = \begin{cases}\chi(n+\mathbb{Z}f) & (n,f)=1\\ 0 & (n,f)>1\end{cases}$$

הגדרה 6.2 טור L של χ

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

הטור מתכנס בהחלט כאשר $\Re(s) > 1$. כאשר $f > 1$ הטור מתכנס (בתנאי) כאשר $\Re(s) > 0$. (לא נוכיח, וכנראה לא נשתמש)
אם $\chi = 1$ אז

$$L(s,\chi) = \zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$$

משפט 6.3 נניח כי $f > 1$ וχ כרקטר פרימיטיבי מודולו f, אז יש ל$L(s,\chi)$ המשכה אנליטית לכל $\mathbb{C}$.

הוכחה: נניח כי $\Re(s) > 1$.

$$\begin{aligned} L(s,\chi) &= \sum_{a=1}^{f}\chi(a)\sum_{n\equiv a(\mod f)}\frac{1}{n^s} \\ &= \sum_{a=1}^{f}\chi(a)\sum_{n=0}^{\infty}\frac{1}{(a+fn)^s} \\ &= f^{-s}\sum_{a=1}^{f}\chi(a)\sum_{n=0}^{\infty}\frac{1}{\left(n+\frac{a}{f}\right)^s} \\ &= f^{-s}\sum_{a=1}^{f}\chi(a)\zeta\left(s,\frac{a}{f}\right) \end{aligned}$$

כאשר

$$\zeta(a,x) = \sum_{n=0}^{\infty}\frac{1}{(n+x)^s}$$

($0 < x \leq 1$)
פונקציית זטא של הורביץ. לפונקציית זטא של הורביץ יש המשכה אנליטית לכל $\mathbb{C}$ עם קוטב יחיד ב$s = 1$. הקוטב פשוט והשארית היא 1.
לכן

$$L(s,\chi) = f^{-s}\sum_{a=1}^{f}\chi(a)\zeta\left(s,\frac{a}{f}\right)$$

אנליטית ב$\mathbb{C}$, פרט אולי, לקוטב ב$s = 1$ (קוטב פשוט).
מתקיים

$$\begin{aligned} \mathrm{Res}_{s=1}(L(s,\chi)) &= \frac{1}{f}\sum_{a=1}^{f}\chi(a) \\ &= \frac{1}{f}\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\chi(b) \\ &= \begin{cases} \frac{1}{f} & \chi \text{ is trivial (only when } f=1) \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

כי נבחר $b_0 \in (\mathbb{Z}/f\mathbb{Z})^*$ כך ש$\chi(b_0) \neq 1$ ואז

$$\begin{aligned}\chi(b_0)\left(\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\chi(b)\right) &= \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\chi(bb_0)\\ &= \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\chi(b)\end{aligned}$$

ולכן

$$\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\chi(b) = 0$$

■

ראינו $\zeta(1-n) = -\frac{B_n}{n}$. בתרגילי בית הראינו כי

$$\zeta(1-n,x) = -\frac{B_n(x)}{n}$$

כאשר

$$B_n(x) = \sum_{k=0}^{n}\binom{n}{k}B_k x^{n-k}$$

ו$B_n(x)$ נקרא פולינום ברנולי. בנוסף

$$\begin{aligned}B_n(0) &= B_n\\ \frac{te^{xt}}{e^t-1} &= \sum_{k=0}^{\infty}\frac{B_k(x)}{k!}\cdot t^k\end{aligned}$$

ל$|t| < 2\pi$.

נחשב

$$\begin{aligned}L(1-n,\chi) &= f^{n-1}\sum_{a=1}^{f}\chi(a)\,\zeta\left(1-n,\frac{a}{f}\right)\\ &= -f^{n-1}\sum_{a=1}^{f}\chi(a)\,\frac{B_n\left(\frac{a}{f}\right)}{n}\end{aligned}$$

נסמן

$$B_{n,\chi} = f^{n-1}\sum_{a=1}^{f}\chi(a)\,B_n\left(\frac{a}{f}\right)$$

אז

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}$$

נכתוב זאת כמשפט:

משפט 6.4

$$L\left(1-n,\chi\right) = -\frac{B_{n,\chi}}{n}$$

הערה 6.5 נציב כעת $\chi = 1$ (ואז $f = 1$) ונקבל

$$\begin{aligned} B_{n,1} &= B_n\left(1\right) \\ &= \sum_{k=0}^{n}\binom{n}{k}B_k \\ &= \underbrace{\sum_{k=0}^{n-1}\binom{n}{k}B_k}_{0} + B_n \\ &= B_n \end{aligned}$$

למשל

$$\begin{aligned} B_{1,1} &= B_1\left(1\right) \\ &= B_0 + B_1 \\ &= 1 + \left(-\frac{1}{2}\right) \\ &= \frac{1}{2} \end{aligned}$$

כלומר

$$\begin{aligned} \zeta\left(0\right) &= L\left(0,1\right) \\ &= -\frac{B_{1,1}}{1} \\ &= -\frac{1}{2} \end{aligned}$$

הערה 6.6 ראינו בשיעורי בית

$$B_n\left(1-x\right) = \left(-1\right)^n B_n\left(x\right)$$

ולכן

$$\begin{aligned}
L\left(1-n,\chi\right) &= -\frac{f^{n-1}}{n}\sum_{a=1}^{f}\chi\left(a\right)B_{n}\left(\frac{a}{f}\right)\\
&= -\frac{f^{n-1}}{n}\sum_{a=1}^{f}\chi\left(a\right)\left(-1\right)^{n}B_{n}\left(1-\frac{a}{f}\right)\\
&= \frac{\left(-1\right)^{n-1}f^{n-1}}{n}\sum_{a=1}^{f}\underbrace{\chi\left(a\right)}_{\chi(-1)\chi(-a)=\chi(-1)\chi(f-a)}B_{n}\left(1-\frac{a}{f}\right)\\
&= \frac{\left(-1\right)^{n-1}\chi\left(-1\right)f^{n-1}}{n}\sum_{a=1}^{f}\chi\left(f-a\right)B_{n}\left(\frac{f-a}{f}\right)\\
&= \frac{\left(-1\right)^{n-1}\chi\left(-1\right)f^{n-1}}{n}\sum_{a'=0}^{f-1}\chi\left(a'\right)B_{n}\left(\frac{a'}{f}\right)\\
&= \left(-1\right)^{n}\chi\left(-1\right)L\left(1-n,\chi\right)
\end{aligned}$$

השוויון האחרון נכון אם $\chi\left(0\right)=\chi\left(f\right)=0$ ואז ניתן להחליף את גבולות הסכום. זה קורה כאשר $f\geq 2$.

אם $f=1$ אז $B_{n}=B_{n}\left(0\right)=\left(-1\right)^{n}B_{n}\left(1\right)$ ולכן ל-n זוגי ניתן לבצע את ההחלפה.
ל-n אי־זוגי (כאשר $n\geq 3$) גם ניתן לבצע את ההחלפה כי כזכור $B_{n}=0$ ל-n כנ"ל.
קיבלנו לכן כי לכל n טבעי ($n\geq 2$)

$$L\left(1-n,\chi\right) = \left(-1\right)^{n}\chi\left(-1\right)L\left(1-n,\chi\right)$$

מתקיים $\chi\left(-1\right)=\pm 1$ ולכן אם $\chi\left(-1\right)=\left(-1\right)^{n+1}$, מתקיים

$$L\left(1-n,\chi\right) = 0$$

(ולכן גם לכל $m\geq 2$ טבעי עם $m\equiv n\left(\mod 2\right)$, מתקיים $L\left(1-m,\chi\right)=0$)
ולכן

$$B_{n,\chi} = 0$$

לכל $n\geq 2$ טבעי אם $\chi\left(-1\right)=\left(-1\right)^{n+1}$.

משפט 6.7 (ללא הוכחה): גם הכיוון ההפוך נכון, כלומר אם $L\left(1-n,\chi\right)=0$ אז $\chi\left(-1\right)=\left(-1\right)^{n+1}$ ומתקיים

$$L\left(s,\chi\right) = \prod_{p\text{ is prime}}\frac{1}{1-\chi\left(p\right)p^{-s}}$$

נמשיך

$$\begin{aligned} L(1-n,\chi) &= -\frac{f^{n-1}}{n}\sum_{a=1}^{f}\chi(a)\,B_n\left(\frac{a}{f}\right) \\ &= -\frac{f^{n-1}}{n}\sum_{a=1}^{f}\chi(a)\sum_{k=0}^{n}\binom{n}{k}B_k\cdot\left(\frac{a}{f}\right)^{n-k} \\ &= -\frac{1}{fn}\sum_{a=1}^{f}\chi(a)\,a^n\sum_{k=0}^{n}\binom{n}{k}B_k\cdot\left(\frac{f}{a}\right)^{k} \end{aligned}$$

קיבלנו

$$L(1-n,\chi) = -\frac{1}{fn}\sum_{a=1}^{f}\chi(a)\,a^n\sum_{k=0}^{\infty}\binom{n}{k}B_k\cdot\left(\frac{f}{a}\right)^{k}$$

נשתמש בנוסחה זו על מנת להגדיר את פונקציית L ה־p־אדית.

6.2 הגדרת פונקציית L ה־p־אדית

כזכור, ל־$x \in \mathbb{Q}_p^*$ $0 \neq$ יש הצגה יחידה בצורה

$$x = p^{\nu_p(x)}\cdot\omega(x)\cdot\langle x\rangle$$

כאשר $\omega(x) \in \mu_{p-1} \subseteq \mathbb{Q}_p$ (μ_{p-1} היא חבורת שורשי היחידה מסדר $p-1$), $\langle x\rangle \in 1+p\mathbb{Z}_p$.
לכן אם $x \in \mathbb{Z}_p^*$,

$$\omega(x) \equiv x \pmod p$$

(כי $\nu_p(x) = 0$ ו־$\omega(x) \in \mathbb{Z}_p$)
כאשר $p = 2$, נשפץ פירוק זה כך ש־$x \in \mathbb{Z}_2^*$

$$\begin{aligned} \langle x\rangle &\in 1+4\mathbb{Z}_2 \\ \omega(x) &= \pm 1 \\ \omega(x) &\equiv x \pmod 4 \end{aligned}$$

תיאור השיפוץ: נכתוב

$$\begin{aligned} x &= 1+2a_1+4a_2+8a_3+\dots \\ &= 1+2a_1+4u \end{aligned}$$

כאשר $a_1 = 0,1$ ו־$u \in \mathbb{Z}_2$.
אם $a_1 = 0$ אז $\omega(x) = 1$ ו־$\langle x\rangle = x$.
אם $a_1 = 1$ אז

$$\begin{aligned} x &= 3+4u \\ &= -1+4(1+u) \\ &= -1(1+4v) \end{aligned}$$

כאשר $v=-1-u\in\mathbb{Z}_2$.
נבחר $\omega(x)=-1$, $\langle x\rangle=1+4v$.

הגדרה 6.8 נניח כי a טבעי זר לp ויהי F טבעי. נגדיר

$$H_p(a,s,F) = \frac{1}{F(s-1)}\langle a\rangle^{1-s}\sum_{k=0}^{\infty}\binom{1-s}{k}B_k\cdot\left(\frac{F}{a}\right)^k$$

נקראת פונקציית זטא של הורביץ. (הנוסחה מתקבלת מהסכום הפנימי בנוסחה

$$L(1-n,\chi) = -\frac{1}{fn}\sum_{a=1}^{f}\chi(a)a^n\sum_{k=0}^{\infty}\binom{n}{k}B_k\cdot\left(\frac{f}{a}\right)^k$$

ע"י החלפת $n\mapsto 1-s$)

נסמן $q=\begin{cases}p & p\neq 2\\ 4 & p=2\end{cases}$

משפט 6.9 נניח כי $q\mid F$. אז $(s-1)H_p(a,s,f)$ אנליטית בעיגול

$$|s-1|_p < qp^{-\frac{1}{p-1}}$$

כלומר, היא שווה לטור חזקות ב$s-1$ המתכנס בעיגול הנ"ל. ל$H_p(a,s,f)$ יש קוטב יחיד בעיגול זה והוא $s=1$. הקוטב פשוט והשארית שם היא $\frac{1}{F}$.

הוכחה: נתבונן בטור $\sum_{k=0}^{\infty}\binom{x}{k}\underbrace{B_k\cdot\left(\frac{F}{a}\right)^k}_{\alpha_k}$. ראינו כי אם קיימים $M>0$ ו$0<r<$ $p^{-\frac{1}{p-1}}$ כך ש$|\alpha_k|_p\le Mr^k$ לכל k, אז הטור מתכנס ושווה לטור חזקות בx בעיגול $|x|_p<R$ ל$R=\left(rp^{\frac{1}{p-1}}\right)^{-1}$.
ראינו (בפרק א') כי

$$|pB_k|_p \le 1$$

ולכן $|B_k|_p\le p$. נקבל

$$\begin{aligned}\left|B_k\cdot\left(\frac{F}{a}\right)^k\right|_p &\underbrace{\le}_{|a|_p=1} p\cdot|F|_p^k\\ &\underbrace{\le}_{q\mid F} p\cdot q^{-k}\end{aligned}$$

נקח $r=\frac{1}{q}$ ו$M=p$ ונקבל את הדרוש:

$$\begin{aligned}R &= \left(\frac{1}{q}\cdot p^{\frac{1}{p-1}}\right)^{-1}\\ &= q\cdot p^{-\frac{1}{p-1}}\end{aligned}$$

ב$s=1$ נקבל

$$\begin{aligned}\frac{1}{F}\langle a\rangle^{1-1}\sum_{k=0}^{\infty}\binom{1-1}{k}B_k\cdot\left(\frac{F}{a}\right)^k &= \frac{1}{F}\langle a\rangle^{0}\sum_{k=0}^{\infty}\binom{0}{k}B_k\cdot\left(\frac{F}{a}\right)^k\\ &= \frac{1}{F}\underbrace{\langle a\rangle^0}_{1}\underbrace{\binom{0}{0}}_{1}\underbrace{B_0}_{1}\cdot\underbrace{\left(\frac{F}{a}\right)^0}_{1}\\ &= \frac{1}{F}\end{aligned}$$

■

טענה 6.10 נניח כי $F \mid f$, אז

$$B_{n,\chi} = F^{n-1}\sum_{a=1}^{F}\chi(a)\cdot B_n\left(\frac{a}{F}\right)$$

כלומר

$$F^{n-1}\sum_{a=1}^{F}\chi(a)\cdot B_n\left(\frac{a}{F}\right) = f^{n-1}\sum_{a=1}^{f}\chi(a)\cdot B_n\left(\frac{a}{f}\right)$$

הוכחה:

$$\begin{aligned}L(s,\chi) &= \sum_{a=1}^{F}\chi(a)\sum_{n=0}^{\infty}\frac{1}{(a+nF)^s}\\ &= F^{-s}\sum_{a=1}^{F}\chi(a)\cdot\zeta\left(s,\frac{a}{F}\right)\end{aligned}$$

וראינו קודם כי

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}$$

■

הגדרה 6.11

$$L_p(s,\chi) = \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)H_p(a,s,F)$$

כאשר F נבחר כך ש$f,q \mid F$ ו

$$\chi:(\mathbb{Z}/f\mathbb{Z})^* \to \left\{z\in\mathbb{C}_p \mid z^{\phi(f)}=1\right\}$$

אי תלות ב־F תוכח בהמשך.

לכן אפשר לראות את χ כהומומורפיזם ל־$\mathbb{C}_p^*$ ונרחיבו לאפס על כל הטבעיים שאינם זרים ל־f.

משפט 6.12 $(s-1)\,L_p(s,\chi)$ אנליטית בעיגול $|s-1|_p < qp^{-\frac{1}{p-1}}$ (שווה לטור חזקות ב־$(s-1)$ - מתכנס)

כאשר $\chi \neq 1$, הפונקציה $L_p(s,\chi)$ אנליטית בעיגול הנ"ל. כאשר $\chi = 1$ יש לה קוטב פשוט ב־$s = 1$ והשארית היא $1 - \frac{1}{p}$.

הוכחה: בדיקת השארית ב־$s = 1$:

$$\begin{aligned}
\mathrm{Res}_{s=1} L_p(s,\chi) &= \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a) \cdot \mathrm{Res}_{s=1} H_p(a,s,F) \\
&= \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a) \cdot \frac{1}{F}
\end{aligned}$$

אם $\chi = 1$ נקבל

$$\begin{aligned}
\mathrm{Res}_{s=1} L_p(s,\chi) &= \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a) \cdot \frac{1}{F} \\
&= \frac{1}{F}\left(F - \frac{F}{p}\right) \\
&= 1 - \frac{1}{p}
\end{aligned}$$

אם $\chi \neq 1$ (כלומר $f > 1$) נקבל

$$\begin{aligned}
\mathrm{Res}_{s=1} L_p(s,\chi) &= \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a) \cdot \frac{1}{F} \\
&= \frac{1}{F}\sum_{a=1}^{F} \chi(a) - \frac{1}{F}\sum_{a=1}^{\frac{F}{p}} \chi(pa)
\end{aligned}$$

כיוון ש־$f \mid F$, מתקיים כי $\sum_{a=1}^{F} \chi(a)$ הוא כפולה שלמה של $\sum_{a=1}^{f} \chi(a) = 0$, ולכן הוא אפס.

באשר למחובר השני: אם $f \mid p$ אז pa לא זר ל־f ולכן $\chi(pa) = 0$ ולכן המחובר השני הוא אפס.

אם $p \nmid f$ אז $\chi(pa) = \chi(p)\,\chi(a)$ ונקבל כמו כן $f \mid \frac{F}{p}$

$$-\frac{1}{F}\sum_{a=1}^{\frac{F}{p}} \chi(pa) = -\frac{\chi(p)}{F}\sum_{a=1}^{\frac{F}{p}} \chi(a)$$

ושוב $\sum_{a=1}^{\frac{F}{p}} \chi(a)$ הוא כפולה שלמה של $0 = \sum_{a=1}^{f} \chi(a)$ ולכן אפס. ■

הגדרה 6.13 לχ פרימיטיבי מודלו f נאמר כי f הוא המנחה של χ (Conductor).
אם ξ כרקטר לא בהכרח פרימיטיבי

$$\xi : (\mathbb{Z}/N\mathbb{Z})^* \quad \to \quad \mathbb{C}^*$$

אז ל $N \mid n$ יש הומומורפיזם טבעי

$$\nu : (\mathbb{Z}/N\mathbb{Z})^* \quad \to \quad (\mathbb{Z}/n\mathbb{Z})^*$$

ל$N \mid n$ המינימלי כך שקיים $\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ כך ש

$$\chi \circ \nu \quad = \quad \xi$$

נקרא המנחה של ξ.

הגדרה 6.14 נניח כי χ_1 הוא כרקטר פרימיטיבי מודולו f_1 וχ_2 והא כרקטר פרימיטיבי מודולו f_2. נסמן $f = \mathrm{lcm}(f_1, f_2)$. אז נוכל להגדיר

$$\chi : (\mathbb{Z}/f\mathbb{Z})^* \quad \to \quad \mathbb{C}^*$$

ע"י $\chi(a + f\mathbb{Z}) = \chi_1(a) \cdot \chi_2(a)$. זהו הומומורפיזם.
יהי $f \mid f'$ המנחה של χ. (למשל, אם f_1, f_2 זרים, אז $f' = f_1 f_2$).
יהי ξ הכרקטר הפרימיטיבי מודולו f' כך ש χ הוא ההרכבה

$$(\mathbb{Z}/f\mathbb{Z})^* \quad \to \quad (\mathbb{Z}/f'\mathbb{Z})^* \underset{\to}{\xi} \mathbb{C}^*$$

מסמנים $\xi = \chi_1 \cdot \chi_2$ ומרחיבים לכל $\mathbb{N}$, כרגיל.

תרגיל: לכל a טבעי מתקיים

$$\xi(a) \quad = \quad \chi_1(a) \cdot \chi_2(a)$$

אלא אם $\chi_1(a) = \chi_2(a) = 0$.
נסתכל כעת על הסכום

$$L_p(1-n, \chi) \quad = \quad \sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi(a) H_p(a, 1-n, F)$$

לn טבעי (ניתן כי $|1-n|_p \leq 1 < qp^{-\frac{1}{p-1}}$)

$$\begin{aligned}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\,H_p(a,1-n,F) &= -\frac{1}{nF}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\langle a\rangle^n\sum_{k=0}^{\infty}\binom{n}{k}\left(\frac{F}{a}\right)^k B_k\\ &= -\frac{1}{nF}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\langle a\rangle^n\sum_{k=0}^{\infty}\binom{n}{k}\left(\frac{F}{a}\right)^{n-k} B_{n-k}\\ &= -\frac{F^{n-1}}{n}\sum_{\substack{a=1\\ p\nmid a}}^{F}\underbrace{\left(\frac{\langle a\rangle}{a}\right)^n}_{\omega(a)^{-n}}\chi(a)\underbrace{\sum_{k=0}^{\infty}\binom{n}{k}B_{n-k}\cdot\left(\frac{a}{F}\right)^k}_{B_n\left(\frac{a}{F}\right)}\end{aligned}$$

מהיחידות בשוויון $a=\omega(a)\langle a\rangle$ נובע כי ω מגדיר כרקטר פרימיטיבי מודולו p:

$$\begin{aligned}\omega:\mathbb{Z}_p^* &\to \mu_{p-1}\subseteq\mathbb{Q}_p^*\\ \omega(xy) &= \omega(x)\,\omega(y)\end{aligned}$$

כי $x=\omega(x)\langle x\rangle$ ו־$y=\omega(y)\langle y\rangle$ ולכן $xy=\underbrace{\omega(x)\,\omega(y)}_{\in\mu_{P-1}}\underbrace{\langle x\rangle\langle y\rangle}_{\in 1+q\mathbb{Z}_p}$ ולכן מהיחידות (ל־$p\neq 2$)
נקבל כי

$$\begin{aligned}\omega(xy) &= \omega(x)\,\omega(y)\\ \langle x\rangle\langle y\rangle &= \langle xy\rangle\end{aligned}$$

מתקיים כי $\omega\,|_{\mathbb{Z}\cap\mathbb{Z}_p^*}$ היא פונקציה קבועה על מחלקות מודולו p: אם $n\equiv m\ (\bmod p)$ זרים ל־p אז

$$\begin{aligned}n &= m+lp\\ &= m\left(1+\underbrace{\frac{l}{m}}_{\in\mathbb{Z}_p}p\right)\\ &= \omega(m)\underbrace{\langle m\rangle\left(1+\frac{l}{m}p\right)}_{\langle n\rangle}\end{aligned}$$

לכן אפשר לראות את ω כהומומורפיזם

$$(\mathbb{Z}/p\mathbb{Z})^* \to \mu_{p-1}$$

הוא לא טריוואלי כי $\omega(x)\equiv x\ (\bmod p)$ ולכן נראה את ω ככרקטר פרימיטיבי מודולו p.
(ל־$p=2$ כרקטר פרימיטיבי מודולו $q=4$)
(ומרחיבים לכל $\mathbb{N}$ כרגיל)

נסמן ב־$\chi\omega^{-n}$ את הכרקטר הפרימיטיבי המתאים למכפלה. נמשיך

$$\begin{aligned} L_p(1-n,\chi) &= -\frac{F^{n-1}}{n}\sum_{\substack{a=1\\ p\nmid a}}^{F}\omega(a)^{-n}\chi(a)B_n\left(\frac{a}{F}\right) \\ &= -\frac{F^{n-1}}{n}\sum_{\substack{a=1\\ p\nmid a}}^{F}\left(\chi\omega^{-n}\right)(a)B_n\left(\frac{a}{F}\right) \end{aligned}$$

השוויון האחרון נכון כי כיוון ש־$p\nmid a$ אז $\omega(a)\neq 0$, ואז לפי התרגיל $\left(\chi\omega^{-n}\right)(a)=\chi(a)\,\omega(a)^{-n}$.

$$\begin{aligned} L_p(1-n,\chi) &= -\frac{F^{n-1}}{n}\sum_{\substack{a=1\\ p\nmid a}}^{F}\left(\chi\omega^{-n}\right)(a)B_n\left(\frac{a}{F}\right) \\ &= -\frac{F^{n-1}}{n}\sum_{a=1}^{F}\left(\chi\omega^{-n}\right)(a)B_n\left(\frac{a}{F}\right)+\frac{F^{n-1}}{n}\sum_{a=1}^{\frac{F}{p}}\left(\chi\omega^{-n}\right)(ap)B_n\left(\frac{ap}{F}\right) \\ &= -\frac{B_{n,\chi\omega^{-n}}}{n}+\frac{p^{n-1}}{n}\left(\frac{F}{p}\right)^{n-1}\sum_{a=1}^{\frac{F}{p}}\left(\chi\omega^{-n}\right)(ap)B_n\left(\frac{a}{F/p}\right) \end{aligned}$$

נסמן ב־$f_{\chi\omega^{-n}}$ את המנחה של הכרקטר $\chi\omega^{-n}$.
אם $p\mid f_{\chi\omega^{-n}}$, אז

$$\left(\chi\omega^{-n}\right)(ap) = 0$$

והמחובר השני שווה ל־0.
אם $p\nmid f_{\chi\omega^{-n}}$ נקבל במחובר השני

$$\frac{1}{n}\left(\chi\omega^{-n}\right)(p)\,p^{n-1}\left(\frac{F}{p}\right)^{n-1}\sum_{a=1}^{\frac{F}{p}}\left(\chi\omega^{-n}\right)(a)B_n\left(\frac{a}{F/p}\right) = \frac{1}{n}\left(\chi\omega^{-n}\right)(p)\,p^{n-1}B_{n,\chi\omega^{-n}}$$

בסה"כ קיבלנו

$$\begin{aligned} L_p(1-n,\chi) &= -\frac{B_{n,\chi\omega^{-n}}}{n}\left(1-\left(\chi\omega^{-n}\right)(p)\,p^{n-1}\right) \\ &= \left(1-\left(\chi\omega^{-n}\right)(p)\,p^{n-1}\right)\left(-\frac{B_{n,\chi\omega^{-n}}}{n}\right) \\ &= \left(1-\left(\chi\omega^{-n}\right)(p)\,p^{n-1}\right)L\left(1-n,\chi\omega^{-n}\right) \end{aligned}$$

הערה 6.15 כדי שתהיה משמעות לביטויים $L\left(1-n,\chi\omega^{-n}\right)$, $B_{n,\chi\omega^{-n}}$, אנחנו תחילה קובעים שיכון $i:\mathbb{Q}_p\left(\mu_{p-1}\right)\to\mathbb{C}$ ומסתכלים על הכרקטרים תחת תמונת שיכון זה.

נסכם:

משפט 6.16 קיימת פונקציית L, p־אדית, אנליטית $L_p(s,\chi)$ בעיגול $|s-1|_p < qp^{-\frac{1}{p-1}}$, פרט, אולי, לקוטב פשוט ב$s=1$.

אם $\chi \neq 1$ אז $L_p(s,\chi)$ אנליטית בעיגול, ואם $\chi = 1$ אז יש ל$L_p(s,\chi)$ קוטב פשוט ב$s=1$, שם השארית שווה ל$1-\frac{1}{p}$.

הפונקציה נתונה באופן הבא: נבחר F טבעי כך ש$F \mid f, q$ ואז

$$L_p(s,\chi) = \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a) H_p(a,s,F)$$

ומתקיים לכל n טבעי

$$\begin{aligned} L_p(1-n,\chi) &= \left(1-\left(\chi\omega^{-n}\right)(p)\,p^{n-1}\right)\left(-\frac{B_{n,\chi\omega^{-n}}}{n}\right) \\ &= \left(1-\left(\chi\omega^{-n}\right)(p)\,p^{n-1}\right) L\left(1-n,\chi\omega^{-n}\right) \end{aligned}$$

(ω נקרא כרקטר של Teichmuller)

ולבסוף, הפונקציה אינה תלויה בF:

יהיו F_1, F_2 עם $F_i \mid f, q$. אז הביטויים $(s-1)L_p(s,\chi,F_1)$ ו$(s-1)L_p(s,\chi,F_2)$ שווים על המספרים השלמים השליליים. (אלה נמצאים בעיגול ההתכנסות $|s-1|_p <$ $qp^{-\frac{1}{p-1}}$)

טור חזקות שיש לו אינסוף אפסים בעיגול ההתכנסות הוא זהותית אפס.

הערה 6.17 ראינו כי

$$L\left(1-n,\chi\omega^{-n}\right) = 0$$

אם ורק אם $\left(\chi\omega^{-n}\right)(-1) = (-1)^{n+1}$ (לכל $n \geq 2$).

מתקיים כי $\omega(-1) = -1$ ולכן $\omega^{-n}(-1) = (-1)^n$ ולכן $\left(\chi\omega^{-n}\right)(-1) = (-1)^{n+1}$ אם ורק אם $\chi(-1) = -1$.

לכן $\chi(-1) = -1$ אם ורק אם $L_p(1-n,\chi) = 0$ לכל $n \geq 2$ טבעי, כלומר $L_p(-m,\chi) = 0$ לכל m טבעי ולכן $L_p(s,\chi) = 0$ זהותית.

לכן המקרה היחיד שמעניין הוא כאשר $\chi(-1) = 1$ (נקרא "כרקטר זוגי").

כאן $L_p(1-n,\chi) \neq 0$ לכל $n \geq 2$.

משפט 6.18 נניח כי $\chi \neq 1$ ונניח כי $pq \nmid f$. נתבונן בפיתוח לטור חזקות, סביב $s=1$, $|s-1|_p < qp^{-\frac{1}{p-1}}$. אז בעיגול ההתכנסות

$$L_p(s,\chi) = \sum_{i=0}^{\infty} a_i (s-1)^i$$

אז לכל $i \geq 1$ מתקיים $|a_i|_p \leq p^{-1}$ וכן $|a_0|_p \leq 1$.

הוכחה: (ארוכה)
נבחר F טבעי כך ש$F \mid f, q$, כך ש$F \nmid pq$.

$$\left|\left(\frac{F}{a}\right)^k B_k\right|_p \leq q^{-k}\cdot p$$

לכן מאחר והוכחנו כי

$$\left|\frac{1}{k!}\right|_p \leq p^{\frac{k-1}{p-1}}$$

נקבל כי

$$\left|\frac{1}{k!}\cdot\left(\frac{F}{a}\right)^k B_k\right|_p \leq q^{-k}\cdot p\cdot p^{\frac{k-1}{p-1}}$$

אם $p\neq 2$ אז נקבל

$$\begin{aligned} q^{-k}\cdot p\cdot p^{\frac{k-1}{p-1}} &= p^{-k}\cdot p\cdot p^{\frac{k-1}{p-1}} \\ &= p^{(k-1)\left(-1+\frac{1}{p-1}\right)} \\ &= p^{-\frac{(k-1)(p-2)}{p-1}} \end{aligned}$$

נטען כי $p^{-\frac{(k-1)(p-2)}{p-1}} < p^{-1}$ לכל $k>3$. אי השוויון בין המעריכים:

$$\begin{aligned} (k-1)(p-2) &> (p-1) \\ &\Longleftrightarrow \\ (k-2)(p-1) &> 1 \end{aligned}$$

והוא נכון ל$k>3$.
ל$k=3$ נקבל $\left|\frac{1}{k!}\cdot\left(\frac{F}{a}\right)^k B_k\right|_p = 0 < p^{-1}$ כי $B_3=0$.
כאשר $p=2$:

$$\begin{aligned} q^{-k}\cdot p\cdot p^{\frac{k-1}{p-1}} &= 2\cdot 4^{-k}\cdot 2^{k-1} \\ &= 2^{-k} \\ &< \frac{1}{4} \end{aligned}$$

ל$k\geq 3$.
לכן קיבלנו לכל $k\geq 3$ כי

$$\left|\frac{1}{k!}\left(\frac{F}{a}\right)^k B_k\right|_p < \frac{1}{q}$$

נשים לב כי

$$\begin{aligned}\binom{1-s}{k} &= \frac{1}{k!}\prod_{i=0}^{k-1}(1-s-i)\\ &= \frac{1}{k!}\sum_{j=0}^{k}c_j(s-1)^j\end{aligned}$$

כאשר $c_j \in \mathbb{Z}$. לכן ל-$k \geq 3$

$$\frac{1}{F}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k = \sum_{j=0}^{k}\alpha_j(s-1)^j$$

כאשר $\alpha_j \in \mathbb{Q}$ כך ש

$$\begin{aligned}\left|\alpha_j\right|_p &= \left|\frac{1}{F}\cdot\frac{1}{k!}\cdot c_j\cdot\left(\frac{F}{a}\right)^k B_k\right|_p\\ &= \left|\frac{1}{F}\right|_p\cdot\left|\frac{1}{k!}\left(\frac{F}{a}\right)^k B_k\right|_p\cdot\left|c_j\right|_p\\ &< \left|\frac{1}{F}\right|_p\cdot\frac{1}{q}\end{aligned}$$

לפי בחירת F,

$$|F|_p = \frac{1}{q}$$

לכן $\left|\alpha_j\right|_p < 1$.
כיוון ש-$\alpha_j \in \mathbb{Q}$, נקבל כי $\left|\alpha_j\right|_p \leq p^{-1}$ לכן

$$\frac{1}{F}\sum_{k=0}^{\infty}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k \equiv \frac{1}{F}\sum_{k=0}^{2}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k \pmod p$$

כעת

$$\begin{aligned}\langle a\rangle^{1-s} &= \exp_p\left((1-s)\operatorname{Log}_p\langle a\rangle\right)\\ &= \sum_{n=0}^{\infty}\frac{(-1)^n\left(\operatorname{Log}_p\langle a\rangle\right)^n}{n!}(s-1)^n\end{aligned}$$

מתקיים

$$\langle a\rangle \equiv 1 \pmod q$$

$$\operatorname{Log}_p\langle a\rangle = \sum_{n=0}^{\infty}\frac{(-1)^{n+1}}{n}\left(\langle a\rangle-1\right)^n$$

נעריך:

$$\begin{aligned}\left|\mathrm{Log}_p\left\langle a\right\rangle\right|_p &\le \max_{n\ge1}\frac{\left|\left\langle a\right\rangle-1\right|_p^n}{|n|_p}\\ &\le \max_{n\ge1}\left\{q^{-n}\cdot p^{\log_p n}\right\}\\ &\le \begin{cases}p^{-1} & p\neq2\\ \frac{1}{4}=q^{-1} & p=2\end{cases}\end{aligned}$$

כי

$$p^{\log_p n-n} \le p^{-1}$$

לכל $n\ge1$ ו

$$2^{\log_2 n-2n} \le 2^{-2}$$

ולכן

$$\left|\mathrm{Log}_p\left\langle a\right\rangle\right|_p \le q^{-1}$$

ולכן נקבל

$$\begin{aligned}\left|\frac{\left(\mathrm{Log}_p\left\langle a\right\rangle\right)^n}{n!}\right|_p &\le \frac{q^{-n}}{|n!|_p}\\ &\le q^{-n}\cdot p^{\left[\frac{n-1}{p-1}\right]}\end{aligned}$$

לכל $n\ge2$:

$$q^{-n}\cdot p^{\left[\frac{n-1}{p-1}\right]} \le p^{-1}q^{-1}$$

$p\neq2$: רוצים

$$p^{-n}\cdot p^{\frac{n-1}{p-1}} \le p^{-2}$$

צריך:

$$\begin{aligned}-n+\frac{n-1}{p-1} &\le -2\\ -np+2n-1 &\le -2p+2\\ -n\left(p-2\right) &\le -2p+4-1\\ \left(2-n\right)\left(p-2\right) &\le -1\end{aligned}$$

זה נכון לכל $n\ge3$.
לכל $n=2$:

$$\begin{aligned}q^{-n}\cdot p^{\left[\frac{n-1}{p-1}\right]} &= q^{-2}\cdot p^{\left[\frac{1}{p-1}\right]}\\ &= q^{-2}\\ &= p^{-2}\\ &\le p^{-2}\end{aligned}$$

כאשר $p=2$:

$$\begin{aligned}4^{-n}\cdot 2^{n-1} &\le 2^{-1}\cdot 4^{-1}\\ 2^{-n} &\le 4^{-1}\end{aligned}$$

נכון ל-$n\ge 2$.
לכן

$$\langle a\rangle^{1-s} \equiv 1-\mathrm{Log}_p\langle a\rangle (s-1) \pmod{pq}$$

(כי לשאר איברי הטור מתקיים $\left|\frac{(\mathrm{Log}_p\langle a\rangle)^n}{n!}\right|_p < p^{-1}q^{-1}$)
נכתוב

$$\frac{1}{F}\sum_{k=0}^{\infty}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k = \frac{1}{F}\sum_{k=0}^{2}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k + f_1(s-1)$$

כאשר

$$f_1(s-1) = \sum_{j=1}^{\infty} d_j (s-1)^j$$

עם $|d_j|_p \le p^{-1}$.

$$\langle a\rangle^{1-s} = 1-\mathrm{Log}_p\langle a\rangle (s-1) + f_2(s-1)$$

כאשר

$$f_2(s-1) = \sum_{j=2}^{\infty} t_j (s-1)^j$$

עם $|t_j|_p \le p^{-1}q^{-1}$

$$L_p(s,\chi) = \frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\left(1-\mathrm{Log}_p\langle a\rangle (s-1) + f_2(s-1)\right)\cdot\left(\frac{1}{F}\sum_{k=0}^{2}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k + f_1(s-1)\right)$$

כעת

$$\left(1-\mathrm{Log}_p\langle a\rangle (s-1)\right) f_1(s-1) = f_1(s-1) - \sum_{j=1}^{\infty} d_j \mathrm{Log}_p\langle a\rangle (s-1)^{j+1}$$

ומתקיים

$$\begin{aligned}\left|d_j \mathrm{Log}_p\langle a\rangle\right|_p &\le p^{-1}q^{-1}\\ &< p^{-1}\end{aligned}$$

נשאר להעריך את הסכומים הבאים:

- $\frac{1}{F}\sum_{k=0}^{2}\binom{1-s}{k}\left(\frac{F}{a}\right)^{k}B_{k}\cdot f_{2}\left(s-1\right)$
- $\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi\left(a\right)\left(1-\mathrm{Log}_{p}\left\langle a\right\rangle \left(s-1\right)\right)\frac{1}{F}\sum_{k=0}^{2}\binom{1-s}{k}\left(\frac{F}{a}\right)^{k}B_{k}$

נחשב

$$\begin{aligned}\frac{1}{F}\sum_{k=0}^{2}\binom{1-s}{k}\left(\frac{F}{a}\right)^{k}B_{k} &= \frac{1}{F}+\frac{1}{F}\left(1-s\right)\frac{F}{a}\left(-\frac{1}{2}\right)+\frac{1}{F}\cdot\frac{\left(1-s\right)\left(-s\right)}{2}\cdot\left(\frac{F}{a}\right)^{2}\left(\frac{1}{6}\right)\\ &= \frac{1}{F}+\frac{1}{2a}\left(s-1\right)+\frac{F}{12a^{2}}s\left(s-1\right)\\ &= \frac{1}{F}+\left(\frac{1}{2a}+\frac{F}{12a^{2}}\right)\left(s-1\right)+\frac{F}{12a^{2}}\left(s-1\right)^{2}\end{aligned}$$

מתקיים

$$\begin{aligned}\left|\frac{1}{F}\right|_{p} &= q\\ \left|\frac{1}{2a}\right|_{p} &= \begin{cases}1 & p\neq2\\ 2 & p=2\end{cases}\\ \left|\frac{F}{12a^{2}}\right|_{p} &= \left|\frac{F}{12}\right|_{p}\\ &= \begin{cases}1 & p=2,3\\ p^{-1} & p\neq2,3\end{cases}\end{aligned}$$

לכן

$$\left|\frac{1}{2a}+\frac{F}{12a^{2}}\right|_{p} = \begin{cases}2 & p=2\\ \leq1 & p=3\\ =1 & p\neq2,3\end{cases}$$

בפרט, כל המקדמים בעלי ערך מוחלט $\geq q$.

נכתוב

$$L_{p}\left(s,\chi\right) = \sum_{i=0}^{\infty}a_{i}\left(s-1\right)^{i}$$

מתקיים מהחישוב שעשינו כי

$$L_{p}\left(s,\chi\right) \equiv \frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi\left(a\right)\left(1-\left(\mathrm{Log}_{p}\left\langle a\right\rangle \right)\left(s-1\right)\right)\cdot\left(\frac{1}{F}+\left(\frac{1}{2a}+\frac{F}{12a^{2}}\right)\left(s-1\right)+\frac{F}{12a^{2}}\left(s-1\right)^{2}\right)$$
$$\left(\mod p\right)$$

נעריך את $|a_0|_p$:

$$a_0 \equiv \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)\left(-\left(\mathrm{Log}_p\langle a\rangle\right)\frac{1}{F}+\left(\frac{1}{2a}+\frac{F}{12a^2}\right)\right)(\mod p)$$

מתקיים

$$\begin{aligned}\left|\frac{\mathrm{Log}_p\langle a\rangle}{F}\right|_p &= q\left|\mathrm{Log}_p\langle a\rangle\right|_p\\ &\leq 1\end{aligned}$$

ולכל $p\neq 2$ מתקיים

$$\left|\frac{1}{2a}+\frac{F}{12a^2}\right|_p \leq 1$$

אם $p=2$, נקבל כי $\left|\frac{F}{12a^2}\right|_p=1$ ולכן מספיק לחשב

$$\sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)\left(\frac{1}{2a}\right)(\mod p) \equiv \frac{1}{2}\sum_{\substack{a=1\\ p\nmid a}}^{F}\left(\frac{\chi(a)}{a}\right)(\mod p)$$

נחשב סכום זה: נטען כי לכל p ראשוני (לאו דווקא $p=2$) מתקיים:

$$\sum_{\substack{a=1\\ p\nmid a}}^{F}\left(\frac{\chi(a)}{a}\right) = 0(\mod p)$$

לא $p\nmid a$ מתקיים

$$a \equiv \omega(a)(\mod q)$$

מתקיים

$$\omega(a) = a(1+u)$$

כאשר $|u|_p\leq q^{-1}$.

$$\frac{\chi(a)}{a} = \frac{\chi(a)}{\omega(a)}(1+u)$$

מתקיים

$$\frac{\chi(a)}{\omega(a)}(1+u) \equiv \frac{\chi(a)}{\omega(a)}(\mod q)$$

ולכן

$$\frac{\chi(a)}{a} \equiv \frac{\chi(a)}{\omega(a)} \pmod q$$

נקבל גם (אם $q=4$)

$$\frac{1}{2}\frac{\chi(a)}{a} \equiv \frac{1}{2}\frac{\chi(a)}{\omega(a)}\left(\mod \frac{1}{2}q\right)$$

ולכן

$$\frac{1}{2}\sum_{\substack{a=1\\p\nmid a}}^{F}\left(\frac{\chi(a)}{a}\right) = \frac{1}{2}\sum_{\substack{a=1\\p\nmid a}}^{F}\left(\frac{\chi(a)}{\omega(a)}\right) \pmod p$$

(כי אם $q=4$, $p=\frac{1}{2}q$, אחרת 2 הפיך מודולו p)
אפשר להניח מראש כי $\chi(-1)=1$ (אחרת ראינו כי L יוצאת פונקציית האפס), ואז

$$\frac{\chi(-1)}{\omega(-1)} = \frac{1}{\omega(-1)} = -1$$

ולכן $\frac{\chi}{\omega}$ כרקטר לא טריוואלי ולכן

$$\sum_{\substack{a=1\\p\nmid F}}^{F}\frac{\chi(a)}{\omega(a)} = 0$$

ולכן $|a_0|_p \le 1$.
כעת נעריך את a_1

$$a_1 \equiv \sum_{a=1}^{F}\chi(a)\left(\frac{F}{12a^2} - \mathrm{Log}_p\langle a\rangle\left(\frac{1}{2a}+\frac{F}{12a^2}\right)\right) \pmod p$$

לפי ההערכות הנ"ל:

$$\left|\underbrace{\mathrm{Log}_p\langle a\rangle}_{\le q^{-1}}\cdot\left(\frac{1}{2a}+\frac{F}{12a^2}\right)\right|_p \le p^{-1}$$

אם $p\neq 2,3$ אז $\left|\frac{F}{12a^2}\right|_p = p^{-1}$.
נניח $p=2,3$. אז

$$a_1 \equiv \frac{F}{12}\sum_{\substack{a=1\\p\nmid a}}^{F}\frac{\chi(a)}{a^2} \pmod p$$

כאן $a^2 \equiv 1 \pmod p$ ולכן

$$\sum_{\substack{a=1\\p\nmid a}}^{F}\frac{\chi(a)}{a^2} \equiv \sum_{\substack{a=1\\p\nmid a}}^{F}\chi(a) \equiv 0 \pmod p$$

וכמו כן $\left|\frac{F}{12}\right|_p = 1$ ל-$p = 2,3$. ולכן

$$|a_1|_p \leq p^{-1}$$

באשר ל-a_2:

$$a_2 \equiv -\sum_{\substack{a=1\\p\nmid a}}^{F}\chi(a)\frac{F}{12a^2}\mathrm{Log}_p\langle a\rangle \pmod p$$

ומאחר ולא $p \nmid a$ מתקיים

$$\left|\frac{F}{12a^2}\mathrm{Log}_p\langle a\rangle\right|_p \leq q^{-1}$$

נובע כי

$$|a_2|_p \leq p^{-1}$$

■

מסקנה 6.19 (מההוכחה): נניח כי $\chi \neq 1$ וכי $pq \nmid f$. נבחר F טבעי, כך ש-$q, f \mid F$ ו-$pq \nmid F$. אז

$$L_p(1,\chi) \equiv -\frac{1}{F}\sum_{\substack{a=1\\p\nmid a}}^{F}\mathrm{Log}_p\langle a\rangle \pmod p$$

הוכחה: בסימונים הקודמים

$$\begin{aligned} L_p(1,\chi) &= a_0 \\ &\equiv \sum_{\substack{a=1\\p\nmid a}}^{F}\chi(a)\left(-\left(\mathrm{Log}_p\langle a\rangle\right)\frac{1}{F}+\left(\frac{1}{2a}+\frac{F}{12a^2}\right)\right) \pmod p \end{aligned}$$

ראינו באופן כללי (לכל p)

$$\sum_{\substack{a=1\\p\nmid a}}^{F}\frac{\chi(a)}{2a} \equiv 0 \pmod p$$

בנוסף אם $p=2,3$ ראינו כי

$$\sum_{\substack{a=1\\p\nmid a}}^{F}\chi\left(a\right)\frac{F}{12a^{2}}\equiv0\left(\mod p\right)$$

ואם $p\neq2,3$ ראינו כי

$$\left|\frac{F}{12a^{2}}\right|_{p}\leq p^{-1}$$

ולכן

$$\left|\chi\left(a\right)\frac{F}{12a^{2}}\right|_{p}\leq p^{-1}$$

ולכן

$$\chi\left(a\right)\frac{F}{12a^{2}}\equiv0\left(\mod p\right)$$

ומכאן

$$\sum_{\substack{a=1\\p\nmid a}}^{F}\chi\left(a\right)\frac{F}{12a^{2}}\equiv0\left(\mod p\right)$$

לכן

$$L_{p}\left(1,\chi\right)\equiv\frac{1}{F}\sum_{\substack{a=1\\p\nmid a}}^{F}\chi\left(a\right)\left(-\left(\operatorname{Log}_{p}\left\langle a\right\rangle\right)\right)\left(\mod p\right)$$

(אולי ניתן להוכיח זאת ישירות בלי להסתבך, זה ההסבר שאני מצאתי) ∎

מסקנה 6.20 באותם תנאים, לכל $m,n\in\mathbb{Z}$ מתקיים

$$L_{p}\left(n,\chi\right)\equiv L_{p}\left(m,\chi\right)\left(\mod p\right)$$

הוכחה: מספיק להראות

$$\sum_{i=1}^{\infty}a_{i}\left(n-1\right)^{i}\equiv\sum_{i=1}^{\infty}a_{i}\left(m-1\right)^{i}\left(\mod p\right)$$

מתקיים

$$\begin{aligned}\left|a_{i}\left(n-1\right)^{i}\right|_{p} &\leq \left|a_{i}\right|_{p}\\ &\leq p^{-1}\end{aligned}$$

לכל $i\geq1$. ∎

נראה כעת הוכחה נוספת של קונגרואנציית Kummer.

משפט 6.21 (תזכורת): יהיו $m,n\geq 2$ טבעיים כך ש־$p-1\nmid m,n$, וכן $m\equiv n\left(\mod\phi\left(p^{l}\right)\right)$.
אז

$$\left(1-p^{n-1}\right)\frac{B_{n}}{n}\equiv\left(1-p^{n-1}\right)\frac{B_{m}}{m}\left(\mod p^{l}\right)$$

הוכחה: מהנתון $p\neq 2$. יהי $\chi=\omega^{n}\neq 1$ (כי $p-1\nmid n$)

$$\begin{aligned}L_{p}\left(1-n,\chi\right) &= \left(1-\underbrace{\left(\chi\omega^{-n}\right)}_{1}\left(p\right)\left(p^{n-1}\right)\right)\left(-\frac{B_{n,\chi\omega^{-n}}}{n}\right)\\ &= -\left(1-p^{n-1}\right)\frac{B_{n}}{n}\end{aligned}$$

לכן

$$\left(1-p^{n-1}\right)\frac{B_{n}}{n}=-L_{p}\left(1-n,\omega^{n}\right)$$

מתקיים $\omega^{n}=\omega^{m}$ כי $n\equiv m\left(\mod\left(p-1\right)\right)$.
נקבל

$$\begin{aligned}\left(1-p^{n-1}\right)\frac{B_{n}}{n} &= -L_{p}\left(1-n,\omega^{n}\right)\\ &= -\sum_{i=0}^{\infty}a_{i}\left(-n\right)^{i}\\ &\equiv -\sum_{i=0}^{\infty}a_{i}\left(-m\right)^{i}\left(\mod p^{l}\right)\end{aligned}$$

כי $n\equiv m\left(\mod p^{l-1}\right)$ ו־$\left|a_{i}\right|_{p}\leq p^{-1}$ לכל $i\geq 1$. לכן

$$\begin{aligned}\left(1-p^{n-1}\right)\frac{B_{n}}{n} &\equiv -\sum_{i=0}^{\infty}a_{i}\left(-m\right)^{i}\left(\mod p^{l}\right)\\ &= -L_{p}\left(1-m,\omega^{n}\right)\\ &= -L_{p}\left(1-m,\omega^{m}\right)\\ &= \left(1-p^{m-1}\right)\frac{B_{m}}{m}\end{aligned}$$

וקיבלנו לכן

$$\left(1-p^{n-1}\right)\frac{B_{n}}{n}\equiv\left(1-p^{m-1}\right)\frac{B_{m}}{m}\left(\mod p^{l}\right)$$

כנדרש. ■

משפט 6.22 יהי n טבעי אי־זוגי. נניח כי $n+1 \nmid p-1$, אז

$$B_{1,\omega^{n}} \equiv \frac{B_{n+1}}{n+1} \pmod p$$

הוכחה: כיוון ש$n+1 \nmid p-1$, מתקיים כי $p \neq 2$ וכן כי $\omega^{n+1} \neq 1$.

כיוון שn אי־זוגי, $\omega^{n} \neq 1$ (אחרת נקבל $n \mid p-1$, אבל n אי־זוגי) מתקיים

$$L_p(1-m,\chi) = \left(1-\left(\chi\omega^{-m}\right)(p)\,p^{m-1}\right)\left(-\frac{B_{m,\chi\omega^{-m}}}{m}\right)$$

נציב $m=1$, $\chi=\omega^{n+1}$ ונקבל

$$L_p(0,\chi) = \left(1-\left(\omega^{n}\right)(p)\right)\left(-B_{1,\omega^{n}}\right)$$

אבל $\left(\omega^{n}\right)(p)=0$, כי ω הוא כרקטר פרימיטיבי מודולו p. לכן

$$\begin{aligned}
B_{1,\omega^{n}} &= -L_p\left(0,\omega^{n+1}\right)\\
&\equiv -L_p\left(1-(n+1),\omega^{n+1}\right) \pmod p\\
&\equiv -\left(1-\left(\omega^{n+1}\cdot\omega^{-(n+1)}\right)(p)\,p^{n+1-1}\right)\left(-\frac{B_{n+1,\omega^{n+1}\cdot\omega^{-(n+1)}}}{n+1}\right)\\
&\equiv -\left(1-p^{n}\right)\left(-\frac{B_{n+1,1}}{n+1}\right)\\
&\equiv \left(1-p^{n}\right)\frac{B_{n+1}}{n+1}\\
&\equiv \frac{B_{n+1}}{n+1}-p^{n}\frac{B_{n+1}}{n+1} \pmod p\\
&\equiv \frac{B_{n+1}}{n+1} \pmod p
\end{aligned}$$

כאשר המעבר האחרון נכון כי מקונגרונאציית Adams מתקיים כי $p^{n}\frac{B_{n+1}}{n+1}$ הוא שלם מודולו p. ∎

משפט 6.23 (Brumer):

$$L_p(1,\chi) \neq 0$$

לא נוכל להוכיח משפט זה. נוכיח מקרה פרטי שלו:

משפט 6.24 יהי p מספר ראשוני רגולרי ($B_k=\frac{U_k}{V_k}$, $p \nmid U_k$ לכל $k \leq p-3$). יהי k טבעי זוגי, כך ש$k \nmid p-1$, $k \leq p-3$. אז

$$L_p\left(1,\omega^{k}\right) \not\equiv 0 \pmod p$$

(ולכן $\left|L_p\left(1,\omega^k\right)\right|_p = 1$)
ובפרט

$$L_p\left(1,\omega^k\right) \neq 0$$

הוכחה:

$$L_p\left(1-k,\omega^k\right) = \left(1-\left(\omega^k\cdot\omega^{-k}\right)(p)\,p^{k-1}\right)\left(-\frac{B_k}{k}\right)$$

כיוון ש$k \nmid p-1$, $\omega^k \neq 1$. כמו כן, $p \neq 2$.

$$\begin{aligned}-L_p\left(1-k,\omega^k\right) &= \left(1-p^{k-1}\right)\frac{B_k}{k}\\ -L_p\left(1-k,\omega^k\right) &\equiv -L_p\left(1,\omega^k\right)\left(\mod p\right)\end{aligned}$$

($\chi \neq 1$, $pq \nmid f$)
לכן

$$L_p\left(1,\omega^k\right) \equiv \left(p^{k-1}-1\right)\frac{B_k}{k}\left(\mod p\right)$$

$p \nmid k$ כי $k \leq p-3$
$B_k = \frac{U_k}{V_k}$, $p \nmid U_k$. ראינו כי $p \mid V_k \iff k \mid p-1$, לכן $p \nmid V_k$, מכאן $\left|B_k\right|_p = 1$
כעת

$$\left|p^{k-1}-1\right|_p = 1$$

ולכן

$$\left|L_p\left(1,\omega\right)\right|_p = 1$$

■

בתנאי המשפט

$$L_p\left(1,\chi\right) \equiv -\frac{1}{F}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi\left(a\right)\operatorname{Log}_p\langle a\rangle\left(\mod p\right)$$

נניח כי χ כרקטר פרימיטיבי מודולו $p \neq 2$ ($f = p$).
אפשר לבחור $F = p$ (כי $f \mid F$, $q \mid F$ ו$pq \nmid F$)

$$L_p\left(1,\chi\right) \equiv -\frac{1}{p}\sum_{a=1}^{p-1}\chi\left(a\right)\operatorname{Log}_p\langle a\rangle\left(\mod p\right)$$

מתקיים

$$\begin{aligned}\operatorname{Log}_p\langle a\rangle &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\left(\langle a\rangle-1\right)^n\\ &\equiv \langle a\rangle - 1\left(\mod p^2\right)\end{aligned}$$

כי

$$\left|\frac{(\langle a\rangle-1)^n}{n}\right|_p \quad < \quad p^{-1}$$

ל-$n\geq 2$, אבל האיברים הנ"ל הם ב-$\mathbb{Q}_p$ ולכן $\left|\frac{(\langle a\rangle-1)^n}{n}\right|_p \leq p^{-2}$
לכן

$$\operatorname{Log}_p\langle a\rangle \quad \equiv \quad \langle a\rangle-1 \left(\mod p^2\right)$$

מתקיים

$$a \quad = \quad \omega(a)\langle a\rangle$$

ואז

$$a^{p-1} \quad = \quad \langle a\rangle^{p-1}$$

$$\langle a\rangle \quad = \quad 1+pu$$

כאשר $|u|_p\leq 1$ ולכן

$$\begin{aligned}\langle a\rangle^{p-1} &= (1+pu)^{p-1}\\ &= \sum_{i=0}^{p-1}\binom{p-1}{i}p^iu^i\\ &\equiv 1+(p-1)\,pu \left(\mod p^2\right)\\ &\equiv 1-pu \left(\mod p^2\right)\end{aligned}$$

לכן

$$\begin{aligned}a^{p-1}-1 &\equiv -pu \left(\mod p^2\right)\\ &\equiv 1-\langle a\rangle \left(\mod p^2\right)\end{aligned}$$

לכן

$$\operatorname{Log}_p\langle a\rangle \quad \equiv \quad -\left(a^{p-1}-1\right) \left(\mod p^2\right)$$

ולכן

$$-\frac{1}{p}\operatorname{Log}_p\langle a\rangle \quad \equiv \quad \frac{a^{p-1}-1}{p} \left(\mod p\right)$$

ולכן

$$L_p(1,\chi) \quad \equiv \quad \sum_{a=1}^{p-1}\chi(a)\,\frac{a^{p-1}-1}{p} \left(\mod p\right)$$

נסכם במשפט.
יהי χ כרקטר מודולו $p \neq 2$

$$L_p(1,\chi) \equiv \sum_{a=1}^{p-1} \chi(a) \cdot \frac{a^{p-1}-1}{p} \pmod p$$

מתרגילי פרק א, במקרה

$$(\mathbb{Z}/p\mathbb{Z})^* \rightarrow \{1\}$$

מקבלים

$$\sum_{a=1}^{p-1} \frac{a^{p-1}-1}{p} \equiv \sum_{a=1}^{p-1} \frac{(p-1)!+1}{p} = w_p \pmod p$$

מתרגיל קל (נוסחת היפוך) מקבלים:

$$\frac{a^{p-1}-1}{p} + w_p \equiv -\sum_{\chi \neq 1 \pmod p} \chi^{-1}(a) L_p(1,\chi) \pmod p$$

נציב $a = 1$

$$w_p \equiv -\sum_{\chi \neq 1 \pmod p} L_p(1,\chi) \pmod p$$

לכן

$$\frac{a^p-1}{p} \equiv \sum_{\chi \neq 1 \pmod p} \left(1 - \chi^{-1}(a)\right) L_p(1,\chi) \pmod p$$

לכן $a^{p-1} \equiv 1 \pmod{p^2} \iff$

$$\sum_{\chi \neq 1 \pmod p} L_p(1,\chi) \equiv \sum_{\chi \neq 1 \pmod p} \chi^{-1}(a) L_p(1,\chi) \pmod p$$

.