Eötvös Loránd Tudományegyetem
Természettudományi Kar

Az első Weil-sejtés Dwork-féle bizonyítása

Anderlik Csaba

Témavezető:
Zábrádi Gergely, egyetemi docens

BSc Szakdolgozat
Algebra és Számelmélet Tanszék

Budapest, 2022.

Köszönetnyilvánítás

Óriási köszönettel tartozom Zábrádi Gergelynek a konzultációkon nyújtott összes segítségért, ahol mindenféle kérdésemre válaszolt, és segített a téma megértésében. Továbbá köszönettel tartozom családomnak, barátaimnak, hogy támogattak ebben a nehéz időszakban.

Tartalomjegyzék

1. fejezet

Bevezetés

A Weil-sejtések eredetéig egészen a 18. század végéig, és 19. század elejéig kell visszamenni, amikor két korszakos géniusz Carl Friedrich Gauss és Bernhard Riemann alkottak. Gauss Disquisitiones Arithmeticae könyvének hetedik részében található egy rész, amely talán tekinthető a Weil-sejtések ősének. Riemann híres hipotézise, amelyet a mai napig a matematikus társadalom bizonyítani próbál volt egy apropója annak, hogy Weil kimondta a sejtéseit, mivel Weil-sejtéseinek utolsó két állítása párhuzamba vonható a hipotézissel.

A Weil-sejtések Riemann által definiált zeta-függvény párjáról szólnak függvénytestekre, vagyis a véges testek fölötti varietás zeta-függvényéről szólnak, és állítanak érdekességeket. Mostantól csak zeta-függvényként hívatkozunk rá. Ezen zeta-függvényt úgy kell érteni, hogy véges testek feletti affin vagy projektív hiperfelületek felett vizsgáljuk. Ez által a zeta-függvényt úgy definiáljuk, hogy

$$Z(H_F/\mathbb{F}_q, T) = \exp\left(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}\right),$$

ahol H_F^s-sel azon halmazt adjuk meg, amely $\mathbb{F}_{q^s}$ véges test felett az F algebrai varietás gyökeit tartalmazza, és így N_s azon szám, amely ezen H_F^s halmaz $\mathbb{F}_{q^s}$ véges test feletti elemszámát adja meg. A következő tételben kimondom a Weil-sejtéseket, amelyek már azóta bizonyítást is nyertek így a tétel megnevezés helytálló.

1.0.1. Tétel (Weil-sejtések)**.** *Legyen F egy n dimenziós $\mathbb{F}_q$ test feletti sima projektív varietás, akkor a következő 3 állítás teljesül, hogy*

1. *(Racionalitás) A $Z(H_F/\mathbb{F}_q, T)$ függvény előáll, mint két racionális együtthatós polinom hányadosa, tehát*

$$Z(H_F/\mathbb{F}_q, T) = \frac{P(T)^{\pm 1}}{\prod_{i=0}^{n-1}(1 - q^i T)},$$

   ahol $P(T)$ egy 1 konstans tagú egész együtthatós polinom, melynek foka β, ahol β a hiperfelület egy bizonyos topológiai tulajdonságával kapcsolatos. Ezen β számot szokás Betti számnak is hívni, továbbá a $P(T)$ polinom hatványkitevőjében lévő ± 1 a dimenzió paritására szerint változik, tehát ha páros, akkor $P(T)$, különben meg $\frac{1}{P(T)}$.

2. *(Függvényegyenlet) Ha α egy reciprok gyöke $P(T)$-nek, akkor a következő egyenlet teljesül, hogy*

$$Z(H_F/\mathbb{F}_q, n - T) = q^{\alpha \cdot (\frac{n}{2} - s)} \cdot Z(H_F/\mathbb{F}_q, T).$$

3. *("Riemann hipotézis") $P(T)$ polinom reciprok gyökeinek komplex abszolútértéke $q^{\frac{n-1}{2}}$.*

A Weil-sejtések teljes bizonyítását Paul Deligne adta 1974-ben, amely étale kohomológiát használ. A teljes bizonyításon kívül még Grothendieck nevét érdemes megemlíteni, aki az első két állítást tudta

bizonyítani, sőt mi több ő tudta először bármelyik Weil-sejtést is kohomológiával bizonyítani, amely irányt már Weil is érezte a sejtések kimondásakor. Azonban Weil első sejtésének született egy olyan bizonyítása, amely megdöbbentette a matematikus társadalmat, mivel nem kohomológiával született a bizonyítása. Ezen bizonyítás Bernard Dwork nevéhez fűződik, aki 1960-ban p-adikus analízist használva sikerült bizonyítania Weil első sejtését. Ez mint Katz and Tate ((1998)) Bernard Dwork-ra megemlékező cikkben is olvasható, hogy akkoriban a matematikus társadalmat meglepte a bizonyítás, mivel egyrészt, ahogy előbb írtam nem kohomológiát használt, továbbá mivel Dwork villamosmérnökből lett matematikus volt, aki először villamosmérnöki dipolmát szerzett, majd csak a katonai szolgálat után szerzett először esti egyetemen hallgatott kurzusokat, majd a Columbia egyetem nappali tagozatán szerzett matematikus Ph.D-t.

A szakdolgozatom témája, mint ahogy a címben is olvasható az első Weil-sejtés Dwork-féle bizonyítása lesz ehhez Koblitz ((2012)) könyvét vesszük alapul, tehát ez azt jelenti, hogy a szakdologzatom felépítése ezen könyvet követi. Továbbá a p-adikus számokhoz, amely az első fejezet a szakdolgozatomban, Gouvea ((2003)) könyvét vettem segítségül. Az Ω megalkotásához szükséges algebrai alapokhoz Herstein ((2006)) könyvét, és az algebrai számelmélet részhez meg Serre ((1995)) könyvét, és a témávezetőm Zábrádi Gergely online elérhető jegyzetét (Zábrádi ((2020))) használtam. Dwork konkrét bizonyításához meg Koblitz ((2012)) könyvén kívül Mustata ((2011)) online elérhető jegyzetét, és Ireland and Rosen ((2013)) könyvét vettem segítségül, ahol Ireland tanítványa volt Dworknak.

2. fejezet

A $\mathbb{Q}_p$ megalkotása és a $\mathbb{Z}_p[X]$ polinomok

2.1. Normák a $\mathbb{Q}$-n és Ostrowski tétele

Az alfejezet során bevezetem a norma és metrika definicióit, amely segítségével bizonyítok pár állítást, hogy végül belássuk, hogy a racionális számok halmazán minden nem-triviális norma a szokásos abszolútérték, és a következőkben bevezetésre váró p-adikus normával ekvivalens.

2.1.1. Definíció. Legyen H egy nem üres halmaz. $d : H \times H \to \mathbb{R}_{\geq 0}$ függvényt metrikának vagy távolságnak nevezzük, ha teljesíti a következő felfételeket:

1. $d(x, y) = 0 \iff x = y \ \forall x, y \in H$
2. $d(x, y) = d(y, x) \ \forall x, y \in H$
3. $d(x, y) \leq d(x, z) + d(y, z) \ \forall x, y, z \in H.$

A (H, d) pár továbbá metrikus térnek nevezzük.

A H halmaz sokféle halmaz lehet mint például tetszőleges test $\mathbb{F}$ mint a valós számok ($\mathbb{R}$), racionális számok ($\mathbb{Q}$). A távolságot is megadhatjuk különbözőképpen, mint például diszkét metrika, vagy az euklidészi metrika.

2.1.2. Definíció. Legyen $\mathbb{F}$ tetszőleges test. $\|\cdot\| : \mathbb{F} \to \mathbb{R}_{\geq 0}$ leképezést normának nevezzük, ha teljesíti a következő feltételeket:

1. $\|x\| = 0 \iff x = 0$
2. $\|x \cdot y\| = \|x\| \cdot \|y\| \ \forall x, y \in \mathbb{F}$
3. $\|x + y\| \leq \|x\| + \|y\| \ \forall x, y \in \mathbb{F}.$

A metrikát szoktuk normából származtatottnak is nevezni, mivel definiálhatjuk a távolságot úgy, mint $d(x, y) = \|x - y\|$.

Ezen rövid két fontos definíció után térjünk át a számunkra fontos esetre.

2.1.3. Definíció. Legyen p egy tetszőleges prímszám. Minden nem negatív egész számra definiáljuk a következő függvényt, hogy $\mathrm{ord}_p : \mathbb{Z}_{>0} \to \mathbb{Z}$, ami minden $x \in \mathbb{Z}$ hozzárendeli azt a legnagyobb hatványát p-nek, ami osztja az x számot, tehát legyen m azon legnagyobb eg, amire igaz, hogy $x \equiv 0 \ (p^m)$. Ezen függvényt nevezzük az x p-adikus értékelésének.

Ezen függvény additív tulajdonságokkal rendelkezik, mivel $x, y \in \mathbb{Z}_{>0}$, akkor $\mathrm{ord}_p(x \cdot y) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$. Az x és az y szorzata után most az összegüknek szeretném megmutatni azon tulajdonságát, hogy $\mathrm{ord}_p(x+y) \geq \min(\mathrm{ord}_p(x), \mathrm{ord}_p(y))$, mivel $x+y$-ból kiemelhető p^m, ahol m a maximális hatvány, amelyre p^m osztja x-et, és y-t is, tehát ezen m egyenlő vagy $\mathrm{ord}_p(x)$-szel, vagy $\mathrm{ord}_p(y)$-nal. Továbbá ezt a függvényt kiterjeszthetjük a racionális számokra is, mivel ha $x = \frac{a}{b}$ alakban írható, akkor az x p-adikus értékelése egyenlő lesz, mint $\mathrm{ord}_p(x) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$ az additív tulajdonság miatt.

2.1.4. Állítás. *Definiáljuk a $|\cdot|_p$ leképezést a racionális számokon úgy, hogy*

$$|x|_p = \begin{cases} \frac{1}{p^{\mathrm{ord}_p(x)}}, & ha \quad x \neq 0; \\ 0, & ha \quad x = 0. \end{cases}$$

Akkor a definiált leképezés norma a racionális számokon.

Bizonyítás. A három feltételt kell ellenőrizni. A norma első feltétele nyilvánvalóan látszik a leképezés definiálásából. A második feltétel teljesül, mivel $p^{\mathrm{ord}_p(x\cdot y)} = p^{\mathrm{ord}_p(x)+\mathrm{ord}_p(y)} = p^{\mathrm{ord}_p(x)} \cdot p^{\mathrm{ord}_p(y)}$, tehát $|x\cdot y|_p = \frac{1}{p^{\mathrm{ord}_p(x\cdot y)}} = \frac{1}{p^{\mathrm{ord}_p(x)}} \cdot \frac{1}{p^{\mathrm{ord}_p(y)}} = |x|_p \cdot |y|_p$, $\forall x, y \in \mathbb{Q}$. A harmadik feltétel nyilvánvaló ha $x = 0$ vagy $y = 0$ vagy $x + y = 0$, tehát feltehetjük, hogy egyik se nulla. Legyen $x = \frac{a}{b}$ és $y = \frac{c}{d}$, ahol $a, b, c, d \in \mathbb{Z}$, és $b, d \neq 0$, akkor

$$\begin{aligned} \mathrm{ord}_p(x+y) &= \mathrm{ord}_p\left(\frac{ad+bc}{bd}\right) = \\ &= \mathrm{ord}_p(ad+cb) - \mathrm{ord}_p(b) - \mathrm{ord}_p(d) \geq \\ &\geq \min(\mathrm{ord}_p(ad), \mathrm{ord}_p(cb)) - \mathrm{ord}_p(b) - \mathrm{ord}_p(d) = \\ &= \min(\mathrm{ord}_p(a) + \mathrm{ord}_p(d), \mathrm{ord}_p(c) + \mathrm{ord}_p(b)) - \mathrm{ord}_p(b) - \mathrm{ord}_p(d) = \\ &= \min(\mathrm{ord}_p(a) - \mathrm{ord}_p(b), \mathrm{ord}_p(c) - \mathrm{ord}_p(d)) = \\ &= \min(\mathrm{ord}_p(x), \mathrm{ord}_p(y)). \end{aligned}$$

Így

$$\begin{aligned} |x+y|_p = \frac{1}{p^{\mathrm{ord}_p\left(\frac{ad+bc}{bd}\right)}} &\leq \max(p^{-\mathrm{ord}_p(x)}, p^{-\mathrm{ord}_p(y)}) = \\ &= \max(|x|_p, |y|_p) \leq |x|_p + |y|_p. \end{aligned}$$

Tehát teljesül a három feltétel, így $|\cdot|_p$ norma $\mathbb{Q}$-n. □

2.1.5. Definíció. Egy normát nem-Arkhimédészi normának nevezünk, ha

$$\|x+y\| \leq max(\|x\|, \|y\|) \ \forall x, y \in \mathbb{F}.$$

Továbbá egy normát Arkimédészi normának nevezünk, ha csak a háromszög-egyenlőtlenséget teljesíti, tehát a maximumos egyenlőtlenséget nem.

Így definiálhatunk Arkhimédészi és nem-Arkimédészi metrikát is az által, hogy $d(x, y) = \|x - y\|$ $\forall x, y \in \mathbb{F}$. Ha a $\|\cdot\|$ norma nem-Arkhimédészi, akkor az általa indukált metrikát nem-Arkhimédészi metrikának nevezzük.

A $\|\cdot\|_p$ definíciója miatt a $\mathbb{Q}$-n ezen norma nem-Arkhimédészi és a szokásos abszolútérték Arkimédészi normát definiál.

Az nem-Arkhimédészi normából indukált metrika esetén a metrika harmadik feltételét egyenlő szárú háromszög-egyenlőtlenségnek mondjuk, mivel legyen $x, y \in \mathbb{F}$, akkor $\|x - y\| \leq \max(\|x\|, \|y\|)$, tehát ha $\|x\| < \|y\|$, akkor $\|x - y\| \leq \|y\|$, továbbá $\|y\| = \|x - (x - y)\| \leq \max(x, x - y)$, mivel $\|x\| < \|y\|$, így $\|y\| = \|x - y\|$. Tehát tetszőleges háromszög egyenlő szárú.

2.1.6. Állítás. *Minden nem-Arkhimédészi norma esetén $\|x\| \leq 1$ $\forall x \in \mathbb{F}$.*

Bizonyítás. Legyen x tetszőleges, akkor $\|x\| = \|1 + x - 1\| \leq \max(1, \|n - 1\|) \leq \max(1, \|1 + n - 2\|) \leq \max(1, \|n - 2\|) = \cdots \leq \max(1, 1) = 1$. □

2.1.7. Lemma. *Legyen $\mathbb{F}$ tetszőleges test egy normával ellátva, akkor a következő két állítás ekvivalens:*

1. $\lim_{n\to+\infty} x_n = a$;
2. *Tetszőleges nyílt gömb, amely tartalmazza az a-t, akkor a nyílt halmaz komplementere csak véges sok tagját tartalmazza az x_n sorozatnak.*

Ezen ekvivalencia által nyert definíció ad egy módot arra, hogy hogyan ellenőrizhető két norma ekvivalenciája.

2.1.8. Definíció. Legyen $\|\cdot\|$ norma egy tetszőleges $\mathbb{F}$ felett, és legyen $r \in \mathbb{R}_{>0}$ és $a \in \mathbb{F}$, akkor $B(a,r)$ halmazt nyílt gömbnek nevezzük, ahol

$$B(a,r) = \{x \in \mathbb{F} : \|x-a\| < r\}.$$

A $\overline{B(a,r)}$ halmazt zárt gömbnek nevezzük, ahol

$$\overline{B(a,r)} = \{x \in \mathbb{F} : \|x-a\| \leq r\}.$$

2.1.9. Állítás. *Legyen $\|\cdot\|$ nem-Arkhimédészi norma egy tetszőleges $\mathbb{F}$ felett, továbbá legyen b tetszőleges eleme a $B(a,r)$, akkor $B(b,r) = B(a,r)$.*

Bizonyítás. Ha $x \in B(a,r) \Rightarrow \|x-a\| < r$, ebből következik, hogy $\|x-b\| = \|x-a+a-b\| \leq \max(\|x-a\|, \|a-b\|) < r$, tehát $x \in B(b,r)$. Ez fordítva is ugyanígy működik. □

2.1.10. Állítás. *Legyen $\mathbb{F}$ tetszőleges test és rajta legyen $\|\cdot\|_1$ és $\|\cdot\|_2$ két norma, akkor a következő állítások ekvivalensek:*

1. *$\|\cdot\|_1$ és $\|\cdot\|_2$ normák ekvivalensek.*
2. *Tetszőleges $\{x_n\}_{n=1}^{\infty} \in \mathbb{F}$ sorozat esetén ha $x_n \to a$ az $\|\cdot\|_1$ norma szerint akkor, és csak akkor ha $x_n \to a$ az $\|\cdot\|_2$ norma szerint is.*
3. *Tetszőleges $x \in \mathbb{F}$ esetén ha $\|x\|_1 < 1$ akkor, és csak akkor ha $\|x\|_2 < 1$.*
4. *Létezik egy pozitív valós szám (α) minden $x \in \mathbb{F}$-re, hogy $\|x\|_1 = \|x\|_2^{\alpha}$.*

A bizonyítást a Gouvea ((2003)) könyv 3.1.3. állítás bizonyításának segítségével végezzük.

Bizonyítás. Körbe fogunk bizonyítani.
1. $\Rightarrow$ 2. :

Ha a két norma ekvivalens, akkor a 2.1.7 lemmából következik a 2.-es.
2. $\Rightarrow$ 3. :

Ha $\|x\| < 1$ tetszőleges normára, akkor $\lim_{n\to+\infty} x^n = 0$, így ha 2. állítás teljesül $a = 0$ esetén, akkor ebből következik a 3.-as.
3. $\Rightarrow$ 4. :

Tegyük fel, hogy 3.-as teljesül. Vegyünk egy tetszőleges $x_0 \in \mathbb{F}$-t, amire teljesül $\|x_0\|_1 < 1$, akkor a 3.-as miatt igaz, hogy $\|x_0\|_2 < 1$. Erre az x_0-ra tudunk olyan α valós számot találni, ami teljesíti a 4.-es egyenlőtlenséget, mivel $\alpha = \dfrac{\log(\|x_0\|_1)}{\log(\|x_0\|_2)}$ megfelelő lesz. Így azt kell ellenőrizni, hogy $\forall x \in \mathbb{F}$ esetén, ahol $\|x\|_1 < 1$, ezen α megegyezik. Három különböző esetre fogjuk bontani a bizonyítást.

Először vizsgáljuk azon $x \in \mathbb{F}$, melyekre $\|x\|_1 = \|x_0\|_1$, akkor $\|x\|_2 = \|x_0\|_2$ is teljesülni kell, mivel különben $\frac{x_0}{x}$ vagy $\frac{x}{x_0}$ a $\|\cdot\|_2$ szerinti értéke kisebb mint 1, de ez ellentmond a 3.-as feltevésnek. Így $\|x\|_1 = \|x\|_2^{\alpha}$, mivel $\|x\|_1 = \|x_0\|_1 = \|x_0\|_2^{\alpha} = \|x\|_2^{\alpha}$.

Második esetben vegyük azon $x \in \mathbb{F}$-eket, melyekre igaz, hogy $\|x\|_1 = 1$, mert akkor a 3.-as miatt $\|x\|_2 = 1$ is teljesül, tehát igaz lesz, hogy $\|x\|_1 = \|x\|_2^{\alpha}$. Továbbá ha létezik olyan $x \in \mathbb{F}$, melyre teljesül az egyenlőseg, akkor bármely egész n kitevőjére is teljesülni fog.

A harmadik esetben, tehát azon x-ekre szeretnénk belátni az állítást, melyek az első két esetben nincsenek benne. Legyen minden $x \in \mathbb{F}$ esetén

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

így a harmadik esetben azt kell belátni, hogy ezen $\beta_x = \alpha$-val. Legyen x tetszőleges, akkor feltehetjük, hogy $\|x\|_1 < 1$, mivel különben vehetjük a reciprokát. Mivel $\|x\|_1 < 1$, így $\|x\|_2 < 1$. Legyen $n, m \in \mathbb{Z}$, hogy

$$\|x\|_1^n < \|x_0\|_1^m \iff \left\|\frac{x^n}{x_0^m}\right\|_1 < 1 \iff \left\|\frac{x^n}{x_0^m}\right\|_2 < 1 \iff \|x\|_2^n < \|x_0\|_2^m$$

Mindkét oldal logaritmusát véve az ekvivalencia, úgy módosul, hogy

$$n\log(\|x\|_1) < m\log(\|x_0\|_1) \iff n\log(\|x\|_2) < m\log(\|x_0\|_2).$$

Ebből következik, hogy

$$\frac{n}{m} < \frac{\log(\|x_0\|_1)}{\log(\|x\|_1)} \iff \frac{n}{m} < \frac{\log(\|x_0\|_2)}{\log(\|x\|_2)}. \tag{2.1}$$

Ezen ekvivalencia akkor, és csak akkor teljesül, ha

$$\frac{\log(\|x_0\|_1)}{\log(\|x\|_1)} = \frac{\log(\|x_0\|_2)}{\log(\|x\|_2)},$$

mivel a 2.1 ekvivalencia miatt azon $\frac{n}{m}$ racionális számok halmaza, melyek kisebb az egyiknél, és azon racionális számok halmaza, amelyek kisebbek a másiknál egyenlő számosságú, és ugyanazon elemeket tartalmazzák, mivel különben lennének olyan törtek, melyek az egyiknél nagyobbak lennének a másiknál, pedig kisebbek.

Tehát ebből következik, hogy $\alpha = \beta$, mivel

$$\frac{\log(\|x_0\|_1)}{\log(\|x\|_1)} = \frac{\log(\|x_0\|_2)}{\log(\|x\|_2)} \iff \frac{\log(\|x_0\|_1)}{\log(\|x_0\|_2)} = \frac{\log(\|x\|_1)}{\log(\|x\|_2)}.$$

4. $\Rightarrow$ 1. :

Ha teljesül a 4. állítás, akkor a következő egyenlőtlenségek ekvivalenciája miatt az egyik norma szerinti nyílt gömb a másik norma szerint is nyílt gömb lesz csak más sugárral, mert

$$\|x-a\|_1 < r \iff \|x-a\|_2^{\alpha} < r \iff \|x-a\|_2 < \sqrt[\alpha]{r}.$$

Ez bizonyítja, hogy a normák által definiált topológikus terek egyenlőek, tehát a két norma ekvivalens. □

2.1.11. Következmény. *Legyen $\rho \in (0,1)$, és p egy adott prímszám, akkor $\|x\|_\rho := \rho^{\mathrm{ord}_p(x)}\ \forall x \in \mathbb{Q}$, akkor által definiált norma ekvivalens $|\cdot|_p$ normával.*

Ezen $\|\cdot\|_\rho$ norma helyett a következő állítás miatt szeretjük inkább használni a $|\cdot|_p$-t.

2.1.12. Állítás. *Legyen $x \in \mathbb{Q}_{>0}$, akkor*

$$\prod_{p\in\{2,3,5,\dots\}\cup\{\infty\}} |x|_p = 1,$$

ahol $|x|_\infty$ a szokásos abszolútérték.

Bizonyítás. Legyen $x = \prod_{i=1}^n p_i^{\alpha_i}$ $n \in \mathbb{N}$, akkor q prímszám esetén, ha $q \neq p_i$, $\forall i \in \{1,2,3,\dots,n\}$, akkor $|x|_q = 1$, ha $q = p_i$, ahol $i \in \{1,2,3,\dots,n\}$, akkor $|x|_q = \frac{1}{q^{\mathrm{ord}_q(x)}}$, és ha $q = \infty$, akkor $|x|_q = |\prod_{i=1}^n p_i^{\alpha_i}|$. Így ezekből látszik, hogy a szorzat egyenlő 1-gyel. □

2.1.13. Definíció. A $\|\cdot\|$ normát triviális normának mondjuk, ha minden nem nulla elem esetén a norma értéke 1, különben 0.

2.1.14. Tétel (Ostrowski)**.** *Minden nem triviális norma $\|\cdot\|$ a $\mathbb{Q}$-n ekvivalens a $|\cdot|_p$, ahol p prím vagy $p = \infty$.*

Bizonyítás. Két esetre fogjuk bontani a bizonyítást.

Első eset ha létezik $n \in \mathbb{N}$, melyre $\|n\| > 1$, akkor létezik minimális n_0 is, melyre igaz, hogy $\|n_0\| > 1$. Az n_0-hoz létezik egy olyan α, hogy $\|n_0\| = n_0^\alpha$, mivel, hogyha $\alpha = \dfrac{\log(\|n_0\|)}{\log(n_0)}$, akkor

$$\|n_0\| = \left(\|n_0\|^{\frac{1}{\log(n_0)}}\right)^{\log(n_0)} = (e^\alpha)^{\log(n_0)} = n_0^\alpha.$$

Az n_0 segítségével minden természetes szám felírható n_0 számrendszerben, tehát $n = a_0 + a_1 n_0 + \cdots + a_i n_0^i$, ahol $\forall i\ 0 \leq a_i < n_0$ és $a_i \neq 0$. A háromszög-egyenlőtlenséget felhasználva, akkor adódik, hogy

$$\|n\| \leq \|a_0\| + \|a_1 n_0\| + \cdots + \|a_i n_0^i\| = \|a_0\| + \|a_1\| \cdot n_0^\alpha + \cdots + \|a_i\| \cdot n_0^{i\alpha}.$$

Mivel minden $a_i < n_0$, így minden $\|a_i\| \leq 1$, akkor adódik, hogy

$$\|n\| \leq 1 + n_0 + \cdots + n_0^{i\alpha} = n_0^{i\alpha} \cdot (1 + n_0^{-\alpha} + \cdots + n_0^{-i\alpha}) \leq n^\alpha \cdot \left(\sum_{j=0}^{\infty} \frac{1}{n_0^{j\alpha}} \right) = \frac{n^\alpha}{1 - n_0^{-\alpha}},$$

mivel $n \leq n_0^i$. Ha n helyett n^N teszünk, ahol $N \in \mathbb{N}$, akkor adódik, hogy $\|n^N\| \leq \frac{n^{N\alpha}}{1-n_0^{-\alpha}}$. N-edik gyököt véve mindkét oldalon kapjuk, hogy

$$\|n\| \leq n^\alpha \cdot \sqrt[N]{\frac{1}{1 - n_0^{-\alpha}}},$$

ha $N \to \infty$, akkor kapjuk, hogy $\|n\| \leq n^\alpha$.

Mivel $n_0^i \leq n < n_0^{i+1}$ adódik az n_0 alapú felírásból, így ha vesszük $\|n_0^{i+1}\| = \|n + n_0^{i+1} - n\| \leq \|n\| + \|n_0^{i+1} - n\|$. Ebből adódik, hogy

$$\begin{aligned}
\|n\| &\geq \|n_0^{i+1}\| - \|n_0^{i+1} - n\| \geq n_0^{(i+1)\cdot\alpha} - (n_0^{i+1} - n)^\alpha \geq \\
&\geq n_0^{(i+1)\cdot\alpha} - (n_0^{i+1} - n_0^i)^\alpha = n_0^{(i+1)\cdot\alpha} \left[1 - \left(1 - \frac{1}{n_0} \right)^\alpha \right] > \\
&> n^\alpha \cdot \left[1 - \left(1 - \frac{1}{n_0} \right)^\alpha \right].
\end{aligned}$$

Így ha megint véve n helyett az n^N és elvégezve a gyökvonást, akkor kapjuk, hogy $\|n\| \geq n^\alpha$. Így az első esetben teljesül az egyenlőség a természetes számokra, de a norma szorzatra vonatkozó tulajdonságából következik, hogy tetszőleges racionális szám esetén $\|x\| = |x|^\alpha$, amely meg a 2.1.10 állítás miatt ekvivalens a $\|\cdot\|_\infty$-vel.

A második esetben, tehát azt vizsgáljuk, amikor nincsen olyan n természetes szám, amire igaz, hogy $\|n\| > 1$, tehát $\|n\| \leq 1$ teljesül $\forall n \in \mathbb{N}$-ra, továbbá létezik olyan n is, melyre teljesül, hogy $\|n\| < 1$, mivel a normánk nem a triviális norma. Vegyünk olyan n_0, amire a normája minimális, akkor n_0 prím szükséges, hogy legyen. Tegyük fel, hogy $n_0 = n_1 \cdot n_2$, akkor $\|n_1\| = \|n_2\| = 1$, mivel n_0 minimális, de ez meg ellentmondás, mivel feltettük, hogy $\|n_0\| < 1$.

Tehát tudjuk, hogy $n_0 = p$, ahol p prím, akkor ebből következik, hogy minden más q prímre, teljesülni-e kell, hogy $\|q\| = 1$.

Tegyük fel, hogy nem teljesül, tehát $\|q\| < 1$, akkor létezik egy olyan $k \in \mathbb{N}$, amire $\|q\|^k < \frac{1}{2}$, és létezik egy olyan $l \in \mathbb{N}$, amire $\|p\|^l < \frac{1}{2}$. Mivel p és q relatív prímek, így felírhatók, úgy, hogy $a \cdot p^l + b \cdot q^k = 1$, ahol $a, b \in \mathbb{Z}$. Így ebből következik, hogy

$$1 = \|1\| = \|a \cdot p^l + b \cdot q^k\| \leq \|a \cdot p^l\| + \|b \cdot q^k\| \leq \|p\|^l + \|q\|^k < \frac{1}{2} + \frac{1}{2} = 1.$$

Ez meg ellentmondás, így $\|q\| = 1$ minden nem p prímre. Így minden $x \in \mathbb{Q}$-ra igaz, ahol $x = q_1^{\beta_1} \cdots q_j^{\beta_j}$, $j \in \mathbb{N}$, hogy $\|x\| = \|q_1^{\beta_1}\| \cdots \|q_j^{\beta_j}\|$. Mivel minden p-n kívüli prím normája 1, így ha q_j-k között nincs a p, akkor $\|x\| = 1$, különben $\|x\| = \|p\|^{ord_p(x)}$, mivel $\|p\| < 1$. A 2.1.10 állítás miatt $|\cdot|_p$ norma ekvivalens a kapott normával . □

2.1.15. Észrevétel. *Az Ostrowski tétel bizonyításában a két eset arra vonatkozott, hogy az abszolútérték Arkhimédészi norma, a $|\cdot|_p$ norma meg nem-Arkhimédészi norma.*

2.2. A p-adikus számok teste a $\mathbb{Q}_p$

Az alfejezet során definiálni fogjuk a Cauchy-sorozatot, amely segítségével megadjuk a $\mathbb{Q}_p$ halmazt, mint Cauchy sorozatok ekvivalenciájának halmazát.

2.2.1. Definíció. Egy sorozatot Cauchy sorozatnak nevezünk egy $\mathbb{Q}$ test felett, ha minden $\epsilon>0$ esetén létezik egy olyan $N > 0$ természetes szám, hogy minden $i, j \geq N$ esetén $|a_i - a_j|_p < \epsilon$.

Az alfejezetben fix p prímszám esetén vizsgálunk minden.

A $\mathbb{Q}$-beli számok Cauchy sorozatának ekvivalenciaosztályai által definiáljuk a $\mathbb{Q}_p$ halmazt. $\mathbb{Q}_p$ halmazának elemei legyenek ezen ekvivalenciaosztályok egy-egy reprezentánsa, ahol a reprezentáns elem a sorozatok határértéke legyen. Ezen határérték, azért létezik, mivel a racionális számok halmaza teljes a $|\cdot|_p$ normára nézve. Ez az egyenlő szárú háromszögegyenlőtlenség miatt teljesül.

2.2.2. Állítás. *A $\mathbb{Q}_p$ halmaz egy test.*

Bizonyítás. A $\mathbb{Q}$ halmaz az összeadásra nézve kommutatív csoportot alkot, mivel a határérték additív, tehát két sorozat összegének határértéke a sorozatok határértékeinek összege, továbbá az additív inverz is ezen tulajdonság miatt nyilvánvalóan látszik. Legyen $\{x_i\}$ és $\{y_i\}$ két tetszőleges Cauchy sorozat, melyek különböző ekvivalenciaosztályból származnak, és ezen sorozatok reprezentánsai x és y legyen.

A következő lépésként be kell látni, hogy a $\mathbb{Q}^\times$ kommutatív csoportot alkot a szorzásra nézve. Akkor $x \cdot y$-hoz tartozó ekvivalencia osztály az $\{x_i\}$ és $\{y_i\}$ sorozatok segítségével definiált $\{x_i y_i\}$ ekvivalenciaosztály. Ez megfelelő lesz, mivel vegyünk $\{x_i\}$ ekvivalenciaosztály egy másik sorozatát, mely legyen $\{x'_i\}$, és vegyünk $\{y_i\}$ ekvivalenciaosztály egy másik sorozatát, mely legyen $\{y'_i\}$, akkor

$$|x'_i y'_i - x_i y_i|_p = |x'_i y'_i - x_i y_i + x'_i y_i - x'_i y_i|_p = |x'_i(y'_i - y_i) + y_i(x'_i - x_i)|_p \leq$$
$$\leq \max(|x'_i|_p |y'_i - y_i|, |y'_i|_p |x'_i - x_i|).$$

Ebből látszik, hogy a maximum első és második tagja is tart nullához, tehát a két sorozat ekvivalens. A multiplikatív inverznél nem annyira könnyű a dolgunk, mint az additívnál, mivel a sorozat 0 elemeit ki kell cserélni a következőképpen, hogyha $x_i = 0$, akkor $x_i = p^i$-nel. Így nem rontjuk el a határértéket és ez által a sorozat minden tagjának tudjuk venni az inverzét, és ez megfelelő lesz, mivel mint a szorzásnál ugyan azt a bizonyítást képesek vagyunk elvégezni.

Végül még a disztributivitást kell még ellenőrzni. Legyen $\{a_i\}$, $\{b_i\}$, $\{c_i\}$ különböző ekvivalenciaosztályok elemei, és továbbá legyen ezen ekvivalencia osztályok reprezentánsai a, b, c. Akkor $a(b + c)$ reprezentánsnak megfelelő ekvivalenciaosztály a következő lesz, hogy $ab + ac$, mivel

$$\{a_i(b_i + c_i)\} = \{a_i b_i + a_i c_i\} = \{a_i b_i\} + \{a_i c_i\}.$$

□

2.2.3. Állítás. *$\mathbb{Q}$ sűrű $\mathbb{Q}_p$-ben.*

A bizonyításhoz Gouvea ((2003)) könyvének 3.2.12. állítás bizonyítását vesszük segítségül.

Bizonyítás. Az állítás bizonyításához arra lesz szükségünk, hogy megmutassuk, hogy tetszőleges $x \in \mathbb{Q}_p$ tetszőleges nagyságú nyílt gömbjében létezik racionális szám. Vegyünk egy fix $\epsilon > 0$-t. Az x legyen a reprezentánsa egy ekvivalenciaosztálynak, akkor ezen ekvivalenciaosztályból válasszunk ki egy tetszőleges $\{x_n\}$ Cauchy-sorozatot. Legyen $\epsilon > \epsilon' > 0$, ekkor tudjuk, hogy létezik egy olyan $N \in \mathbb{N}$, hogy minden $i, j \geq N$ esetén $|x_i - x_j|_p < \epsilon'$. Ekkor legyen $y = x_N$ és legyen az ő konstans sorozata $\{y\}$, amelynek reprezentánsa y'. Ha belátjuk, hogy a $y' \in D(x, \epsilon)$, akkor megvagyunk. Legyen $\{x_n - y\}$ azon Cauchy-sorozat, melynek reprezentánsa legyen $x - y'$, akkor

$$|x - y'|_p = \lim_{n\to\infty} |x_n - y|_p$$

Mivel ha $n \geq N$, akkor $|x_n - y|_p = |x_n - x_N|_p < \epsilon'$, így a határérték legfeljebb ϵ', így teljesül, hogy $y' \in D(x, \epsilon)$. □

2.2.4. Állítás. *Legyen $\{x_n\}$ tetszőleges Cauchy-sorozat és y_n egy tetszőleges sorozat, melyre teljesül, hogy $\lim_{n\to\infty} |x_n - y_n|_p = 0$, akkor y_n Cauchy-sorozat.*

Bizonyítás. Legyen $i, j \geq N$, ahol $N \in \mathbb{N}$ és legyen $\epsilon > 0$, akkor

$$|y_i - y_j|_p = |y_i - x_i + x_i - x_j + x_j - y_j|_p \leq \max(|y_i - x_i|_p, |x_i - x_j|_p, |x_j - y_j|_p) \leq \epsilon.$$

Ebből látszik, hogy az állítás teljesül. □

A következő állítás bizonyításához Gouvea ((2003)) könyvének 3.2-es fejezetét használjuk.

2.2.5. Állítás. *$\mathbb{Q}_p$ teljes a $|\cdot|_p$-re nézve.*

Bizonyítás. Legyen $\{\alpha_i\}_{i=1}^{\infty}$ egy Cauchy-sorozat $\mathbb{Q}_p$-ben. A $\mathbb{Q}$ sűrű $\mathbb{Q}_p$-ben, így minden i-re létezik egy olyan x_i racionális szám, melyhez ha hozzárendelünk az x_i-ből álló konstans sorozatot, melyet jelöljünk $\{x_i'\}_{i=1}^{\infty}$-vel, akkor teljesül, hogy $|\alpha_i - x_i'|_p < \frac{1}{i}$, tehát $\lim_{i\to\infty} |\alpha_i - x_i'|_p = 0$, és a 2.2.4 állítás miatt tudjuk, hogy így $\{x_i'\}_{i=1}^{\infty}$ is Cauchy-sorozat. Továbbá mivel $x_{ii=1}'^{\infty}$ Cauchy-sorozat minden tagja egy konstans sorozat, így $\{x_i\}_{i=1}^{\infty}$ sorozat is Cauchy sorozat lesz. Azt állítom, hogy ezen Cauchy-sorozat ekvivalenciaosztályának reprezentánsa lesz a $\{\alpha_i\}_{i=1}^{\infty}$ Cauchy-sorozat limesze, jelöljük a limeszt α-val. Továbbá ezen $\alpha \in \mathbb{Q}_p$.

Legyen $\epsilon > 0$, mivel $\{x_i\}_{i=1}^{\infty}$ Cauchy-sorozat, így létezik ϵ-hoz olyan $N \in \mathbb{N}$, hogy minden $i, j \geq N$ esetén teljesül, hogy $|x_i - x_j|_p < \frac{\epsilon}{2}$. Továbbá definiáljuk $\{x_i - x_j\}$ ekvivalenciaosztály reprezentánsát, mint $\alpha - x_j'$-t. Ekkor minden $i \geq N$ esetén teljesül, hogy

$$|\alpha - x_j'|_p = \lim_{i\to\infty} |x_i - x_j|_p \leq \frac{\epsilon}{2} < \epsilon$$

Tehát $\{\alpha - x_j'\}_{j=1}^{\infty}$ sorozat 0-hoz konvergál $\mathbb{Q}_p$-ben, így $\{x_j'\}$ konvergál α-hoz $\mathbb{Q}_p$ és továbbá az elején kijött, hogy $|\alpha_i - x_i'|_p$ nullához konvergál. Ekkor a 2.2.4 állítás miatt $\{\alpha_i\}$ konvergál α-hoz, és $\alpha \in \mathbb{Q}_p$, tehát az állítást beláttuk. □

2.2.6. Lemma. *Azon $a \in \mathbb{Q}$-ra, melyre teljesül, hogy $|x|_p \leq 1$, akkor minden $i \in \mathbb{N}$ létezik egy olyan α egész szám, hogy $|\alpha - a|_p \leq p^{-i}$, ahol $\alpha \in \{1, 2, \ldots, p^i - 1\}$.*

Bizonyítás. Legyen $a = \frac{x}{y}$, ahol $\gcd(x, y) = 1$. A $|x|_p \leq 1$ összefüggés miatt, így $|y|_p = 1$, akkor p^i-vel is relatív prímek. Így felírható, hogy $sy + rp^i = 1$ alakban, ahol $s, r \in \mathbb{Z}$. Legyen $\alpha = sx \in \mathbb{Z}$. $sy + rp^i = 1$ alakban írás miatt, p-adikusan egy elég kis értéktől eltekintve az s és y egymás multiplikatív inverzei. Ebből következik, hogy $|\alpha - a|_p \leq p^{-i}$, mivel

$$|\alpha - x|_p = |sx - a|_p = \left|sx - \frac{x}{y}\right|_p = \left|\frac{x}{y}\right|_p |sy - 1|_p \leq |sy - 1|_p \leq p^{-i}.$$

Ez által minden i-re létezik olyan egész szám, mely megfelel a kritériumnak. □

2.2.7. Tétel. *A $\mathbb{Q}_p$ minden olyan a elemére, melyre $|a|_p \leq 1$ feltétel teljesül, akkor pontosan egy olyan eleme létezik az ekvivalenciaosztálynak, mely teljesíti a következőket:*

1. *$a_i \in \{0, 1, \ldots, p^i - 1\}$ $\forall i$-re,*
2. *$a_i \equiv a_{i+1}$ $(mod\ p^i)$ $\forall i$-re.*

Bizonyítás. A bizonyítás két részre bontható egyrészt be kell látni, hogy létezik ilyen elem, továbbá az elem egyediségét is. Először lássuk, be a létezést.

Legyen $\{b_i\}$ az a reprezentánshoz tartozó ekvivalenciaosztály egyik eleme. Legyen $N(j) \in \mathbb{N}$, mely minden $i, k \geq N(j)$ esetén $|b_i - b_k|_p \leq \frac{1}{p^j}$, $\forall j \in \mathbb{N}$. Észrevehető ezen $N(j)$ definíciója által, hogyha $i \geq N(1)$, akkor $|b_i|_p \leq 1$, mivel

$$|b_i|_p = |b_i - b_k + b_k|_p \leq \max(|b_k|_p, |b_i - b_k|_p)$$

minden $k \geq N(1)$ esetén, és mivel $|b_k|_p \to |a|_p \leq 1$ ha $k \to \infty$. A 2.2.6 lemma miatt létezik minden j-re olyan a_j, hogy $0 \leq a_j < p^j$, és továbbá $|a_i - b_{N(j)}|_p \leq p^{-j}$.

Most lássuk be a második feltételt. Legyen $j \in \mathbb{N}$, akkor

$$\begin{aligned}|a_j - a_{j+1}|_p &= |a_j + b_{N(j)} - b_{N(j)} + b_{N(j+1)} - b_{N(j+1)} - a_{j+1}|_p \leq \\ &\leq \max(|a_j - b_{N(j)}|_p, |a_{j+1} - b_{N(j+1)}|_p, |b_{N(j)} - b_{N(j+1)}|_p) \leq \\ &\leq \max(p^{-j}, p^{-(j+1)}, p^{-j}) = p^{-j}.\end{aligned}$$

Ez által beláttuk, hogy $a_i \equiv a_{i+1}\ (mod\ p^i)$. Végül annyi maradt még, hogy belássuk, hogy $\{a_i\}$ tényleg az a ekvivalenciaosztályában lévő elem. Legyen $i \in \mathbb{N}$, akkor

$$\begin{aligned}|a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} + b_{N(j)} - b_j|_p \leq \\ &\leq \max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_{N(j)} - b_j|_p) \leq \\ &\leq \max(p^{-j}, p^{-j}, p^{-j}) = p^{-j}.\end{aligned}$$

Így $\{a_i\}$ tényleg az a ekvivalenciaosztályában lévő elem.

Legyen $\{a'_i\}_{i=1}^{\infty}$ és $\{a_i\}_{i=1}^{\infty}$ az a ekvivalenciaosztályában lévő két különböző Cauchy-sorozat, mely teljesíti a tétel feltételeit. Ha a két Cauchy-sorozat különböző, akkor minden N-re ha $a_N \neq a'_N$, akkor $a_N \not\equiv a'_N\ (p^N)$. Az első feltétel miatt minden $i \geq N$-re teljesül, hogy $a_i \not\equiv a'_i\ (p^N)$, mivel

$$a_i \equiv a_N \not\equiv a'_N \equiv a'_i \quad (p^N).$$

Így következik, hogy $\{a'_i\}_{i=1}^{\infty}$ és $\{a_i\}_{i=1}^{\infty}$ Cauchy-sorozatok nem ekvivalensek, mivel $|a_i - a'_i|_p > p^{-N}$. □

Abban az esetben ha $x \in \mathbb{Q}_p$, de nem teljesül, hogy $|x|_p \leq 1$, akkor definiálhatunk x' p-adikus számot, amelyre már teljesül a feltétel, úgyhogy $x' = x \cdot p^m$, ahol m megfelelően nagy természetes szám, melyre már teljesül, hogy $|x'|_p \leq 1$, ekkor x'-höz hozzátudjuk rendelni az 2.2.7 tételben állított Cauchy-sorozatot, ahol $\{x'_i\}_{i=1}^{\infty}$ legyen az x'-höz tartozó sorozat. Ekkor minden tagját feltudjuk írni úgy, mint

$$x'_i = y_0 + y_1 p + \cdots + y_{i-1} p^{i-1},$$

ahol $y_0, y_1, \ldots, y_{i-1} \in \{0, 1, \dot{;} p-1\}$. Ez alapján minden i-re képesek vagyunk megalkotni ezen összeget, amely az 2 feltétel miatt tudjuk, hogy csak a p^i-es tagban tér el ez előzőtől. Ezek alapján megkaphatjuk a x-hez tartozó Cauchy-sorozatot is úgy, mint

$$x = \frac{y_0}{p^m} + \frac{y_1}{p^{m-1}} + \cdots + \frac{y_{m-1}}{p} + y_m + \ldots.$$

Ezen 2.2.7 tétel segítségével tudunk egy egyértelműbb definíciót adni a $\mathbb{Q}_p$-beli elemekre.

2.2.8. Definíció. Tetszőleges $a \in \mathbb{Q}_p$ szám felírható a következő sor alakban, mint

$$a = \sum_{n=-m}^{\infty} a_n p^n,$$

ahol $m \in \mathbb{Z}$, $a_n \in \{0, 1, \ldots, p-1\}\ \forall n \in \mathbb{N}$.

Továbbá azon $x \in \mathbb{Q}_p$, melyekre teljesül, hogy $|x|_p \leq 1$, azon elemek "hatványsorba" fejtetőek. Ezen résztestet a következőképpen definiáljuk.

2.2.9. Definíció. Azon $x \in \mathbb{Q}_p$, melyekre teljesül, hogy $|x|_p \leq 1$ p-adikus egészeknek nevezzük, továbbá ezen számok halmazát $\mathbb{Z}_p$-vel jelöljük.

2.2.10. Észrevétel. *$\mathbb{Z}_p$ résztest főideálgyűrűt alkot.*

Továbbá tudjuk definiálni azon számok halmazát, melyek $\mathbb{Z}_p$ felett invertálhatóak, tehát nem oszthatók p-vel. Ezen számok halmazát úgy jelöljük, hogy $\mathbb{Z}_p^{\times} = \{x \in \mathbb{Z}_p; |x|_p = 1\}$ és p-adikus egységeknek nevezzük.

A valós számok körben ha megadunk egy sort, és vizsgálni szeretnénk ennek a sornak a konvergenciáját, akkor nem elég csak megnézni, hogy a sor együtthatóiból álló sorozat nullához konvergál-e,

mivel olyan is előfordulhat, hogy ezen sorozat nullához tart, de a sorunk mégis divergens. Erre az egyik leghíresebb példa a

$$\sum_{n=1}^{\infty} \frac{1}{n}.$$

A másik irány az nyilvánvalóan teljesül, hogyha a sorunk konvergens, de az együtthatók sorozata nem nullához tart, akkor alulról lehetne becsülni egy olyan sorral, amikor végtelen sokszor ugyanazt a nem nulla elem a tagja, tehát egy divergens sorral alulról becsülhető, amelyből meg ellentmondásra jutunk. Ezen tulajdonság a p-adikus számok körben megváltozik, melyet a következő állítás is mutat.

2.2.11. Állítás. *Legyen $\{x_n\} \in \mathbb{Q}_p$-beli sorozat, akkor a következő két állítás ekvivalens:*

1. *$\{x_n\}$ sorozat nullához tart,*
2. *$\sum_{i=0}^{\infty} x_n$ sorozat konvergens $\mathbb{Q}_p$-ben.*

Bizonyítás. 2. $\Rightarrow$ 1.

A valós esetben meggondoltak miatt teljesül.

1. $\Rightarrow$ 2.

Egy sor definíció szerint akkor, és csak akkor konvergens ha a részletösszegekből álló sorozat konvergál nullához. Tehát vegyünk tetszőleges $n, m \in \mathbb{N}$ és $n > m$, akkor

$$|S_m - S_n|_p = |x_m + x_{m-1} + \cdots + x_{n+1}|_p \leq \max(|x_m|_p, |x_{m-1}|_p, \ldots, |x_{n+1}|_p),$$

mivel a maximum mindegyik tagja konvergál a feltétel miatt nullához, így a részletösszegek sorozata nullához konvergál, tehát a sor konvergens. □

2.2.12. Állítás. *$\mathbb{Z}_p$ egyetlen prím ideálja $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}$ és $\mathbb{Z}_p$ összes ideálja $p^n\mathbb{Z}_p$ alakú, ahol $n \in \mathbb{N}$.*

Bizonyítás. A $\mathbb{Z}_p$ összes eleme felírható, mint $p^n \cdot u$, ahol u $\mathbb{Z}_p$-beli egységelem, tehát így a $p^n\mathbb{Z}_p$ halmazok ideálok lesznek. Azt kéne még belátni, hogy nincs más. Tegyük fel, hogy létezik más típusú ideál is, akkor ezen ideál valamely $c \in \mathbb{Q}$-re olyan alakú lesz, hogy $c\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < c\}$. Mivel $c \in \mathbb{Q}$ ezért létezik olyan m, melyre teljesül, hogy $\frac{1}{p^m} \leq c$, így azt állítom, hogy $c\mathbb{Z}_p = p^m\mathbb{Z}_p$ teljesül. Ez azért igaz, mivel minden $x \in \mathbb{Z}_p$-nek p-adikus értékelése valamely p hatványnak az inverze.

Az első állításnál, ha belátjuk, hogy $p\mathbb{Z}_p$ maximális ideál, akkor abból következik, hogy $p\mathbb{Z}_p$ prím ideál, mivel $\mathbb{Z}_p/p\mathbb{Z}_p$ test. Ha $\mathbb{Z}_p/p\mathbb{Z}_p$ test, abból adódik, hogy integritási tartomány is, melyből következik, hogy $p\mathbb{Z}_p$ prím ideál. A $p\mathbb{Z}_p$ maximális ideálságának bizonyítását Zábrádi ((2020)) jegyzete alapján fogjuk végezni. Legyen $x = \sum_{n=0}^{\infty} x_n p^n$ és vegyük azt a leképezést, mely egy $\mathbb{Z}_p$-beli számhoz hozzárendeli a $\mod p$ maradékát, akkor a képtér $\mathbb{Z}/p\mathbb{Z}$ lesz, mely másként írható úgy, mint a p elemszámú véges test. Továbbá a leképezés homomorfizmus és a magtere a $p\mathbb{Z}_p$, így $p\mathbb{Z}_p$ maximális ideál. □

2.3. Hatványsorral megadott függvények

A rész során tisztázni fogom a $\mathbb{Q}_p$ együtthatós hatványsorok alaptulajdonságait, melyek a valós és komplex analízisben is fontos szerepet játszanak. Ezek a függvények nem mások, mint a binomiális sor, exponenciális függvény, logaritmus függvény és a trigonometrikus függvények. Ha valós számok felett néztük ezeket a függvényeket, akkor a valós számegyenes egy részintervallumán vannak értelmezve, de mivel a $\mathbb{Q}_p$ egy totálisan nem-összefüggő topológikus tér, így nincsek a valós számoknál megszokott intervallumhoz hasonló halmazok, így ezen függvények a $\mathbb{Q}_p$ gömbjein lesznek értelmezve.

A könnyebbség kedvéért nulla középpontú hatványsorokra mondjuk ki a tételeket, állításokat, de minden megáll különböző középpontban is. A valós és komplex számok körében tudjuk, hogyha a hatványsorok konvergenciájának vizsgálatát a középpont egy bizonyos sugarú környezetében értjük. A $\mathbb{Q}_p$-beli hatványsorokban is ez megegyezik.

2.3.1. Állítás. *Legyen* $f(X) = \sum_{n=0}^{\infty} a_n X^n$, $f(X) = \mathbb{Q}_p[[X]]$ *és legyen* $f(X)$ *konvergenciasugara:*

$$r = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|a_n|_p}},$$

akkor

1. *ha* $r = 0$, *akkor* $f(X)$ *csak a nullában konvergens,*
2. *ha* $r = \infty$, *akkor* $f(X)$ *az egész* $\mathbb{Q}_p$*-n konvergens.*
3. *ha* $0 < r < \infty$ *és* $\lim_{n\to\infty} |a_n|_p r^n = 0$, *akkor* $f(X)$ *konvergens a* $|x|_p \leq r$, *és ha a limesz nem tart nullához, akkor az* $f(x)$ *konvergens a* $|x|_p < r$

Bizonyítás. A bizonyításunkat megkönnyíti a 2.2.11 állítás, mivel így tudjuk, azon $x \in \mathbb{Q}_p$-ek halmaza, melyre $\lim_{n\to\infty} |a_n x^n|_p = 0$ lesz a sorunk konvergens, és ebből következik is mind a három állítás. □

Legyen $f(X) = \sum_{n=0}^{\infty} a_n X^n$ és $g(X) = \sum_{n=0}^{\infty} b_n X^n$ két formális hatványsor, akkor az összegükön vagy a különbségükön a következő hatványsort értjük. Legyen $h_1(X) = f(X) \pm g(X) = \sum_{n=0}^{\infty} (a_n \pm b_n) X^n$. Ha a két hatványsor szorzatát úgy definiáljuk, hogy $h_2(X) = f(X) \cdot g(X) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k \cdot b_{n-k} \right) x^n$. Ha $f(X)$ és $g(X)$ konvergensek, akkor $h_1(X)$ és $h_2(X)$ is konvergens lesz. Továbbá $h_1(X)$ konvergenciasugara az $f(X)$, $g(X)$ konvergenciasugarainak összege, és $h_2(X)$ konvergenciasugara az $f(X)$ és a $g(X)$ konvergenciasugarai közül a kisebbikkel egyenlő. Ezen kijelentések egyértelműek az előző állítás fényében.

A következő vizsgálandó tulajdonság két formális hatványsor kompozíciója, ahol a belső függvény konstans értéke 0. A következő tétel, amely hatványsorok kompozícióról szól, megtalálható Gouvea ((2003)) könyvében (5.4.3-as tétel).

2.3.2. Tétel. *Legyen* $f(X) = \sum_{n=1}^{\infty} a_n X^n$ *és* $g(X) = \sum_{n=1}^{\infty} b_n X^n$ *két formális hatványsor. Továbbá legyen* $h(X) = f(g(X))$ *formális kompozíció, akkor tegyük fel, hogy*

1. $g(X)$ *konvergens,*
2. $f(g(X))$ *is konvergens,*
3. *minden* n*-re* $|b_n x^n|_p \leq |g(x)|_p$,

akkor $h(X)$ *konvergens, és* $f(g(X)) = h(X)$.

Ezen tételt nem fogjuk bizonyítani, de a bizonyítás megtalálható az előbb is említett könyvben.

Ezek után áttérünk a rész címében leírtakra, tehát azon függvényekre, melyeket hatványsorral adtunk meg, mint például az exponenciális, logaritmus, és binomiális sor. Először általánosságban fogunk ilyen függvényekről belátni bizonyos tulajdonságokat.

2.3.3. Állítás. *Legyen* $F(X) = \sum_{n=0}^{\infty} a_n X^n$, *ahol az együtthatók* $\mathbb{Q}_p$*-beliek. Továbbá legyen a konvergenciasugara* r *és* $\lim_{n\to\infty} |a_n|_p x^n = 0$, *akkor* $f : \overline{B(0,r)} \to \mathbb{Q}_p$ *függvény, melyet minden* $x \in \overline{B(0,r)}$ *esetén, úgy definiálunk, hogy* x*-hez hozzárendeljük* $F(x)$ *értéket, és akkor* f *függvény korlátos és egyenletesen folytonos a* $\overline{B(0,r)}$ *halmazon.*

Bizonyítás. Két részre bontjuk a bizonyítást. Először belátjuk, hogy korlátos. Az $\{|a_n|_p x^n\}_{n=0}^{\infty}$ korlátos felülről és alulról is, mivel fix $x \in \overline{B(0,r)}$ esetén teljesül, hogy $\lim_{n\to\infty} |a_n|_p x^n = 0$, és ez által véges értékként tudjuk definiálni a $M_r := max(|a_n|_p r^n)$-t. A következő egyenlőtlenség miatt az f korlátos:

$$|F(x)|_p = \left|\sum_{n=0}^{\infty} a_n x^n\right|_p \leq \max(|a_n x^n|_p) \leq \max(|a_n|_p r^n) = M_r.$$

Az egyenletes folytososságot, úgy fogjuk belátni, hogy az f Lipschitz folytonos, mivel abból következik az egyenletes folytonosság. Így kell találni egy megfelelő Lipschitz konstansot, ezen konstans legyen $M_r \cdot \frac{1}{r}$, mivel

$$|f(x)-f(y)|_p = \left|\sum_{n=0}^{\infty} a_n(x^n - y^n)\right|_p = |x-y|_p \cdot \left|\sum_{n=0}^{\infty} a_n \left(\sum_{k=0}^{n-1}(x^k \cdot y^{n-1-k})\right)\right|_p \leq$$
$$\leq |x-y|_p \max(|a_n|_p |x^k \cdot y^{n-1-k}|_p) \leq |x-y|_p \frac{M_r}{r}.$$

Az utolsó lépés, azért tehető meg, mivel

$$\max(|a_n|_p |x^k \cdot y^{n-1-k}|_p) \leq \max(|a_n|_p r^{n-1})_p = \frac{M_r}{r}.$$

A Lipschitz konstansnak $M_r \cdot \frac{1}{r}$ tényleg megfelelő lesz, így egyenletesen folytonos f. □

2.3.4. Észrevétel. *Az előző állítás miatt a valós esethez hasonlóan teljesül, hogy kompakt halmazon folytonos függvény egyenletesen is folytonos.*

A bizonyításból még az is kiderült, hogy nem használtuk ki, hogy $\overline{B(0,r)}$ kompakt csak azt, hogy teljes nem-Arkhimédészi térben vagyunk, tehát ha olyan teljes nem-Arkhimédészi térben, melyben a zárt gömbök nem kompakt, akkor is teljesül fog az előző állítás.

2.3.5. Tétel. *Legyen $f(X) = \sum_{n=0}^{\infty} a_n X^n$, ahol $f(X) \in \mathbb{Q}_p[[X]]$, és $\alpha \in \mathbb{Q}_p$, $0 < \alpha \leq r$, ahol r a konvergenciasugara. Továbbá legyen $m \geq 0$-ra $b_m = \sum_{m=0}^{n} \binom{n}{m} a_n \alpha^{n-m}$ és legyen ez által $g(X) = \sum_{m=0}^{\infty} b_m (X-\alpha)^m$, akkor*

1. *b_m konvegens sor minden m-re, és jól-definiált,*
2. *$f(X)$ és $g(X)$ konvergenciasugara megegyezik,*
3. *tetszőleges $\beta \in \overline{B(0,r)}$ teljesül, hogy $f(\beta) = g(\beta)$.*

Bizonyítás. Az tétel első állítása könnyen látszódik, mivel

$$\left|\binom{n}{m} a_n \alpha^{n-m}\right|_p \leq |a_n \alpha^{n-m}|_p = |a_n \alpha^n|_p \cdot |\alpha^{-m}| \to 0,$$

mivel $|a_n \alpha^n|_p$ tart 0-hoz és $|\alpha^{-m}|_p$ véges, így ebből következik b_m konvergenciája.

A második és harmadik állítását együtt fogjuk belátni. Legyen $\beta \in \overline{B(0,r)}$, akkor

$$f(\beta) = \sum_{n=0}^{\infty} a_n(\beta - \alpha + \alpha)^n = \sum_{n=0}^{\infty}\sum_{m=0}^{n} a_n \binom{n}{m} \alpha^{n-m}(\beta-\alpha)^m,$$

amely ekvivalens azzal, hogy $f(\beta) = \sum_{m=0}^{\infty}\sum_{n=m}^{\infty} a_n \binom{n}{m} \alpha^{n-m}(\beta-\alpha)^m = g(\beta)$. A konvergenciához meg azt kell belátni, hogy

$$\left|a_n \binom{n}{m} \alpha^{n-m}(\beta-\alpha)^m\right|_p$$

tart nullához. α, β eleme $\overline{B(0,r)}$, így létezik egy r-nél kisebb vagy egyenlő r' is melyre teljesül, hogy $|\alpha|_p \leq r'$ és $|\beta|_p \leq r'$. Ez által

$$\left| a_n \binom{n}{m} \alpha^{n-m}(\beta-\alpha)^m \right|_p \leq |a_n \alpha^{n-m}(\beta-\alpha)^m|_p \leq |a_n|_p (r')^n \to 0,$$

ha n tart végtelenbe. Ha m tart végtelen esetén is 0-hoz fog tartani, mivel $a_n\binom{n}{m}\alpha^{n-m}(\beta-\alpha)^m = 0$, ha $m \geq n$, tehát az előbbi szumma csere tényleg lehetséges. Ez által kijött a 2. és 3. állítás is. □

A hatványsor formában megadott függvényekhez, azért kapcsolódik ez a tétel, mivel komplex számok között a függvényeknek lehet egy olyan tulajdonsága, amit analitikus folytonosságnak nevezünk, és ott gyakori, hogy azzal próbáljuk meg analitikusan folytatni egy függyényt, hogy a konvergenciasugár egy másik pontjában fejtjük hatványsorba. De ez a $\mathbb{Q}_p$-ben megváltozik az előző tétel által, mivel az új pont körül hatványsorba fejtett függvény konvergenciasugar megegyezik és minden pontban ugyanazt az értéket veszi fel ezen gömbön belül.

Ha már a komplex számok körében egy ismert tulajdonságnál tartunk, akkor ki szeretném mondani az ottani unicitás tételéhez hasonló állítást.

2.3.6. Állítás. *Legyen $f(X)$ és $g(X)$ formális hatványsorok és tegyük fel, hogy $x_n \in \mathbb{Q}_p$, ahol x_n nem-stacionáriusan tart 0-hoz, és $f(x_n) = g(x_n)$ minden n-rem, akkor $f(X) = g(X)$.*

2.3.7. Definíció. Az x_n stacionáriusan tart egy x-hez, ha létezik egy olyan $N \in \mathbb{N}$, hogy minden $m \geq N$-ra teljesül, hogy $x_m = x$.

Bizonyítás. Legyen $h(X) = f(X) - g(X) = \sum_{m=1}^{\infty} a_m X^m$, akkor tudjuk, hogy $\{x_n\}_{n=1}^{\infty}$ sorozat mentén $h(x_n) = 0$ minden n-re. Azt kéne belátni, hogy $\{a_m\}_{m=1}^{\infty}$ sorozat 0. Tegyük fel, hogy létezik k, melyre $a_k \neq 0$, akkor

$$h(X) = a_k X^k + a_{k+1}X^{k+1} + \dots.$$

Ez által $h(X) = X^k(a_k + a_{k+1}X + \dots) = X^k h_1(X)$, ahol $h_1(X)$ egy hatványsor, mely x_n mentén nem nulla. Ebből következik, hogy x_n elég nagy n-ek esetén is tudjuk, hogy $h(x_n) = x_n^k h_1(x_n) \neq 0$, de ez meg ellentmondás, mivel $h(x_n) = 0$. □

A következőkben konkrét hatványsorral megadott függvényekről lesz szó, először a logaritmus függvényt vizsgáljuk. A komplex esetből tudjuk, hogy a logaritmus függvény előáll, mint $f(X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n}$ hatványsor. Ezen $f(X)$ konvergenciasugarát vizsgáljuk.

2.3.8. Állítás. *Az $f(X)$ hatványsor konvergens az egységgömbön.*

Bizonyítás. Először vizsgáljuk meg a hatványsor együtthatóinak p-adikus abszolútértékét, amely $p^{\mathrm{ord}_p(n)}$, mivel $|a_n|_p = |\frac{(-1)^{n+1}}{n}|_p = p^{\mathrm{ord}_p(n)}$. A hatványsor konvergenciasugárt meghatározhatjuk a 2.3.1 állítás segítségével, amely által

$$r = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|a_n|_p}}.$$

Ebből következik, hogy a konvergenciasugár 1, mivel

$$\sqrt[n]{p^{\mathrm{ord}_p(n)}} \leq p^{\frac{\log n}{n \log p}} \to 1,$$

ha $n \to \infty$. Továbbá $|x|_p = 1$ esetén a hatványsor divergens, mivel $|\frac{1}{n}|_p$ sorozat nem konvergál nullához. □

Az $f(X)$ által definiált hatványsor, tehát a $B(0,1)$ gömbön konvergens, mivel ezen $f(X)$ hatványsorral szeretnénk megadni a $\mathbb{Q}_p$-n a logaritmust, úgyhogy az 1-ben vegye fel 0 értéket és tartsa a logaritmus azonosságokat.

2.3.9. Definíció. Legyen $U_1 = B(1,1) = \{x \in \mathbb{Z}_p : |x-1|_p < 1\} = 1 + p\mathbb{Z}_p$, akkor legyen p-adikus logaritmusa $x \in U_1$-nek:

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

2.3.10. Állítás. *Legyen $x, y \in 1 + p\mathbb{Z}_p$, akkor $\log_p(xy) = \log_p(x) + \log_p(y)$.*

Bizonyítás. Legyen $x', y' \in p\mathbb{Z}_p$ és $1 + x' = x, 1 + y' = y$, így $(1 + x')(1 + y') = 1 + (x' + y' + x'y')$, ahol $(x' + y' + x'y') \in p\mathbb{Z}_p$. A hatványsorba beírva, így adódik, hogy

$$\log_p((1 + x')(1 + y')) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x' + y' + x'y')^n}{n}.$$

Azonban, mivel a $[-1, 1]$ intervallum mentén teljesül az azonosság, hogy $\log_p(1 + x') + \log_p(1 + y') = \log_p((1 + x')(1 + y'))$, így

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

Ezt másképpen mondva

$$\sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x' + y' + x'y')^n}{n} = \sum_{n,m=0}^{\infty} c_{n,m} x'^n \cdot y'^k,$$

és így ha $[-1, 1]$ intervallumbelből veszünk $\hat{x}, \hat{y}$ számokat teszünk, akkor ezen számok felett teljesül az azonosság, így a hatványsor $c_{n,m}$ együtthatói 0-k lesznek, ha $n \neq m$, ekkor a hatványsorra teljesül, hogy

$$\sum_{n=0}^{\infty} c_n x'^n y'^n = \left(\sum_{n=0}^{\infty} c'_n x'^n \right) + \left(\sum_{n=0}^{\infty} c''_n y'^n \right),$$

ahol $c_n = c'_n + c''_n$. Továbbá, mivel $n = 0$ vagy $m = 0$ esetén teljesül, hogy $c_{n,0} = \frac{(-1)^{n+1}}{n}$ vagy $c_{0,m} = \frac{(-1)^{m+1}}{m}$, így

$$\sum_{n=0}^{\infty} c'_n x'^n = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x'^n}{n} \quad , \quad \sum_{n=0}^{\infty} c''_n y'^n = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{y'^n}{n}.$$

□

Mostantól térjünk át az exponenciális függvény vizsgálatára. Most is a komplex esetből definiált hatványsorból indulunk ki, tehát

$$g(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

2.3.11. Állítás. *Legyen $g(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$ hatványsor akkor, és csak akkor konvergens ha $|x|_p < p^{\frac{-1}{p-1}}$.*

Bizonyítás. Először lássuk be, hogy teljesül azon egyenlőség, hogy

$$\mathrm{ord}_p(n!) = \sum_{k=0}^{\infty} \left[\frac{n}{p^k} \right] = \sum_{k=0}^{\left[\log_p(n)\right]} \left[\frac{n}{p^k} \right],$$

ahol $\log_p$ most a p alapú logaritmus. Ezen összeg azért teljesül, mivel az 1-től n-ig a p-vel osztható számok száma pont $\left[\frac{n}{p}\right]$, p^2 oszthatók száma $\left[\frac{n}{p^2}\right]$, és így tovább. Ez által $n!$ p-adikus értékelése pont ezen összeg lesz. A mértani sor összegképlete miatt az összeg kisebb, mint $\frac{n}{p-1}$, tehát

$$\sum_{k=0}^{\infty}\left[\frac{n}{p^k}\right] < \sum_{k=0}^{\infty}\frac{n}{p^k} = \frac{n}{p-1},$$

így ebből látszódik, hogy $|\frac{1}{n!}|_p < p^{\frac{-n}{p-1}}$. 2.3.1 állítás miatt adódik, hogy akkor, és csak akkor konvergens ha $|x|_p \leq p^{\frac{-1}{p-1}}$. Vegyünk egy $y \in \mathbb{Q}_p$, melyre teljesül, hogy $|y|_p = p^{\frac{-1}{p-1}}$, és vegyük azon n-ket, ahol $n = p^m$. Ebből következik, hogy $\mathrm{ord}_p(p^m!) = \sum\limits_{k=0}^{m} p^k = \frac{p^m-1}{p-1}$, és így $\mathrm{ord}_p\left(\frac{y^{p^m}}{p^m}\right) = \frac{p^m}{p-1} - \frac{p^m-1}{p-1} = \frac{1}{p-1}$, amely nem konvergens, tehát $g(X)$ csak a $B\left(0, p^{\frac{-1}{p-1}}\right)$ konvergens. □

2.3.12. Következmény. *Az* $\mathrm{ord}_p(n!) = \frac{n-S_n}{p-1}$, *ahol* S_n *az* n *számjegyeinek összege.*

Bizonyítás. Azt tudjuk, hogy $\mathrm{ord}_p(n!) = \sum\limits_{k=0}^{\infty}\left[\frac{n}{p^k}\right]$, mivel $n = \sum\limits_{l=0}^{\infty} a_l p^l$, így

$$\mathrm{ord}_p(n!) = \sum_{k=0}^{[log_p(n)]}\left[\frac{n}{p^k}\right] = \sum_{k=0}^{[log_p(n)]}\left[\frac{\sum\limits_{l=0}^{[log_p(n)]} a_l p^l}{p^k}\right] =$$

$$= \sum_{k=0}^{[log_p(n)]}\sum_{l=k}^{[log_p(n)]} a_l p^{l-k} = \sum_{l=0}^{[log_p(n)]}\sum_{k=0}^{[log_p(n)]} a_l p^{l-k}$$

$$= \sum_{l=0}^{[log_p(n)]} a_l \frac{p^l-1}{p-1} = \frac{1}{p-1}\sum_{l=0}^{[log_p(n)]}(a_l p^l - a_l) = \frac{n-S_n}{p-1}.$$

□

Ha $p \neq 2$, akkor az előző állítás mutatja, hogy csak a nyílt egységgömbön konvergens a $g(X)$ hatványsor, mivel $|x|_p < p^{\frac{-1}{p-1}}$ egyenlőtlenség ekvivalens azzal, hogy $|x|_p < 1$. Ez azért ekvivalens, mivel $\frac{-1}{p-1}$ érték -1 és p^{-1} között van, és ezen két érték között nincs más p-adikus érték, így minden $x \in B\left(0, p^{\frac{-1}{p-1}}\right)$ teljesül, hogy $|x|_p \leq p^{-1}$ vagyis $|x|_p < 1$.

2.3.13. Definíció. Legyen $B\left(0, p^{\frac{-1}{p-1}}\right) = \left\{x \in \mathbb{Q}_p : |x|_p < p^{\frac{-1}{p-1}}\right\}$. A p-adikus exponenciális függvényt, úgy definiáljuk, hogy $\exp_p : B\left(0, p^{\frac{-1}{p-1}}\right) \to \mathbb{Q}_p$, ahol tetszőleges $x \in B\left(0, p^{\frac{-1}{p-1}}\right)$-re teljesül, hogy $\exp_p(x) = \sum\limits_{n=0}^{\infty}\frac{x^n}{n!}$.

2.3.14. Állítás. *Ha* $x, y \in B\left(0, p^{\frac{-1}{p-1}}\right)$ *és* $x+y$ *is eleme* $B\left(0, p^{\frac{-1}{p-1}}\right)$*-nek, akkor teljesül, hogy*

$$\exp_p(x+y) = \exp_p(x)\cdot\exp_p(y).$$

Bizonyítás. A p-adikus logaritmus additív tulajdonságát leíró állításnak a bizonyítását fogjuk körülbelül megismételni, mivel

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

$$= \sum_{n=0}^{\infty}\sum_{k=0}^{n}\frac{n!}{n!(n-k)!k!}x^k y^{n-k} = \sum_{k=0}^{\infty}\frac{x^k}{k!}\cdot\sum_{k=0}^{\infty}\frac{y^k}{k!} =$$

$$= \exp_p(x)\cdot\exp_p(y).$$

□

A valós esetben a logaritmus függvény és az exponenciális függvény egymás inverzei, ami meg a p-adikus esetben arra fog módosulni, hogy $B\left(0, p^{\frac{-1}{p-1}}\right)$ gömbön lesznek egymás inverzei, amit a következő állítás fog mutatni.

2.3.15. Állítás. *Legyen $x \in B\left(0, p^{\frac{-1}{p-1}}\right)$, akkor teljesülni fog, hogy*

$$|\exp_p(x) - 1|_p < 1,$$

tehát $\exp_p(x)$ benne van $\log_p$ értelmezési tartományában, és ezen x-re igaz, hogy $\log_p(\exp_p(x)) = x$. Legyen továbbá $x \in B\left(0, p^{\frac{-1}{p-1}}\right)$, akkor

$$|\log_p(1+x)|_p < p^{\frac{-1}{p-1}},$$

tehát $\log_p(1+x)$ eleme $\exp_p$ értelmezési tartományának, és $\exp_p(\log_p(1+x)) = 1+x$.

Bizonyítás. A 2.3.2 tételt fogjuk használni mindkét irány bizonyításához, és mivel a két irány bizonyítása hasonló, így csak az állítás első részét látjuk be. Ha $|x|_p < p^{\frac{-1}{p-1}}$, akkor adódik, hogy

$$\left|\frac{x^n}{n!}\right|_p < \frac{-n}{p-1} \cdot \frac{n}{p-1} = 1.$$

Továbbá következik belőle, hogy $|\exp_p(x)-1|_p < 1$, mivel a hatványsorba behelyettesítve a sor minden tagja kisebb lesz, mint 1. Azonban a 2.3.12 következmény miatt még az is adódik, hogy

$$\left|\frac{x^n}{n!}\right|_p < |x|_p,$$

mivel vegyük $\frac{x^{n-1}}{n!}$-t, akkor

$$\operatorname{ord}_p\left(\frac{x^{n-1}}{n!}\right) > \frac{n-1}{p-1} - \frac{n-S_n}{p-1} = \frac{S_n - 1}{p-1} \geq 0,$$

tehát $\left|\frac{x^{n-1}}{n!}\right|_p < 1 \Rightarrow \left|\frac{x^n}{n!}\right|_p < |x|_p$. Ebből következik, hogy $|\exp_p(x) - 1|_p = |x|_p$ és $|\exp_p(x)|_p > \left|\frac{x^n}{n!}\right|_p$ minden $n \geq 2$-re, tehát beláttuk a 2.3.2 tétel feltételeit, így következik az állítás. □

2.3.16. Észrevétel. *Az előző állításból az is látszódik, hogy $\exp_p$ izomorfizmus a $B\left(0, p^{\frac{-1}{p-1}}\right)$ halmazon.*

Bizonyítás. Az előző bizonyításban kijött, hogy $|\exp_p(x) - 1|_p = |x|_p$, ha $x \in B\left(0, p^{\frac{-1}{p-1}}\right)$, tehát $|\exp_p(x) - \exp_p(0)|_p = |x - 0|_p$. Továbbá $|\exp_p(x)|_p = 1$, ha $x \in B\left(0, p^{\frac{-1}{p-1}}\right)$, mivel

$$\left|\sum_{n=0}^{\infty} \frac{x^n}{n!}\right|_p = \max\left(1, \max_{n=2}^{\infty}\left(p^{\frac{1-S_n}{p-1}}\right)\right) = 1,$$

mert $\frac{1-S_n}{p-1} \geq 1$, ha $n \geq 2$. Így ha vesszük a

$$|\exp_p(x) - \exp_p(y)|_p = |\exp_p(y)|_p \cdot |\exp_p(x-y) - 1|_p = |x-y|_p.$$

□

A következő elemi függvény, melyet hatványsorral tudunk definiálni az a binomiális sor, mely a valós esetben is fontos szerepet játszik, ott tudjuk, hogy a nyílt egységgömbön belül konvergens, és attól függően konvergens a zárt egységgömbön, hogy milyen szám szerint nézzük a binomiális sort. A p-adikus esetben a következő állítás alapján látszani fog, hogy ez egy kicsit megváltozik.

2.3.17. Állítás. *Legyen*

$$(1+X)^{\alpha} = B_{\alpha,p}(X) = \sum_{n=0}^{\infty} \frac{\prod_{k=0}^{n-1}(\alpha - i)}{n!} X^n$$

az α szerinti binomiális sor. Ha $|\alpha|_p > 1$, akkor $B_{\alpha,p}(X)$ konvergens a $B(0, p^{\frac{-1}{p-1}})$ gömbön. Ha $|\alpha|_p \leq 1$, akkor $B_{\alpha,p}(X)$ konvergens a $B(0, \frac{p^{\frac{-1}{p-1}}}{|\alpha|_p})$ gömbön.

Bizonyítás. Ha $|\alpha|_p \leq 1$, akkor

$$\left| \frac{\prod_{k=0}^{n-1}(\alpha - i)}{n!} \cdot x^n \right|_p \leq \left| \frac{x^n}{n!} \right|_p,$$

amiből meg következik, hogy a $B\left(0, p^{\frac{-1}{p-1}}\right)$-n konvergens.

Ha $|\alpha|_p > 1$, akkor minden k-ra $|\alpha - k|_p = |\alpha|_p$, tehát

$$\left| \frac{\prod_{k=0}^{n-1}(\alpha - i)}{n!} \cdot x^n \right|_p = \frac{|(\alpha \cdot x)^n|_p}{|n!|_p}$$

ebből következik, hogy a $B\left(0, \frac{p^{\frac{-1}{p-1}}}{|\alpha|_p}\right)$ gömbön konvergens. □

Az előző állítás miatt és, mivel a $\prod_{k=0}^{n-1}(X-k)$ folytonos függvény, így ha $\alpha \in \mathbb{Z}_p$, akkor $B_{\alpha,p}(X) \in \mathbb{Z}_p[[X]]$. Ez azért teljesül, mivel tudunk olyan $\alpha_0 \in \mathbb{Z}$ számot választani, hogy

$$\left| \binom{\alpha_0}{n} - \frac{\prod_{k=0}^{n-1}(\alpha - k)}{n!} \right|_p < 1,$$

mivel $\prod_{k=0}^{n-1}(X-k)$ folytonos.

Továbbiakban definiálni fogunk két új hatványsorral megadott függvényt ehhez szükségünk lesz a számelméletben gyakran használt Möbius-függvényhez, melyet úgy szoktunk definiálni, hogy

$$\mu(n) = \begin{cases} 0 & \text{,ha } \exists p \text{ prím, hogy } \quad p^2 | n; \\ 1 & \text{,ha } \quad n = 1; \\ -1 & \text{,ha } \nexists p \text{ prím, hogy } \quad p^2 \nmid n. \end{cases}$$

Ezen Möbius-függvényre tudunk egy igazán hasznos állítást, mely teszőleges $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ teljesül, hogy

$$\sum_{d|n} \mu(d) = \sum_{\substack{(\epsilon_1,\ldots,\epsilon_s),\\ \epsilon_i \in \{0,1\}}}^{s} \mu(p_1^{\epsilon_1} \cdots p_s^{\epsilon_s}) = \sum_{i=1}^{s} (-1)^{\sum_i \epsilon_i} = \sum_{i=0}^{s} \binom{s}{i} (-1)^{s-k} = (1-1)^s = 0.$$

A Möbius-függvény segítségével, tehát a következő hatványsort definiáljuk, úgyhogy

$$A(X) = \prod_{n=1}^{\infty} (1 - X^n)^{\frac{-\mu(n)}{n}} = \prod_{n=1}^{\infty} B_{\frac{-\mu(n)}{n},p}(-X^n).$$

2.3.18. Állítás. *$A(X)$ egyenlő formálisan $\exp(X)$, ahol $\exp(X)$ a valós exponenciális függvény.*

Bizonyítás. Gondoljuk $A(X)$, mint egy valós értékű függvényre, majd vegyük a valós logaritmusát $A(X)$-nek, akkor

$$\log\left(\prod_{n=1}^{\infty}(1-X^n)^{\frac{-\mu(n)}{n}}\right) = -\sum_{n=1}^{\infty}\frac{\mu(n)}{n}\log(1-X^n) =$$
$$= -\sum_{n=1}^{\infty}\frac{\mu(n)}{n}\sum_{m=1}^{\infty}(-1)^{m+1}\frac{(1-X^n-1)^m}{m} =$$
$$= \sum_{n=1}^{\infty}\frac{\mu(n)}{n}\sum_{m=1}^{\infty}\frac{X^{nm}}{m} = \sum_{\substack{i=1,\\ i=nm}}^{\infty}\frac{X^i}{i}\sum_{n|i}\mu(n) = X.$$

Így tényleg teljesül az állítás. □

$A(X)$-nek van egy kis gondja, mivel azon hatványsorral megadott függvényeket szeretjük igazán, melyek legalább az egységgömbben konvergensek. A következő gondolatmenetben látni fogjuk, hogyha $n = p$, akkor csak a $B\left(0, p^{\frac{-1}{p-1}}\right)$ gömbön konvergens a binomiális sor, így ezáltal $A(X)$ se lehet ezen kívül konvergens.

A binomiális sor esetén láttuk, hogyha az $|\alpha|_p \leq 1$, akkor $B\left(0, p^{\frac{-1}{p-1}}\right)$ gömbön kovergens a binomiális sor, ha $|\alpha|_p > 1$, akkor $B\left(0, \frac{p^{\frac{-1}{p-1}}}{|\alpha|_p}\right)$ gömbön konvergens. A következő áll így elő, hogy

$$\left|\frac{-\mu(n)}{n}\right|_p = \begin{cases} 0, & \text{ha } \exists p_0 \text{ prím, hogy} \quad p_0^2|n; \\ 1, & \text{ha} \quad n = 1; \\ p^{ord_p(n)}, & \text{ha } \nexists p_0 \text{ prím, hogy} \quad p_0^2 \nmid n. \end{cases}$$

Itt az X változó a binomiális sorban az n. hatványon szerepel, így egy tetszőleges $x \in \mathbb{Q}_p$ esetén, akkor konvergens az n-hez tartozó binomiális sor, ha

$$|x|_p^n < \frac{p^{\frac{-1}{p-1}}}{\left|\frac{-\mu(n)}{n}\right|_p} \iff |x|_p < \sqrt[n]{\frac{p^{\frac{-1}{p-1}}}{\left|\frac{-\mu(n)}{n}\right|_p}},$$

tehát ha $n = p$, akkor az adódik, hogy

$$|x|_p < \sqrt[p]{\frac{p^{\frac{-1}{p-1}}}{\left|\frac{-\mu(p)}{p}\right|_p}} = \sqrt[p]{\frac{p^{\frac{-1}{p-1}}}{p}} = p^{\frac{-1}{p-1}},$$

különben ha $p \nmid n$, akkor $\frac{-\mu(n)}{n} \in \mathbb{Z}_p$, tehát a binomiális sor együtthatói is $\mathbb{Z}_p$-beliek, így $A(X) \in \mathbb{Z}_p[[X]]$.

Az $A(X)$ hatványsornál előbb beláttuk, hogy $p|n$, akkor gond van az egységgömbön való konvergenciával. Ez által definiáljuk egy új hatványsorral megadott függvényt.

2.3.19. Definíció. Artin-Hasse exponenciális függvénynek nevezzük, azon $E_p(X)$-vel jelölt függvényt, melyre teljesül, hogy

$$E_p(X) = \prod_{\substack{n=1,\\ p\nmid n}}^{\infty}(1-X^n)^{\frac{-\mu(n)}{n}}.$$

2.3.20. Állítás. *$E_p(X) \in \mathbb{Z}_p[[X]]$, és formálisan $E_p(X) \in \mathbb{Q}[[X]]$.*

Bizonyítás. Tekintjük az $E_p(X)$-t a valós számok felett, és vegyük valós logaritmusát, akkor

$$\log\left(\prod_{\substack{n=1,\\ p\nmid n}}^{\infty}(1-X^n)^{\frac{-\mu(n)}{n}}\right)=\sum_{\substack{n=1,\\ p\nmid n}}^{\infty}\frac{\mu(n)}{n}\sum_{m=1}^{\infty}\frac{X^{nm}}{m}=$$
$$=\sum_{\substack{i=1,\\ i=nm}}^{\infty}\frac{X^i}{i}\sum_{n|i,p\nmid n}\mu(n)=\sum_{m=0}^{\infty}\frac{X^{p^m}}{p^m},$$

tehát

$$E_p(X)=\exp\left(\sum_{m=0}^{\infty}\frac{X^{p^m}}{p^m}\right)\in\mathbb{Q}[[X]].$$

Az $E_p(X)\in\mathbb{Z}_p[[X]]$, azért adódik, mert tudjuk minden n-re, ahol $p\nmid n$, akkor $B_{\frac{-\mu(n)}{n},p}(-X^n)\in 1+X^n\mathbb{Z}_p[[X]]$, mivel a hatványsor egy adott i-re X^i együtthatóját csak véges sok elem szorzatából kapjuk meg, és továbbá, mivel véges sok $\mathbb{Z}_p$-beli szám szorzata $\mathbb{Z}_p$, így $E_p(X)\in\mathbb{Z}_p[[X]]$. □

2.4. $\mathbb{Z}_p$, $\mathbb{Q}_p$ feletti polinomok tulajdonságai

Az alfejezet során először $\mathbb{Z}_p$, $\mathbb{Q}_p$ feletti polinomok irreducibilitására, reducibilitására mondom ki és bizonyítom be a Schönemann-Eisenstein tételét, mely a racionális számok körében is ismert. Végül kimondom és bizonyítok egy tételt, mely segít $\mathbb{Z}_p$ feletti polinomegyenletek megoldásinak generálására, ez lesz a Hensel lemma, ami szintúgy az valós számok köréből is ismert.

2.4.1. Definíció. Legyen $P(X)=a_0+a_1X+\cdots+a_nX^n$ tetszőleges n-ed fokú polinom, mely együtthatóira teljesül, hogy együttesen relatív prímek, tehát $\gcd(a_0,a_1,\ldots,a_n)$=1, akkor primitív polinomnak nevezzük.

2.4.2. Lemma (p-adikus Gauss lemma)**.** *Legyen $P(X)=a_0+a_1X+\cdots+a_nX^n$ tetszőleges n-ed fokú polinom, ha $P(X)$ polinom felbontható két polinom szorzatára, amelyeknek az együtthatói $\mathbb{Q}_p$-beliek, akkor felbontható két olyan polinom szorzatára is, melyek együtthatói $\mathbb{Z}_p$-beliek.*

A bizonyítást itt nem végezem el, mivel a lemma bizonyítása megegyezik az általános esettel, amikor $\mathbb{Q}_p$ helyett $\mathbb{Q}$-ra nézzük és $\mathbb{Z}_p$ helyett $\mathbb{Z}$-re nézzük. Ezen bizonyítás elérhető Kiss ((2007)) könyvében.

2.4.3. Tétel (p-adikus Schönemann Eisenstein tétel)**.** *Legyen $P(X)=a_0+a_1X+\cdots+a_nX^n$ tetszőleges n-ed fokú polinom, melynek együtthatói $\mathbb{Z}_p$-beliek. Ha teljesül, hogy*

$$a_i\equiv 0\ (\mathrm{mod}\ p)\quad \forall \mathrm{i}\ \in\{0,1,\ldots,n-1\},\quad a_0\not\equiv 0\ (\mathrm{mod}\ p),\quad \text{és } a_n\not\equiv 0\ (\mathrm{mod}\ p),$$

akkor a $P(X)$ polinom irreducibilis $\mathbb{Q}_p$ felett.

A bizonyítás a Herstein ((2006)) könyve alapján fog menni.

Bizonyítás. A bizonyítás indirekt módon fogom végezni, tehát tegyük fel, hogy felbomlik két $\mathbb{Q}_p$-beli együtthatós polinom szorzatára. Mivel $a_n\not\equiv 0\ (\mathrm{mod}\ p)$, ezért az általánosság elvét meg nem sértve feltehetjük, hogy a $P(X)$ polinom primitív. Ekkor tudjuk használni a 2.4.2-os Gauss lemmát, így felbomlik két $\mathbb{Z}_p$ együtthatós polinom szorzatára is, melyek legyenek $R(X)$ és $S(X)$. $R(X)$ legyen r-ad fokú polinom, $S(X)$ meg legyen s-ed fokú polinom, ahol $sr=n$, tehát

$$R(X)=b_0+b_1X+\cdots+b_rX^r,\quad S(X)=c_0+c_1X+\cdots+c_sX^s.$$

A a_0 együtthatója ez alapján előáll, mint b_0c_0, és mivel $a_0\not\equiv 0\ (\mathrm{mod}\ p)$, így b_0 és c_0 közül csak az egyiket oszthatja p, mivel különben p^2-t is osztaná a_0-t. Tegyük fel, hogy b_0 osztható p-vel és c_0 meg nem oszható p-vel. Továbbá azt is észrevehetjük, hogy $R(X)$ polinom összes együtthatóját nem

oszthatja p, mivel $a_n \not\equiv 0 \ (mod\ p)$, tehát feltehető, hogy legyen i azon legkisebb index, melyre már p nem osztja $R(X)$ együtthatóit. De, mivel

$$a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_1 c_{i-1} + b_0 c_i$$

előáll ilyen alakban, és mivel $a_i \equiv 0 \pmod p$, tehát az összeg minden tagja osztható p-vel, ami az első tag kivételével látszik is, mivel b_j-k oszthatók p-vel, ahol $j \in \{0, 1, \ldots, i-1\}$. De sajnos b_i és c_0 se osztható p-vel, így ellentmondásra jutottunk, tehát $P(X)$ irreducibilis. □

A történelem során a matematikusokat nagyon érdekelte a polinomegyenletek megoldhatósága különböző halmazok felett, így tehát az is érdekes, hogy egy polinomegyenletnek $\mathbb{Q}_p$ vagy $\mathbb{Z}_p$ felett van-e megoldása, melyre a következő tétellé vált lemma lesz a segítségünkre, melynek neve Hensel lemma.

2.4.4. Definíció. Legyen $P(X) = a_0 + a_1 X + \cdots + a_n X^n$ tetszőleges n-ed fokú polinom, melynek együtthatói tetszőleges gyűrűbeli elemek, akkor egy polinom formális deriváltján azon polinomot értjük, hogy $P'(X) = a_1 + 2a_2 X + \cdots + n a_{n-1} X^{n-1}$.

2.4.5. Tétel (p-adikus Hensel lemma)**.** *Legyen $P(X) = c_0 + c_1 X + \cdots + c_n X^n$ tetszőleges n-ed fokú polinom, melynek együtthatói p-adikus egészek. Legyen x_0 egy olyan p-adikus egész, melyre teljesül, hogy $P(x_0) \equiv 0 \ (mod\ p)$ és $P'(x_0) \not\equiv 0 \ (mod\ p)$. Akkor létezik olyan x p-adikus egész, melyre teljesül, hogy $P(x) = 0$ és $x \equiv x_0 \ (mod\ p)$.*

Bizonyítás. A tétel bizonyításunk azon fog múlni, hogy találunk-e egy olyan egyértelmű sorozatot, melynek tagjai egész számok, és továbbá teljesül $j \geq 1$ esetén, hogy

1. $P(a_j) \equiv 0 \pmod{p^{j+1}}$;
2. $a_j \equiv a_{j+1} \pmod{p^j}$;
3. $0 \leq a_j < p^{j+1}$.

Ezen sorozat egyértelmű létezését j szerinti indukcióval fogjuk bizonyítani.

Az a_0-ás tagot válassszuk, úgy hogy $a_0 \in \{0, 1, 2, \ldots, p-1\}$ szám legyen, továbbá legyen kongruens x_0 modulo p. Ezen választás miatt és 2, 3 feltételekből következik, hogy a_1 $a_0 + b_1 p$ alakban áll elő, ahol $b_1 \in \{0, 1, 2, \ldots, p-1\}$, ebből követekezően a 2, 3 feltételeket teljesíti is, tehát csak az 1 feltételt kell ellenőrizni.

$$\begin{aligned} P(a_1) = P(a_0 + b_1 p) &= \sum_{i=0}^{n} c_i (a_0 + b_1 p)^i = \\ &= \sum_{i=0}^{n} c_i \cdot \left(\sum_{k=0}^{i} \binom{i}{k} \cdot a_0^k \cdot (b_1 p)^{i-k} \right) \equiv \\ &\equiv \sum_{i=0}^{n} c_i a_0^i + \sum_{i=0}^{n} c_i (a_0^{i-1} b_1 p) \qquad (\text{mod } p^2). \end{aligned}$$

Tehát ha csak a p^2-el nem osztható tagokra vagyunk kíváncsiak, akkor a $P(a_1) = P(a_0) + P'(a_0) b_1 p$.

$$P(a_1) \equiv 0 \pmod{p^2} \qquad \Longleftrightarrow \qquad P(a_0) + P'(a_0) b_1 p \equiv 0 \pmod{p^2},$$

mivel $P(a_0) \equiv mp \ (mod\ p^2)$ a feltételek miatt, ahol $m \in \{0, 1, 2, \ldots, p-1\}$. Továbbá a feltételekből az is adódik, hogy $mp + P'(a_0) b_1 p \equiv 0 \pmod{p^2}$, mely ekvivalens azzal, hogy $m + P'(a_0) b_1 \equiv 0 \pmod p$. Ezen kongruencia b_1-re nézve egyértelműen megoldható, mivel egyrészt $P'(a_0) \not\equiv 0 \pmod p$, továbbá 2.2.6 lemma miatt a b_1-et választhatjuk a $\{0, 1, 2, \ldots, p-1\}$ halmazból, tehát $b_1 \equiv -\frac{m}{P'(a_0)} \pmod p$. A feltételek miatt ezen b_1 egyértelmű.

Az indukciós feltételt használva tegyük fel, hogy $j-1$-ig teljesül. Ekkor a 2, 3 feltételek miatt tudjuk, hogy a_j pont $a_{j-1} + b_j p^j$ alakban áll elő, tehát már csak a harmadik feltételt kell ellenőrizni.

Így adódik, hogy

$$P(a_j) = P(a_{j-1} + b_j p^j) = \sum_{i=0}^{n} c_i (a_{j-1} + b_j p^j)^i =$$
$$= \sum_{i=0}^{n} c_i \cdot \left(\sum_{k=0}^{i} \binom{i}{k} \cdot a_{j-1}^k \cdot (b_j p^j)^{i-k} \right) \equiv$$
$$\equiv \sum_{i=0}^{n} c_i a_{j-1}^i + \sum_{i=0}^{n} c_i (a_{j-1}^{i-1} b_j p^j) \qquad (\text{mod } p^{j+1}).$$

Tehát

$$P(a_j) \equiv P(a_{j-1}) + P'(a_{j-1}) b_j p^j \qquad (\text{mod } p^{j+1}).$$

Azonban $P(a_{j-1}) \equiv 0 \pmod{p^j}$, így ebből adódik, hogy

$$P(a_{j-1}) \equiv m' p^j \qquad (\text{mod } p^{j+1}).$$

Ez által

$$P(a_{j-1}) + P'(a_{j-1}) b_j p^j \qquad (\text{mod } p^{j+1})$$

ekvivalens azzal, hogy $m' + P'(a_{j-1}) b_j \pmod{p}$. A b_1 esethez megegyező módon itt is egyértelműen választható a b_j a $\{0, 1, 2, \ldots, p-1\}$ halmazból, tehát $b_j \equiv -\frac{m'}{P'(a_{j-1})} \ (mod\ p)$. Ebből következik, hogy egyértelműen létezik ilyen sorozat.

Sőt, mi több a sorozatból az állításunk is következik, mivel

$$x = a_0 + b_1 p + b_2 p^2 + b_3 p^3 + \ldots$$

alakban keressük, akkor $P(x) \equiv P(a_j) \equiv 0 \ (mod\ p^{j+1})$, tehát ebből következik, hogy P(x)=0, és mivel $a_0 \equiv x_0 \pmod{p}$, így $x \equiv x_0 \pmod{p}$, és abból következően, hogy a sorozat egyértelmű, így x is egyértelmű. □

A valós számok körében ismert egy módszer, amellyel képesek vagyunk meghatározni egy teszőleges f differenciálható függvény zérushelyét. Ezt a módszert Newton módszernek is nevezzük. A módszer úgy szól, hogy vegyünk egy tetszőleges x_0 számot, és a következő egyenlet szerint generáljuk le a sorozat további tagjait, ahol az egyenlet:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)},$$

akkor a sorozat határértéke megadja a függvény egyik zérushelyét. Ezen módszer megegyezik azzal, amit a Hensel lemma bizonyításában végeztünk, mivel $a_{n+1} = a_n + b_n p$ alakban kerestük. Ha ezen egyenletben a b_n-t kifejezzük a bizonyításban meggondoltakkal, akkor kapjuk, hogy $a_{n+1} = a_n - \frac{P(a_n)}{P'(a_n)}$, mivel $P(a_n) = mp$ és $b_n = -\frac{m}{P'(a_n)}$, akkor

$$b_n = -\frac{\frac{P(a_n)}{p}}{P'(a_n)}.$$

Ezt behelyettesítve az egyenletbe kapjuk a Newton módszerrel megegyező egyenletet.

Ezen módszer a $\mathbb{Z}_p$ körében mindig működik, mivel egyrészt a $\frac{P(a_n)}{P'(a_n)}$ szám mindig $\mathbb{Z}_p$-ben marad sőt, mi több a $P'(a_n)$ soha sem lesz kongruens nullával modulo p.

Ezen felfedezés által érdemes egy másik formában is megfogalmazni a tételt, mely Gouvea ((2003)) könyvében is megfogalmazódott.

2.4.6. Tétel. *Legyen $P(X) = c_0 + c_1 X + \cdots + c_n X^n$ tetszőleges n-ed fokú polinom, melynek együtthatói $\mathbb{Z}_p$-beliek. Tegyük fel, hogy létezik olyan $a_1 \in \mathbb{Z}_p$, melyre $|P(a_1)|_p < 1$ és $|P'(a_1)|_p = 1$. Minden $n \geq 1$-re ha a_{n+1}-et úgy definiáljuk, hogy*

$$a_{n+1} = a_n - \frac{P(a_n)}{P'(a_n)},$$

akkor a megadott sorozat határértéke legyen $a \in \mathbb{Z}_p$, mely egy egyértelmű p-adikus egész, és továbbá teljesül, hogy $|a - a_1|_p < 1$ és $P(a) = 0$.

A Hensel lemmának sok féle felhasználása ismert, abból megpróbálnék ismertetni egyet. Legyen $a \in \mathbb{Z}_p$, $a \neq 0 \pmod{p}$, akkor ha vesszük azt a polinomot, hogy $P(X) = aX - 1$, akkor ezen polinom gyöke pont az a p-adikus egész inverze lesz. A Newton-féle approximációs módszerrel vagy a Hensel lemma bizonyításában leírt módszerrel meghatározható az a inverze. Ha csak közelítve szeretnénk meghatározni az inverzét, akkor használjuk inkább a $F(X) = \frac{1}{X} - a$ függvényt, mivel így az

$$x_{n+1} = x_n - \frac{\frac{1}{x_n} - a}{\frac{-1}{x_n^2}} = x_n + x_n^2 \cdot (\frac{1}{X} - a) = 2x_n - ax_n^2,$$

és nem az lesz belőle, hogy

$$x_{n+1} = x_n - \frac{ax_n - 1}{a} = \frac{1}{a},$$

amely numerikusan kevésbé hasznos.

3. fejezet

Az Ω megalkotása

3.1. A p-adikus norma kiterjesztése

Ezen alfejezet fő állítása az lesz, hogy tetszőleges $\mathbb{Q}_p$ bővítésén van olyan norma, mely a $|\cdot|_p$ norma kiterjesztése és ezen kiterjesztés egyértelmű.

A következő két definícióban tisztázzuk a kompakt és lokálisan kompakt halmaz definícióját.

3.1.1. Definíció. *M metrikus térnak az X halmazát kompaktnak mondjuk, ha minden sorozatnak létezik konvergens részsorozata.*

Ezen definíció ekvivalens azzal, hogy az X halmaz teljes és teljesen korlátos.

3.1.2. Definíció. *M metrikus tér egy X halmazát lokálisan kompaktnak nevezzük, ha a tér minden pontjának létezik kompakt környezete.*

Ezen fejezet során Gouvea ((2003)) könyvét követjük. Gouvea ((2003)) könyvének különösen 6.3-as részét.

3.1.3. Állítás. *A $\mathbb{Z}_p$ kompakt metrikus tér, a $\mathbb{Q}_p$ lokális kompakt metrikus tér.*

A bizonyításban egy kicsit követjük Robert ((2000)) könyvének 1.5-ös alfejezetét.

Bizonyítás. A $\mathbb{Q}_p$ lokális kompaktsága következik a $\mathbb{Z}_p$ kompaktságából, mivel a $\mathbb{Z}_p$ az 0 egy kompakt környezete. A lokális kompaktság, azért ekvivalens azzal, hogy a nulla egy környezete kompakt, mivel veszünk egy tetszőleges $y \in \mathbb{Q}_p$ elemmel való eltolást, akkor megkaphatjuk $y + \mathbb{Z}_p$-t. Az eltolás, mint leképezés folytonos, így $y + \mathbb{Z}_p$ kompakt, mivel kompakt halmaz folytonos képe kompakt. A másik irány egyértelmű.

Az előző fejezet során láttuk, hogy $\mathbb{Q}_p$ a $|\cdot|_p$ normára nézve teljes, és $\mathbb{Z}_p$ zárt részhalmaza $\mathbb{Q}_p$-nek. Így elég csak azt belátni, hogy teljesen korlátos. Legyen $\epsilon > 0$, akkor elég belátni, hogyha $\epsilon = p^{-n}$ esetekre, mivel ha $p^{-k-1} < \epsilon < p^{-k}$, akkor az ϵ sugarú gömb megegyezik p^{-k-1} sugaru gömbbel. Tudjuk, hogy

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

teljesül, és mivel $\mathbb{Z}/p^n\mathbb{Z}$ kompakt, így ha veszünk egy redukált maradékrendszert, mint például a szokásos $\{0, 1, \ldots, p^n - 1\}$ halmazt. Ha tetszőleges $i \in \{0, 1, \ldots, p^n - 1\}$ esetén

$$i + p^n\mathbb{Z}_p = \{i + p^n x : x \in \mathbb{Z}_p\} = \{x \in \mathbb{Z}_p : |i - x|_p \leq p^{-n}\}$$

gömbök megadják $\mathbb{Z}_p$-nek egy ϵ-hálóját, $\mathbb{Z}_p$ teljesen korlátos, és mivel teljes is, így $\mathbb{Z}_p$ kompakt. □

A norma definícióját eddig egy F test felett definiáltuk, most az F test véges bővítésén is definiálni fogjuk.

3.1.4. Definíció. Legyen V véges dimenziós vektortér F felett és legyen $\|\cdot\|$ F feletti norma. A $\|\cdot\|_V$ leképezést a V feletti vektortér normának nevezzük, ha a következő feltételeket teljesíti:

1. $\|x\|_V = 0 \iff x = 0$,
2. $\|ax\|_V = \|a\|\|x\|_V \ \forall x \in V$ és $\forall a \in F$,
3. $\|x + y\|_V \leq \|x\|_V + \|y\|_V \ \forall x, y \in V$.

3.1.5. Definíció. Legyen $\|\cdot\|_1$ és $\|\cdot\|_2$ V feletti normák akkor, és csak akkor ekvivalensek ha létezik olyan c_1 és c_2 pozitív valós számok, melyekre teljesül, hogy $\|x\|_2 \leq c_1\|x\|_1$ és $\|x\|_1 \leq c_2\|x\|_2 \ \forall x \in V$.

3.1.6. Észrevétel. *Az előző definíció ekvivalens alakja úgy szól, hogy $\|\cdot\|_1$ és $\|\cdot\|_2$ V feletti normák akkor, és csak akkor ekvivalens ha $\|\cdot\|_1$ norma szerinti tetszőleges Cauchy-sorozat, Cauchy-sorozat $\|\cdot\|_2$ norma szerint is.*

3.1.7. Állítás. *Ha V véges dimenziós vektortér egy lokálisan kompakt F test felett, akkor minden V felett definiált norma ekvivalens.*

Bizonyítás. Legyen $\{b_1, b_2, \ldots, b_n\}$ bázis a V felett. A $\|\cdot\|_{\sup}$ leképezést nevezzük sup-normának, mely $\forall v = a_1b_1 + a_2b_2 + \cdots + a_nb_n \in V$ esetén

$$\|a_1b_1 + a_2b_2 + \cdots + a_nb_n\|_{\sup} = \max_{i=1}^{n}(\|a_i\|),$$

ahol $\|\cdot\|$ egy tetszőleges F feletti norma.

A sup-norma tényleg norma lesz, mivel a norma első két feltétele egyértelműen adódik. Továbbá a harmadik feltétel is teljesül, mivel $\forall x = a_1b_1 + a_2b_2 + \cdots + a_nb_n, y = c_1b_1 + c_2b_2 + \cdots + c_nb_n \in V$ esetén

$$\begin{aligned}\|(a_1b_1 + a_2b_2 + \cdots + a_nb_n) + (c_1b_1 + c_2b_2 + \cdots + c_nb_n)\|_{\sup} = \\ = \|(a_1 + c_1)b_1 + (a_2 + c_2)b_2) + \cdots + (a_n + c_n)b_n\|_{\sup} = \\ = \max_{i=1}^{n}(\|a_i + c_n\|) \leq \max_{i=1}^{n}(\|a_i\|) + \max_{i=1}^{n}(\|c_i\|) = \\ = \|x\|_{\sup} + \|y\|_{\sup}.\end{aligned}$$

Így sup-norma tényleg norma.

Legyen egy tetszőleges $\|\cdot\|_V$ norma V felett, ha belátjuk, hogy ezen tetszőleges norma ekvivalens a sup-normával, akkor beláttuk az állítás. Legyen $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n \in V$ tetszőleges elem, akkor

$$\begin{aligned}\|x\|_V = \|a_1b_1 + a_2b_2 + \cdots + a_nb_n\|_V \leq \\ \leq \|a_1\| \cdot \|\|b_1\|_V + \cdots + \|a_n\| \cdot \|\|b_n\|_V \leq n \cdot (\max(\|a_i\|)) \max(\|b_i\|_V),\end{aligned}$$

így ha c_1-et úgy választjuk meg, hogy $c_1 = n \cdot (\max(\|b_i\|_V))$, akkor az ekvivalencia definíciójának egyik egyenlőtlenségét beláttuk, már csak egy olyan c_2-t kell találni, mely a fordított egyenlőtlenséget bizonyítja.

Ezen egyenlőtlenség bizonyításához az az ötlet, hogy a sup-norma szerinti egységgömbön lévő elemekre találunk c_2-t, és az egységgömb minden skalárszorosára is teljesülni fog, mivel az elemeket visszaképezzük az egységgömbre, majd a skalárral visszaszorzva kapjuk az egyenlőtlenséget.

Ezen ötletet, akkor most formalizáljuk. Legyen $B(1)_{\sup} = \{x \in V : 0 < \|x\|_{\sup} \leq 1\}$, akkor tetszőleges $x \in B(1)_{\sup}$ teljesül, hogy $\|x\|_V \geq \epsilon$, ahol $\epsilon > 0$, mivel különben a $B(1)_{\sup}$ kompakt halmazban létezne egy olyan $\{x_i\}_{i=1}^{\infty}$ sorozat, mely a V norma szerint tartana nullához. Ez meg azért lehetetlen, mivel $B(1)_{\sup}$ kompakt, így létezik $\{x_{i_j}\}_{j=1}^{\infty}$ egy részsorozat, mely konvergál x-hez, akkor

$$\|x\|_V = \|x - x_{i_j} + x_{i_j}\|_V \leq \|x - x_{i_j}\|_V + \|x_{i_j}\|_V \leq c_1\|x - x_{i_j}\|_{\sup} + \|x_{i_j}\|_V,$$

mivel mindkét tag tart nullához, így $\|x\|_V = 0$, és ez ellentmondás, mivel $x \in B(1)_{\sup}$.

Következő lépésként, akkor vegyünk egy tetszőleges $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n$-et, melynek a sup-normája legyen $\|x\|_{\sup} = \|a_i\| = \max(\|a_i\|)$, akkor $\|\frac{x}{a_i}\|_{\sup} = 1$, így $\|\frac{x}{a_i}\|_V \geq \epsilon \cdot \|\frac{x}{a_i}\|_{\sup}$, amiből meg következik az állítás. □

3.1.8. Következmény. *Legyen $V = K$ test, akkor legfeljebb egy norma létezik K felett, mely az F feletti norma kiterjesztése.*

Legyen $K = F(\alpha)$ F test véges bővítés és legyen $a_0+a_1x+\cdots+x^n$ olyan 1 főegyüttható irreducibilis polinom, melynek együtthatói F-belik és, melynek α gyöke. Ekkor értelmet nyer az α elemmel való szorzás, mint F-lineáris leképezés K-ból K-ba, akkor ezen leképezésnek a mátrixát jelöljük A_α-val.

3.1.9. Definíció. Az $\mathbb{N}_{K/F}(\alpha)$-val jelölt értéket a K vektortérben lévő α-hoz tartozó értékelésnek nevezzük, ha $\mathbb{N}_{K/F}(\alpha) =\det(A_\alpha)$.

3.1.10. Állítás. *Az előző definíciója K vektortérben lévő α-hoz tartozó értékelés ekvivalens a következő két definícióval:*

1. $\mathbb{N}_{K/F}(\alpha) = (-1)^n a_n$,
2. $\mathbb{N}_{K/F}(\alpha) = \prod_{i=1}^{n} \alpha_i$, *ahol az α_i az α konjugáltjai F feletti.*

Bizonyítás. Legyen az α elemhez tartozó 1 főegyüttható irreducibilis polinom: $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, melynek gyökei az α elem konjugáltjai. Ezen állításból következik a 2. és a 3. ekvivalenciája, mivel $(-1)^n \cdot a_0 = \prod_{i=1}^{n} \alpha_i$.

Az 1. és a 2. ekvivalenciája abból következik, hogy vegyük a

$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

bázist, akkor az α elemmel való szorzás mátrixa az lesz, hogy

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & \cdots & -a_2 \\ \vdots & 0 & \ddots & \ddots & & \vdots \\ & \vdots & & \ddots & 0 & -a_{n-2} \\ 0 & 0 & & & 1 & -a_{n-1} \end{pmatrix},$$

melynek determinánsa pont a $(-1)^n a_0$. □

Legyen β egy teszőleges eleme $K = F(\alpha)$-nak, akkor a $\mathbb{N}_{K/F}(\beta)$ értéket kétféleképpen definiálhatjuk:

1. $\mathbb{N}_{K/F}(\beta)$ egyenlő a β elemmel való szorzás mátrixának determinánsával;
2. $\mathbb{N}_{K/F}(\beta) = \mathbb{N}_{F(\beta)/F}(\beta)^{[K:F(\beta)]}$

3.1.11. Állítás. $\mathbb{N}_{K/F}(\beta)$ *két definíciója ekvivalens.*

Bizonyítás. A β elemmel való szorzás mátrix blokk diagonális mátrix lesz, mivel ha választuk egy tetszőleges bázist $F(\beta)$ vektortérben, melyet F felett nézünk, és választunk egy tetszőleges bázist K vektortérben, melyet $F(\beta)$ felett nézünk, akkor a K vektortér bázisát F felett megkaphatjuk ezen bázis elemek szorzataként, tehát β elemmel szorzás K-beli mátrixa megkapható, mint

$$M = \begin{pmatrix} M_\beta & 0 & 0 & \cdots & 0 \\ 0 & M_\beta & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & M_\beta \end{pmatrix},$$

ahol M_β a β elemmel való szorzás mátrixa az $F(\beta)$ felett. Ebből már következik a definíció ekvivalenciája, mivel M mátrix nagysága $[K : F(\beta)] \times [K : F(\beta)]$-s. □

3.1.12. Észrevétel. *Legyen $\alpha, \beta \in K$, akkor $\mathbb{N}_{K/F}(\alpha \cdot \beta) = \mathbb{N}_{K/F}(\alpha)\mathbb{N}_{K/F}(\beta)$, tehát az $\mathbb{N}_{K/F}$ multiplikatív tulajdonságú.*

Mostantól térjünk vissza arra az esetre mikor az $F = \mathbb{Q}_p$. Legyen α egy algebrai szám, mely eleme $\mathbb{Q}_p^{\text{alg cl}}$ és legyen az α elemmel való bővítés foka n, mely tartalmazza α és $\mathbb{Q}_p$ elemeinek kombinációt, akkor ezen bővítés Galois bővítés. Legyen $\|\cdot\|$ K feletti norma, amely $|\cdot|_p$ norma kiterjesztése, és melyről tudjuk, hogy egyedi a 3.1.8 következmény miatt. Így ezen normán α-nak és α konjugáltjainak megegyező értéke kell, hogy legyen, mivel legyen $\|\cdot\|_\sigma$ olyan $\mathbb{Q}_p(\alpha)$ feletti norma, mely $\|x\|_\sigma = \|\sigma(x)\|$ $\forall x \in K$, akkor 3.1.8 következmény miatt tudjuk, hogy $\|\cdot\|_\sigma = \|\cdot\|$, így $\|\alpha\| = \|\alpha\|_\sigma = \|\sigma(\alpha)\| = \|\alpha_i\|$, ahol α_i azon konjugáltja α-nak, melyre teljesül, hogy $\sigma(\alpha) = \alpha_i$. Így tudjuk, hogy $\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)$ értékelés egyenlő a konjugáltakhoz tartozó értékeléssel.

Így α értékkel való bővítés feletti $\|\cdot\|$ normát definiálhatjuk úgy, mint $|\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(x)|_p^{\frac{1}{n}}$, ahol $x \in \mathbb{Q}_p(\alpha)$.

Az $\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)$-ra teljesül, hogy felírható, mint a konjugáltjainak szorzata, tehát

$$N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha) = \prod_{i=0}^{n-1} \alpha_i.$$

Ez által adódik, hogy

$$|\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p = \|\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\| = \|\prod_{i=0}^{n-1} \alpha_i\| = \prod_{i=0}^{n-1} \|\alpha_i\| = \|\alpha\|^n.$$

Ez mutatja, hogy α esetén tényleg megfelelő a normának a definíciója. Továbbá $\mathbb{Q}_p$ nem Galois-bővítésein is teljesül ezen definíció. Ha $\alpha \in K$, akkor

$$\mathbb{N}_{K/\mathbb{Q}_p}(\alpha) = \mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)^{[K:\mathbb{Q}_p(\alpha)]},$$

és mivel az is teljesül, hogy

$$n = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = \frac{[K : \mathbb{Q}_p]}{[K : \mathbb{Q}_p(\alpha)]}.$$

3.1.13. Tétel. *Legyen K véges bővítése $\mathbb{Q}_p$-nek, melynek bővítésének foka n. Továbbá legyen $\|\cdot\| : K \to R_{\geq 0}$ menő leképezés, amelyet úgy definiálunk, hogy minden $x \in K$ esetén*

$$\|x\| = |\mathbb{N}_{K/\mathbb{Q}_p}(x)|_p^{\frac{1}{n}},$$

akkor ezen leképezés norma K felett, és a $|\cdot|_p$ kiterjesztése.

3.1.14. Lemma. *Legyen $|\cdot|_p$ K test felett definiált norma, akkor $|1+x|_p \leq 1$ $\forall x \in K$, melyre $|x|_p \leq 1$.*

Bizonyítás. A $\mathbb{N}_{K/\mathbb{Q}_p}$ definíciója miatt feltehetjük, hogy a $K = \mathbb{Q}_p(x)$, tehát x primitív elem, továbbá az x elemmel való bővítés foka legyen n.

Legyen $\|\cdot\|_{\sup}$ azon mátrix norma, mely egyenlő $\max|m_{i,j}|_p$, ahol $M = \{m_{i,j}\}_{i,j=1}^n$ $\mathbb{Q}_p$ feletti mátrix. Vegyük az x elemmel való $\mathbb{Q}_p$ lineáris leképezést a $\{1, x, x^2, \ldots, x^{n-1}\}$ bázisban, mely mátrixa legyen $A = \{a_{i,j}\}$.

3.1.15. Állítás. *A $\{\|A^i\|_{\sup}\}_{i=1}^\infty$ sorozat korlátos.*

Bizonyítás. A bizonyítás indirekt módon fog menni, tehát tegyük fel, hogy nem korlátos, így létezik minden $j \in \mathbb{N}$-re egy i_j, hogy $\|A^{i_j}\|_{\sup} \geq j$. Ez által definiáljuk β_j-t, mely az A^{i_j} elemeinek maximuma. b_j legyen továbbá egyenlő, mint a $|\beta_j|_p = b_j$. Legyen $B_j = \frac{A^{i_j}}{\beta_j}$, akkor $\|B_j\|_{\sup} = 1$. Mivel tudjuk, hogy a sup-normára nézve az egységgömb kompakt, mivel $\mathbb{Q}_p$ lokálisan kompakt, így létezik egy konvergens részsorozat, mely tart egy B mátrixhoz. Ebből adódik, hogy a B mátrix determinánsa 0, mert

$$det(B_j) = \frac{det(A^{i_j})}{\beta^n} \leq \frac{det(A^{i_j})}{j^n} = \frac{|N_{\mathbb{Q}_p(x)/\mathbb{Q}_p}|_p^{i_j}}{j^n} = \frac{|x|_p^{i_j}}{j^n} \leq \frac{1}{j^n},$$

így $j \to \infty$ esetén teljesül, hogy $\det(B)=0$. $\det(B)=0$ következik, hogy létezik olyan $y \in \mathbb{Q}_p(x)$, melyre teljesül, hogy $By = 0$. Vegyük a $\{x^i y\}_{i=0}^{n-1}$ bázist, akkor az is igaz, hogy $Bx^i y = 0$. Azonban vehetjük x^j helyett az A^j mátrixot, mivel A^j-t az x^j elemmel való szorzással definiáltuk. Ebből adódik, hogy $(BA^j)y = (A^jB)y = A^jBy = 0$, mivel a B mátrix az A^{i_j} mátrixok limesze. $A^jBy = 0$ miatt az $\{A^j\}_{j=1}^{\infty}$ sorozat korlátos. □

Ez által $\{\|A^i\|_{\sup}\}_{i=1}^{\infty}$ sorozat korlátos. Legyen ezen C a korlát. $|1+x|_p$ értékét, így már képesek vagyunk becsülni. Legyen $N \in \mathbb{N}$ elég nagy, akkor

$$|1+x|_p^N = |det(1+A)^N|_p^{\frac{1}{n}} \leq (\|(1+A)^N\|_{\sup})$$

egyenlőtlenség teljesül, mivel $|\det(A)|_p = \max(|a_{i,j}|_p)^n = \|A\|_{\sup}^n$. Továbbá az is adódik, hogy

$$\left(\left\|(1+A)^N\right\|_{\sup}\right) \leq \left(\max_{i=0}^{N}\left(\left\|\binom{N}{i}A^i\right\|_{\sup}\right)\right) \leq \max_{i=0}^{N}\left(\left\|A^i\right\|_{\sup}\right) \leq C.$$

melyből következik, hogy

$$|1+x|_p \leq (\|(1+A)\|_{\sup}) \leq \sqrt[N]{C}$$

. Ha $N \to \infty$ esetén igazoltuk a lemmát. □

A Tétel bizonyítása: A $\mathbb{Q}_p$-beli elemekre látszódik, hogy ez megegyezik a régi definícióval. A norma első, két tulajdonsága egyértelműen adódik. A háromszög-egyenlőtlenség belátásához szükséges komolyabb munka. Legyen $x, y \in K$, ahol $|y|_p \geq |x|_p$, akkor legyen $z = \frac{x}{y}$ ebből adódik, hogy $|z|_p \leq 1$. A következő 3.1.14 lemma miatt teljesül, hogy $|1+z|_p \leq 1$, melyből következik a háromszög-egyenlőtlenség. Így $|x|_p = |\mathbb{N}_{K/\mathbb{Q}_p}(x)|_p^{\frac{1}{n}}$ tényleg norma K felett. □

3.1.16. Észrevétel. *Legyen $K = F(\alpha)$ az F test α elemmel való bővítés és ezen bővítés foka legyen n, akkor létezik egy n-fokú 1 főegyütthatós polinom $(a_0 + a_1x + \cdots + x^n)$, melynek az α gyöke, akkor $\|\alpha\|_K$ feletti értéke megkapható, mint $|a_0|_p^{\frac{1}{n}}$.*

3.1.17. Definíció. Legyen K véges bővítése egy $\mathbb{Q}_p$-nak, és legyen A azon összes $x \in K$-k halmaza, mely kielégítenek egy $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ alakú egyenletet, ahol $a_i \in \mathbb{Z}_p$ $\forall i$-re, akkor ezen halmazt nevezzük a $\mathbb{Z}_p$ test algebrai egész lezártjának a K testben.

3.1.18. Állítás. *Legyen K véges bővítése a $\mathbb{Q}_p$-nek, melynek legyen n a foka. Továbbá legyen A és M a következő halmazok:*

$$\mathcal{O}_K = \{x \in K : |x|_p \leq 1\},$$
$$\mathfrak{p}_K = \{x \in K : |x|_p < 1\}.$$

Akkor teljesül, hogy $\mathcal{O}_K$ gyűrű, továbbá $\mathbb{Z}_p$ test algebrai egész lezártja, és $\mathfrak{p}_K$ egyedi maximális ideál $\mathcal{O}_K$-ban. Így $\mathcal{O}_K/\mathfrak{p}_K$ test, mely $\mathbb{F}_p$ egy legfeljebb n-ed fokú bővítése.

3.1.19. Észrevétel. *Az $\mathcal{O}_K$ gyűrűt szokás a K bővítés értékelési gyűrűjének is nevezni a $|\cdot|_p$ normára nézve.*

Bizonyítás. Négy lépésben fogjuk az állítást belátni. Először lássuk be, hogy $\mathcal{O}_K$ algebrai egész lezártja $\mathbb{Z}_p$-nek K testben. Az egyértelműen látszik, hogy $\mathcal{O}_K$ gyűrű, mivel ki tudjuk használni, hogy $|\cdot|_p$ nem-Arkhimédészi norma. Legyen $\alpha \in K$, mely m-ed fokú bővítése Q_p-nek és legyen $\mathbb{Z}_p$ felett algebrai egész, akkor létezik egy olyan m-ed fokú $\mathbb{Z}_p$-beli együtthatós irreducibilis polinom, melynek gyöke $(\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0 = 0)$. Tegyük fel, hogy $\alpha \notin \mathcal{O}_K$, akkor teljesül, hogy

$$|\alpha|_p^m = |a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \cdots + a_0|_p \leq$$
$$\leq \max_{i=1}^{m}(|a_i\alpha^i|_p) \leq \max_{i=1}^{m}(|\alpha^i|_p) = |\alpha|_p^{m-1},$$

de ez meg ellentmondás, mivel feltettük, hogy $\alpha \notin \mathcal{O}_K$, így $\alpha \in \mathcal{O}_K$. Továbbá ebből következik, hogy az α konjugáltjai $\mathbb{Q}_p$ felett is $\mathcal{O}_K$-nak elemei, mivel $|\alpha_i|_p = \prod_{j=1}^{m} |\alpha_j|_p = |\alpha|_p \leq 1$. Ez azért igaz, mivel a konjugáltak által meghatározhatók a polinom együtthatói, így az együtthatók nem csak $\mathbb{Q}_p$-beliek, hanem $\mathbb{Z}_p$-beliek is.

Az látszik, hogy $\mathfrak{p}_K$ ideál $\mathcal{O}_K$-ban, mivel ez is könnyen ellenőrizhető a nem-Arkhimédészi norma tulajdonságai által. Tegyük fel, hogy $\mathfrak{p}_K$ nem maximális, tehát létezik olyan $\mathfrak{p}'_K$ ideál, melynek szigorú részhalmaza és nem a teljes $\mathcal{O}_K$. Azonban ez ellentmondás, mivel ha $\beta \in \mathcal{O}_K$, és $\beta \notin \mathfrak{p}_K$, akkor $|\beta|_p = 1$, és így $\frac{1}{\beta}$ is eleme az $\mathfrak{p}'_K$-nek, mely ellentmondás, mivel akkor $1 \in \mathfrak{p}'_K$, tehát $\mathfrak{p}'_K = \mathcal{O}_K$.

Így teljesül, hogy $\mathcal{O}_K/\mathfrak{p}_K$ test és $\mathfrak{p}_K \cap \mathbb{Z}_p = p\mathbb{Z}_p$. Így ha vesszük azt a beleképezést, hogy $a + p\mathbb{Z}_p \mapsto a + \mathfrak{p}_K$, ahol $a \in \mathbb{Z}_p$, tehát ez azt jelenti, hogy $\mathcal{O}_K/\mathfrak{p}_K$-nek résztestje a $\mathbb{Z}_p/p\mathbb{Z}_p$, ahol tudjuk, hogy $\mathbb{Z}_p/p\mathbb{Z}_p$ p elemű véges test ($\mathbb{F}_p$).

Végül már csak annyi maradt hátra, hogy belássuk, hogy $\mathcal{O}_K/\mathfrak{p}_K$ n-ed fokú bővítés. Az biztosan tudjuk, hogy $[\mathcal{O}_K/\mathfrak{p}_K : \mathbb{F}_p] \leq [K : \mathbb{Q}_p]$, tehát elég csak azt belátni, hogy n-nél kisebb nem lehet. Legyen $\alpha_i \in \mathcal{O}_K$ ($i \in \{1, \ldots, n\}$), és vegyük azt a leképezést, mely egy $\mathcal{O}_K$-beli elemhez hozzárendeli $\mathcal{O}_K/\mathfrak{p}_K$-beli mellékosztályt, tehát $\widehat{\alpha} \mapsto \alpha + \mathfrak{p}_K$. Azt tudjuk, hogy tetszőleges $n+1$ darab K-beli szám esetén ezek biztosan összefüggőek, tehát létezik olyan $\beta_i \in \mathbb{Q}_p$ ($i \in \{1, \ldots, n\}$), melyre $\alpha_1\beta_1 + \cdots + \alpha_n\beta_n = 0$. Ha felszorzunk a β-k közül azon legnagyobb p hatvánnyal, mely osztja valamelyiket, akkor így $\mathbb{Z}_p$-beli számokat kapunk, tehát feltehető, hogy β-k $\mathbb{Z}_p$-beliek. Továbbá lesz egy olyan β, mely nem lesz eleme $p\mathbb{Z}_p$-nek. Az előbb definiált leképezés miatt tudjuk, hogy $\widehat{\alpha_1}\widehat{\beta_1} + \cdots + \widehat{\alpha_n}\widehat{\beta_n} = 0$ teljesül, tehát $\widehat{\alpha_i}$ lineárisan összefüggőek, mivel létezik olyan i, melyre $\widehat{\beta_i}$ nem nulla. Így beláttuk, hogy $[\mathcal{O}_K/\mathfrak{p}_K : \mathbb{F}_p] = n$. □

3.2. Út az Ω-ig

A következő fejezet során Gouvea ((2003)) könyvének a 6.4-es fejezete és az eddig is követett Koblitz ((2012)) könyve lesz a segítségünkre.

A $|\cdot|_p$ norma $\mathbb{Q}_p$ feletti definíciója miatt tudjuk, hogy $x \in \mathbb{Q}_p$ szám normája megkapható a p-adikus értékelése segítségével, akkor ezen tulajdonság és $\mathbb{N}_{K/\mathbb{Q}_p}$ definíciója maitt meghatározható tetszőleges $\mathbb{Q}_p$ véges bővítésében lévő elemeknek a p-adikus értékelése, mivel

$$\log_p(\|\alpha\|) = \log_p\left(|\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{\frac{1}{n}}\right) = \frac{1}{n}\log_p\left(p^{-\operatorname{ord}_p\left(\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)\right)}\right) =$$

$$= \frac{-\operatorname{ord}_p\left(\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)\right)}{n} = \frac{-\operatorname{ord}_p\left(\prod_{i=1}^{n}\alpha_i\right)}{n} = (-1)\cdot\sum_{i=1}^{n}\frac{\operatorname{ord}_p(\alpha_i)}{n} =$$

$$= (-1)\cdot\frac{n\operatorname{ord}_p(\alpha)}{n} = -\operatorname{ord}_p(\alpha),$$

ahol n a bővítés foka, $\alpha \in K$, és $\log_p$ a p alapú logaritmust jelenti. Ez által tudjuk, úgy definiálni K test feletti normát, ahol K test véges bővítése a $\mathbb{Q}_p$-nek, hogy tetszőleges $x \in K^\times$ elem esetén legyen a K feletti normájának értéke: $\|x\| = p^{-\operatorname{ord}_p(x)}$, különben ha x=0, akkor $\operatorname{ord}_p = \infty$ által $|x| = 0$. Mostantól így jelölhetjük $\|\cdot\|$ normát $|\cdot|_p$-vel.

A p-adikus értékelés $\mathbb{Q}_p$ körében tudjuk, hogy a leképezés képhalmaza az egész számok, így ez által ás az előző definíció miatt tudjuk, hogy a $\mathbb{Q}_p$ véges bővítésein a p-adikus értékelés képhalmaza $\frac{1}{n}\mathbb{Z}$ halmaz vagy azon valamilyen részhalmaza lesz.

3.2.1. Állítás. *A p-adikus értékelés $K^\times$-ból $\mathbb{Q}$ additív csoportjába képező homomorfizmus, mely képhalmaza $\frac{1}{e}\mathbb{Z}$, ahol e K-nak a $\mathbb{Q}_p$ feletti bővítés fokának osztója.*

Bizonyítás. A p-adikus értékelés, mint leképezés homomorfizmus következik abból, hogy ezen elképezés additív tulajdonságú, tehát

$$\operatorname{ord}_p(xy) = \operatorname{ord}_p(x) + \operatorname{ord}_p(y).$$

Legyen $x \in K^\times$, melyre teljesül, hogy $\mathrm{ord}_p(x) = \frac{d}{e}$, ahol d és e relatív prímek. Így létezik olyan q melyre teljsül, hogy $dq \equiv 1 \pmod p$, tehát $qd = 1 + se$ alakban felírható, ahol $s \in \mathbb{Z}$, így ebből kikeverhető, hogy $q\frac{d}{e} = \frac{1}{e} + s$, tehát p-adikus értékelés képe tényleg $\frac{1}{e}\mathbb{Z}$. □

3.2.2. Definíció. Legyen K n-ed fokú bővítése $\mathbb{Q}_p$-nek, akkor az e számot nevezzük a $k = K/\mathbb{Q}_p$ hányadostest elágazási indexének, ahol ezen e az előző állításban szerepett kapott e legyen. Továbbá a k hányadostest bővítésének foka legyen f.

A következőkben látni fogjuk, hogy az f definíciója megfelelő lesz és, hogy a K, mint $\mathbb{Q}_p$ feletti véges bővítés foka $f \cdot e$ lesz.

A K bővítést az e értékei alapján különbözőképpen nevezzük. Először is ha $e = 1$, akkor azt mondjuk, hogy a K bővítést nem-elágazónak nevezzük és szokás úgy is jelölni, hogy K^{unram}. Továbbá ha $e = n$, ahol n a K bővítésének foka, akkor a K bővítést teljesen elágazónak nevezzük, és ha $e > 1$, de kisebb, mint n, akkor elágazó bővítésnek hívjuk.

A teljesen elágazó eseteben az elágazási indexet, ha a p prím osztja, akkor vad elágazásnak nevezzük, ha a p prím nem osztja az elágazási indexet, akkor szelíd elágazásnak nevezzük.

3.2.3. Definíció. Legyen K véges bővítése $\mathbb{Q}_p$-nek és legyen e az elágazási index, akkor azon K-beli számot, melynek p-adikus értékelése $\frac{1}{e}$ nevezzük irreducibilis elemnek vagy prímelemnek és π-vel jelöljük.

Az irreducibilis elem elnevezést használja Serre ((1995)) könyve is, de mivel főideálgyűrűben az irreducibilis és a prímelemek megegyeznek, így prímelemnek fogjuk hívni.

Elágazó esetekben a prímelem nem egyértelmű, mivel több K-beli szám értéke is lehet $\frac{1}{e}$, de ha nem-elágazó esetben, megszokás szerint p prímet választjuk irreducibilis elemnek.

A következő állítások csoportja miatt látni fogjuk miért prímelemnek szokás hívni.

3.2.4. Állítás. *Legyen K véges bővítése $\mathbb{Q}_p$-nek és legyen π egy fix prímelem, akkor a következő állítások teljesülnek:*

1. *$\mathfrak{p}_K$ ($\subset \mathcal{O}_K$) főideál, és π generálja az ideált.*
2. *x tetszőleges eleme K-nak, akkor felírható, mint $x = \pi^{e\,\mathrm{ord}_p(x)} \cdot u$, ahol $u \in \mathcal{O}_K^\times$, tehát egy egységelem, így $K = \mathcal{O}_K^\times\left[\frac{1}{\pi}\right]$.*
3. *k hányadostest véges bővítése $\mathbb{F}_p$-nek, melynek foka legfeljebb $n = [K : \mathbb{Q}_p]$, tehát k elemszáma p-nek egy megfelelő hatványa.*
4. *Minden eleme a $\mathcal{O}_K$-nak gyöke egy 1 főegyüttható polinomnak, melynek együtthatói $\mathbb{Z}_p$-beliek. Ezen állítás megfordítása is igaz.*
5. *$\mathcal{O}_K$ kompakt topológikus gyűrű.*
6. *$\pi^m\mathcal{O}_K$ halmaz teljesen nem-összefüggő, Hausdorff (T_2), lokálisan kompakt topológikus tér, mely továbbá a nulla pont egy környezete K-ban.*
7. *Legyen i a k hányadostest elemeinek száma és legyen $A = \alpha_1, \alpha_2, \cdots, \alpha_i$ azon halmaz, mely részhalmaza $\mathcal{O}_p$-nek, ahol α-k a k hányadostestbeli elemek egy-egy reprezentánsai, akkor tetszőleges $x \in K$ felírható, mint*

$$x = \sum_{j=-m}^{\infty} a_j \pi^j,$$

ahol $m = e\,\mathrm{ord}_p(x)$ és $a_j \in A$ minden j-re.

Bizonyítás. A 5.-ös, 6.-os, 7.-es állítások bizonyítása megegyezik a Q_p-ben végzett bizonyítással, így ezeket itt nem látjuk be. A többi állításnak a bizonyítását itt most nem végezzük el, de megtalálható Gouvea ((2003)) könyvében, azon belül pontosan 6.4.5.-ös lemma utáni problémában vannak segítségek a bizonyításhoz. □

3.2.5. Tétel. *Legyen K n-ed fokú bővítése $\mathbb{Q}_p$-nak. A k hányadostest foka legyen f és az elágazási index e, akkor $n = e \cdot f$.*

Bizonyítás. A bizonyításunk arról szól, hogyha veszünk egy f elemű bázis a k hányadostestben, akkor ha π elem e különböző hatványainak és egy k-beli bázisnak kombinációiból a K test egy bázisát kapjuk.

Legyen $\{\hat{\alpha}_1, \hat{\alpha}_2, \ldots, \hat{\alpha}_f\}$ k-beli bázis, és ez által legyen $\{\alpha_1, \alpha_2, \ldots, \alpha_f\}$ bázis $\mathcal{O}_K$-ban. Ez által ha $\mathcal{O}_K$ összes eleme előáll $\pi^j\alpha_i$-k $\mathbb{Q}_p$ lineáris kombinációjaként, ahol $j \in \{0, \ldots, e-1\}$, $i \in \{1, \ldots, f\}$, akkor megfelelő p esetén teljesül, hogy K összes eleme előáll ezen elemek $\mathbb{Q}_p$ lineáris kombinációjaként, mivel $p^l x \in \mathcal{O}_K$, ha $x \in K$. Ennek köszönhetően mostantól fix $x \in \mathcal{O}_K$ esetén, akkor elég $\mathbb{Z}_p$ lineáris kombinációként is előállani. Azonban, mivel x modulo π^j mindig felírható, mint

$$x = x_{0,1}\alpha_1 + \cdots + x_{0,f}\alpha_f + \cdots + x_{j-1,1}\alpha_1\pi^{j-1} + \cdots + x_{j-1,f}\alpha_f\pi^{j-1}$$

alakban $j \in \{0, \ldots, e-1\}$-re, ahol a kombináció együtthatói már $\mathbb{Z}_p$-beliek. Ennél nagyobb hatványokra látható π^e és p-nek a p-adikus értékelése megegyezik, tehát x írható, mint

$$x = x_{0,1}\alpha_1 + \cdots + x_{0,f}\alpha_f + \cdots + x_{j-1,f}\alpha_1\pi^{j-1} + \cdots + x_{e-1,f}\alpha_f\pi^{e-1} + px',$$

ahol $x' \in \mathcal{O}_K$. Az előző gondolatmenet miatt x' is felírható az $\alpha_i\pi^j$-k segítségével, tehát

$$\begin{aligned} x = {} & x_{0,1}\alpha_1 + \cdots + x_{0,f}\alpha_f + \cdots + x_{e-1,f}\alpha_1\pi^{e-1} + \cdots + x_{e-1,f}\alpha_f\pi^{e-1} + \\ & + p \cdot (x'_{0,1}\alpha_1 + \cdots + x'_{0,f}\alpha_f + \cdots + x'_{e-1,f}\alpha_1\pi^{e-1} + \cdots + x'_{e-1,f}\alpha_f\pi^{e-1} + px''). \end{aligned}$$

Innen látszik, hogy x'' már p^2-tel szorzódik, és így x felírható tovább minden $x^{(s')}$-re, ahol (s')-val a s darab vesszőt szimbolizálom. Ennek köszönhetően minden j, i-re, ahol $j \in \{0, \ldots, e-1\}$, $i \in \{1, \ldots, f\}$, kialakul $\mathbb{Z}_p$-ben konvergens összeg, mint például

$$x_{j,i} + px'_{j,i} + px''_{j,i} + \cdots + p^s x^{(s')}_{j,i} + \ldots,$$

amelynek a határértékét jelöljük $y_{j,i}$-vel. Így x véglegesen felírható, mint

$$x = \sum_{0=1}^{e-1}\sum_{i=1}^{f} y_{j,i}\pi^j\alpha_i,$$

tehát tényleg generálja K összes elemét a

$$\begin{gathered} \alpha_1, \alpha_2, \ldots, \alpha_f, \\ \alpha_1\pi, \alpha_2\pi, \ldots, \alpha_f\pi, \\ \ldots, \\ \alpha_1\pi^{e-1}, \alpha_2\pi^{e-1}, \ldots, \alpha_f\pi^{e-1} \end{gathered}$$

számok halmaza. Ez által a generátorrendszerséget beláttuk.

Az állítás bizonyításához már csak arra van szükségünk, hogy az előző generátorrendszer lineárisan független.

Azt kell belátni, hogy

$$0 = \sum_{0=1}^{e-1}\sum_{i=1}^{f} x_{j,i}\pi^j\alpha_i,$$

csak akkor teljesül, ha minden $x_{j,i}$ együttható nulla. Tegyük fel, hogy összefüggő, tehát ezen együtthatók között létezik olyan $x_{j,i}$, mely nem nulla tehát, akkor létezik egy olyan együttható is, mely nem osztható p-vel. Ez azért igaz, mivel előbb láttuk, hogy ezen $x_{j,i}$ együtthatók nem csak $\mathbb{Q}_p$-beliek, hanem $\mathbb{Z}_p$-beliek is.

A következő gondolatmenetem az összefüggőségre e értéke szerint fog menni. Ha $e = 1$, akkor a dupla szummát modulo π szerint kell nézni, tehát így azt kapjuk, hogy

$$0 = \sum_{i=1}^{f} x_{0,i}\alpha_i.$$

Ez azért ellentmondás, mivel $\hat{\alpha}$-k k-ban bázist alkotnak, tehát az összes együttható csak nulla lehet modulo π, tehát osztható p-vel. Ha $e > 1$, akkor $x_{0,i}$ együtthatók oszthatók π^2-is, mivel a p-adikus értékelése $\frac{x_{0,i}}{\pi}$, szigorúan nagyobb, mint 1. Így modulo π^2 $x_{0,i}$ és $x_{1,i}$ együtthatók kongruensek nullával, tehát oszthatók p-vel, így $e = 2$ esetén újból ellentmondásra jutottunk. Ezen gondolatmenet folytatása által minden e értékre ellentmondásra juthatunk, így minden $x_{j,i}$ együttható osztható p-vel, tehát minden $x_{i,j} \in \mathbb{Z}_p$. Ez által beláttuk, hogy

$$\begin{gathered}\alpha_1, \alpha_2, \ldots, \alpha_f, \\ \alpha_1\pi, \alpha_2\pi, \ldots, \alpha_f\pi, \\ \ldots, \\ \alpha_1\pi^{e-1}, \alpha_2\pi^{e-1}, \ldots, \alpha_f\pi^{e-1}\end{gathered}$$

elemek halmaza tényleg egy bázisa K-nak. □

A K véges bővítésünk teljesen elágazó, akkor a $\mathbb{Q}$ felett is ismert Schönemann-Eisenstein tétel is teljesül, amely a következő alakban mondunk ki:

3.2.6. Állítás (Schönemann-Eisenstein tétele)**.** *Legyen K teljesen elágazó véges bővítése $\mathbb{Q}_p$-nek és legyen π a prímelem. Továbbá legyen $P(x) = x^e + \cdots + a_0$ polinom, ahol $a_i \equiv 0 \pmod p$ $\forall i \in \{0, 1, \ldots, e-1\}$, és $a_0 \not\equiv 0 \pmod{p^2}$, ahol ezen $P(x)$ polinomot szokás Eisenstein-polinomnak is nevezni, akkor π prímelem gyöke lesz az Eisenstein-polinomnak.*

A bizonyítás megegyezik $\mathbb{Q}_p$ és $\mathbb{Q}$ felettivel, tehát mégegyszer itt nem írjuk le ugyanazon bizonyítást.

3.2.7. Észrevétel. *Az állítás fordítása is teljesül, tehát β legyen gyöke az Eisenstein-polinomnak, akkor a $\mathbb{Q}_p$-t a β elemmel bővítve teljesen elágazó bővítést kapunk.*

3.2.8. Állítás. *Legyen K teljesen elágazó bővítése $\mathbb{Q}_p$-nek és legyen a bővítésének foka e, akkor tetszőleges $\alpha \in \mathbb{Z}_p$-hez, melyre teljesül, hogy $\operatorname{ord}_p(\alpha) = 1$, létezik olyan $\beta \in K$, hogy*

$$|\beta^e - \alpha|_p < \frac{1}{p}.$$

Bizonyítás. Vegyük azt az Eisenstein-polinomot, melynek $-a_0 = \alpha$, akkor a 3.2.6 állítás miatt létezik egy olyan $\beta \in K$, melyre teljesül, hogy $\operatorname{ord}_p(\beta) = \frac{1}{e}$, és gyöke a polinomnak. Továbbá

$$\beta^e - \alpha = -a_{e-1}\beta^{e-1} - \cdots - a_1\beta$$

egyenlőség teljesül, ahol a jobb oldal p-adikus értékelése kisebb, mint $\frac{1}{p}$, tehát beláttuk az állítást. □

A $\mathbb{Q}_p$ véges bővítésein teljesül egy jól-ismert tételünk is, ami nem más mint a Hensel-lemma. A következő állítás rögtön következik a Hensel-lemmából.

3.2.9. Állítás. *Legyen K egy szelíd totálisan elágazó bővítése $\mathbb{Q}_p$-nek. Ha létezik olyan $\beta \in \mathbb{Q}_p$ szám, mely gyöke a $X^e - b$ polinomnak, ahol $b \in \mathbb{Z}_p$ és $\operatorname{ord}_p(b) = 1$, akkor $K = \mathbb{Q}_p(\beta)$.*

Bizonyítás. Az $X^e - b$ Eisenstein polinom, így a 3.2.7 észrevétel miatt, teljesül az állítás. □

3.2.10. Tétel. *Minden f-re pontosan egy nem-elágazó bővítése létezik $\mathbb{Q}_p$-nek, melyet úgy kaphatunk meg, hogy a $\mathbb{Q}_p$-t a $(p^f - 1)$-edik primitív egységgyökkel bővítünk.*

Bizonyítás. Három lépésben fogjuk belátni a tételt, először belátjuk, hogy létezik f-ed fokú nemelágazó bővítése $\mathbb{Q}_p$-nek, majd azt, hogy ezen bővítés, úgy áll elő, mint a $(p^f - 1)$. primitív egységgyökkel való bővítése a $\mathbb{Q}_p$-nek, végül belátjuk az egyediséget.

Azt tudjuk, hogy $\mathbb{Q}_p$ f-ed fokú véges bővítésének p-adikus értékelési gyűrűjének és maximális ideáljának hányadosteste $\mathbb{F}_p$-nek legfeljebb f-ed fokú bővítése. Ha az $\mathbb{F}_{p^f}$-nek vesszük egy $\overline{\alpha}$ generátorelemét, akkor Schönemann-Eisenstein tétel miatt létezik egy olyan $\overline{P(x)} = x^f + \overline{a_{f-1}}x^{f-1} + \cdots + \overline{a_0}$ irreducibilis 1 főegyüttható polinom, amelynek gyöke, ahol $\overline{P(X)}$ polinom együtthatói $\mathbb{F}_p$-beliek. Az

$\mathbb{F}_p$-beli számokhoz meghatározhatunk $\mathbb{Z}_p$-beliek, mivel $\overline{a_i} \equiv a_i \pmod p$, ahol $a_i \in \mathbb{Z}_p$, és $\overline{a_i} \in \mathbb{F}_p$ gyöke $\overline{P(X)}$-nek. A $\overline{P(x)}$ polinomhoz így hozzátudunk rendelni egy $\mathbb{Z}_p$ együtthatós polinomot, amelyet jelöljünk $P(X)$-el, mely $\mathbb{Q}_p$ felett is irreducibilis lesz. Ha veszünk egy $\alpha \in \mathbb{Q}_p^{\text{alg cl}}$ számot, mely gyöke a $P(X)$ irreducibilis polinomak, akkor ha ezzel bővítjük a $\mathbb{Q}_p$-t kapunk f-ed fokú bővítését $\mathbb{Q}_p$-nek, melyet jelöljünk K-vel. Továbbá a $\alpha + M$, ahol M maximális ideálja K-nak, gyöke lesz a $\overline{P(X)}$-nek, tehát K test hányadostestének $\mathbb{F}_p$ feletti bővítésének foka f lesz, így beláttuk, hogy létezik f-ed fokú nem-elágazó bővítése $\mathbb{Q}_p$-nek.

Legyen F egy f-ed fokú nem-elágazó bővítése a $\mathbb{Q}_p$-nek, továbbá a megszokott módon definiáljuk hozzá az értékelési gyűrűjét (A) és ezen gyűrű maximális ideálját (M). Végső soron legyen π az irreducibilis elem. Vegyük a $\mathbb{F}_p^f$ egy $\overline{\alpha}$ generátorelemét, mely modulo M értéke legyen $\alpha_0 \in A$, akkor feltehetjük, hogy $\alpha \in \overline{\mathbb{Q}_p}$ elemre teljesül, hogy $\alpha^{p^f-1} - 1 = 0$ és $\alpha_0 \equiv \alpha \pmod \pi$. Innentől a Hensel-lemma bizonyításában használt gondolatmenettel megalkotjuk az α-t a π különböző hatványainak kombinációjából.

Modulo π^2 teljesül, hogy $\alpha_0 + \alpha_1\pi$ kongruens egy α-val, tehát $(\text{mod } \pi^2)$

$$0 \equiv (\alpha_0 + \alpha_1\pi)^{p^f-1} - 1 \equiv \sum_{i=0}^{p^f-1} \left(\binom{p^f-1}{i} \alpha_0^i (\pi\alpha_1)^{p^f-1-i} \right) - 1 \equiv$$
$$\equiv \alpha_0^{p^f-1} + (p^f-1)\pi\alpha_1\alpha_0^{p^f-2} - 1 \equiv \alpha_0^{p^f-1} + \pi\alpha_1\alpha_0^{p^f-2} - 1.$$

Ebből kifejezhető az α_1 modulo π, akkor ezen gondolatmenetet tovább folytatva $\pi^j \ \forall j \in \mathbb{N}$ hatványra megkapjuk az α értékét, amely kielégíti a $\alpha^{p^f-1} - 1 = 0$ egyenletet. Az α primitív (p^f-1). egységgyök lesz $\mathbb{Q}_p$ felett, mivel α első (p^f-1) darab hatványa különböző lesz, mivel modulo M különböző, tehát az α elemmel való bővítés foka legalább f. Azonban az is teljesül, hogy $F \subset \mathbb{Q}_p(\alpha)$, ahol α (p^f-1). egységgyök F-ban, így pontosan f-ed fokú, és mivel F nem-elágazó bővítése $\mathbb{Q}_p$-nek, így beláttuk, hogy $\mathbb{Q}_p(\alpha)$ f fokú nem-elágazó bővítése $\mathbb{Q}_p$-nek. □

3.2.11. Következmény. *Legyen K n-ed fokú bővítése $\mathbb{Q}_p$-nek, melyre teljesül, hogy e az elágazási indexe, f a hányadostest foka, akkor $K = K_f^{\text{unram}}(\pi)$, ahol π gyöke a K_f^{unram} feletti Eisenstein-polinomnak.*

Bizonyítás. A 3.2.5 tétel miatt tudjuk, hogy K $\mathbb{Q}_p$ feletti bővítésének foka $e \cdot f$. Jelöljük $E(X)$-el azon 1 főegyütthatós irreducibilis polinomot, melynek π gyöke, akkor a π konjugáltjai is gyökei kell, hogy legyenek, tehát $E(x) = \prod(x - \pi_i)$ alakban előáll. Legyen $E(X)$ polinom foka d és a konstans tag meg legyen c, akkor $\text{ord}_p(c) = \frac{d}{e}$, mivel $c \in K_f^{\text{unram}}$, így $\text{ord}_p(c) = 1$, és a fokszámtétel miatt teljesül, hogy $e = d$, tehát $E(X)$ Eisenstein polinom és $K = K_f^{\text{unram}}(\pi)$. □

3.2.12. Következmény. *Legyen K véges bővítése $\mathbb{Q}_p$-nek és legyen $m = p^f - 1$. Ha létezik egy olyan $\alpha \in K$ és ζ egy primitív m. egységgyök $\overline{\mathbb{Q}_p}$-ben, melyre teljesül, hogy $\alpha \equiv \zeta \ (\text{mod } p)$, akkor K tartalmaz egy f fokú nem-elágazó bővítését $\mathbb{Q}_p$-nek.*

A következmények bizonyítása következik a 3.2.10 tételből.

Legyen K azon egyedi (p^f-1)-ed fokú nem-elágazó bővítése $\mathbb{Q}_p$-nek, melyet úgy kapunk meg, hogy (p^f-1)-edik primitív egységgyökkel bővítjük a $\mathbb{Q}_p$-t. A Dwork tételének bizonyításában, és általában is fontos szerepet fog játszani azon K hányadostestéről $\mathcal{O}_K$-ba menő felemelés, melyet Teichmüller felemelésnek szokás nevezni. Továbbá ezen felemelés ad egy izomorf megfeleltetést az egységgyökök multiplikatív csoportja és a p-adikus egységek csoportja között, vagyis jelen esetben az $\mathcal{O}_K$-beli elemekkel.

3.2.13. Definíció. Legyen K egy egyedi s-ed fokú nem-elágazó bővítése $\mathbb{Q}_p$-nek, akkor azon multiplikatív csoporthomomorfizmust, mely leírható, mint

$$\begin{array}{rccc} \tau_s: & \mathbb{F}_{p^s} & \to & \mathcal{O}_K \\ & x & \mapsto & \tau_s(x). \end{array}$$

Az $\mathbb{F}_{p^s}$-beli x-eket szokás a primitív p^s-edik egységgyökkel reprezentálni, amelyeket Teichmüller reprezentánsoknak is neveznek.

3.2.14. Lemma (Krasner-lemma)**.** *Legyen $a, b \in \overline{\mathbb{Q}_p}$, és ha a összes a_i konjugáltjára teljesül, hogy*

$$|b-a|_p \leq |a_i - a|_p,$$

akkor $\mathbb{Q}_p(a) \subset \mathbb{Q}_p(b)$.

Bizonyítás. A bizonyításunk indirekt módon fog menni, tehát tegyük fel, hogy $a \notin \mathbb{Q}_p(b)$, akkor az a számmal való tovább bővítés foka több, mint 1, így létezik legalább egy a_i konjugáltja a-nak, mely nem eleme $\mathbb{Q}_p(b)$-nek és nem az a-val egyenlő. Továbbá létezik egy olyan automorfizmus, mely $\mathbb{Q}_p(b)$-t fixen hagyja, és a képe az a_i konjugált. Azt a korábbiakban láttuk, hogy a konjugáltaknak a p-adikus értékelése megegyezik tetszőleges véges testbővítés felett. Így felírható azon egyenlőség, hogy $|b-a|_p = |\sigma(b) - \sigma(a)|_p = |b - a_i|_p$. Így ebből következik, hogy

$$|a_i - a|_p = |a_i - b + b - a|_p \leq \max(|a_i - b|_p, |b-a|_p) = |b-a|_p < |a_i - a|_p,$$

amely meg ellentmondás, így teljesül, hogy $\mathbb{Q}_p(a) \subset \mathbb{Q}_p(b)$. □

Két polinom távolságát definiálhatjuk az együtthatóik különbségének maximumával, tehát

$$|P-G|_p = \max_{i=1,j=1} |a_i - b_j|_p,$$

ahol $P(X) = \sum_{i=1} a_i X^i$, $P \in F[X]$, és $G(X) = \sum_{j=1} b_i X^i$, $G \in F[X]$.

3.2.15. Állítás. *Legyen K véges bővítése $\mathbb{Q}_p$-nek, és legyen $P(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ $\mathbb{Q}_p$ együtthatós irreducibilis polinom, melynek $\overline{\mathbb{Q}_p}$-ben a gyökei különbözőek, akkor $\forall \epsilon > 0$ teljesül, hogy $\exists \delta > 0$, hogy $G(X) = \sum_{i=0}^{n} b_i X^i \in K[X]$, melyre teljesül, hogy $|G(X) - P(X)|_p < \delta$, akkor $P(X)$ minden α_i gyökére létezik pontosan egy olyan β_j gyöke $G(X)$-nek, melyre teljesül, hogy $|\beta_j - \alpha_i|_p < \epsilon$.*

Bizonyítás. Legyen β tetszőleges gyöke a $G(X)$ polinomnak. Akkor igaz lesz, hogy

$$|P(\beta)|_p = |P(\beta) - G(\beta)|_p = \left| \sum_{i=1}^{n} (a_i - b_i)\beta^i \right|_p \leq$$
$$\leq \max_{i=1}^{n}(|\beta|_p^i, |a_i - b_i|_p) \leq |P-G|_p \max(1, |\beta|_p^n) < \delta C_1^n,$$

ahol $C_1 = \max(1, |\beta|_p^n)$. Továbbá legyen $C_2 = \min_{i,j=1}^{n}(|\alpha_i - \alpha_j|_p)$, amelyből következik, hogy $|\beta - \alpha_i|_p < C_2$ pontosan egy i-re teljesülhet, azért mert különben $|\alpha_i - \alpha_j|_p \leq \max(|\alpha_i - b|_p, |b - \alpha_j|_p) < C_2$ is igaz lenne, amely meg ellentmondás. Így

$$C_1^n \delta > |P(\beta)|_p = \left| a_n \prod_{i=1}^{n} (\alpha_i - \beta) \right|_p = |a_n|_p \prod_{i=1}^{n} |\alpha_i - \beta|_p$$
$$\Updownarrow$$
$$|\alpha_i - \beta|_p < \frac{C_1^n \delta}{|a_n|_p \prod_{j \neq i} |\alpha_j - \beta|_p} \leq \frac{C_1^n \delta}{|a_n|_p C_2^{n-1}},$$

amelyre teljesül, hogy kisebb, mint ϵ megfelelő δ segítségével. □

3.2.16. Tétel. $\mathbb{Q}_p^{\text{alg cl}} = \overline{\mathbb{Q}_p}$ *nem teljes.*

A bizonyításban Gouvea ((2003)) könyvének 6.8.4-es tételének bizonyítása lesz a segítségünkre.

Bizonyítás. Ha megmutatjuk, hogy tudunk egy olyan $\{a_i\}_{i=0}^{\infty}$ Cauchy-sorozatot mutatni, melynek nincsen $\overline{\mathbb{Q}_p}$-ban határértéke. Definiáljunk minden j-re egy ζ_j számot, melyek legyenek $(p^{2^j} - 1)$.

primitív egységgyökök $\overline{\mathbb{Q}_p}$ felett, akkor legyenek az $\{a_i\}_{i=0}^{\infty}$ sorozat elemei $a_i = \sum_{j=0}^{i} \zeta_j p^j$. Ezen definiálás által adódik, hogy $\{a_i\}_{i=0}^{\infty}$ sorozat Cauchy, mivel $n > m$

$$|a_n - a_m|_p = \left| \sum_{i=m+1}^{n} \zeta_i p^i \right|_p \leq \max_{i=m+1}^{n} \left(p^{-i}\right).$$

Be fogjuk látni, hogy ennek a sorozatnak nincs határértéke $\overline{\mathbb{Q}_p}$ felett. Ezt indirekten fogjuk belátni tegyük fel, hogy létezik egy $\alpha \in \overline{\mathbb{Q}_p}$, mely a határértéke $\{a_i\}_{i=0}^{\infty}$ Cauchy-sorozatnak. Így létezik egy irreducibilis polinom $\overline{\mathbb{Q}_p}$ felett, melynek gyöke, és a polinom együtthatói $\mathbb{Q}_p$-beliek. Tegyük fel, hogy valamilyen véges d foka van, ha az α elemmel bővítünk. Az $\alpha = \sum_{n=0}^{\infty} \zeta_n p^n$ alakban írható. Mivel modulo p α kongruens ζ_0-lal, így alkalmazható a 3.2.12 következmény, tehát $d = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \geq [\mathbb{Q}_p(\zeta_0) : \mathbb{Q}_p] = 2^0$. Ezt minden j-re eljátszható, így következik, hogy $d \geq 2^j$, de ez meg ellentmondás, mivel feltettük, hogy létezik egy polinom, melynek gyöke, így tényleg nincs határértéke $\{a_j\}_{j=0}^{\infty}$ Cauchy-sorozatnak. □

3.2.17. Észrevétel. *Az előző bizonyításban definiált Cauchy-sorozat nem csak $\overline{\mathbb{Q}_p}$-ben van benne, hanem azon unióban van benne, amely az összes véges nem-elágazó $\mathbb{Q}_p$ bővítéséből áll. Szokás ezt a bővítést maximális nem-elágazó bővítésnek is nevezni.*

Az előző tételben láttuk, hogy $\mathbb{Q}_p$ algebrai lezártja nem teljes a p-adikus értékelésre nézve, tehát tovább kell bővíteni a $\mathbb{Q}_p$-t, hogy egy teljes, algebrailag zárt testet kapjuk. Ez megegyező módon fogjuk csinálni, úgymint ahogy a $\mathbb{Q}$-ról $\mathbb{Q}_p$-re léptünk. Ezen módon megkapjuk az Ω-t, mely a $\overline{\mathbb{Q}_p}$ olyan bővítése, amely teljes. Továbbá a p-adikus értékelés kiterjesztése is megegyező azzal, mint a $\mathbb{Q}_p$-ról $\mathbb{Q}_p$ véges bővítésére vettünk. A következő tétel miatt látni fogjuk, hogy ezen Ω megfelelő lesz, tehát algebrailag zárt és teljes is lesz.

Az Ω-ban minden korábban definiált halmaz, leképezés, topológia megegyezik a $\mathbb{Q}_p$-ben definiáltakkal, és a $\mathbb{Q}_p$ bővítéseiben definiáltakkal is, mivel ezek egymásba ágyazott sűrű halmazok.

3.2.18. Tétel. *Ω algebrailag zárt.*

Bizonyítás. Legyen $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ polinom, melynek együtthatói Ω-beliek. Arra van szükségünk, hogy belássuk, hogy Ω-ban van gyöke $P(X)$-nek. A $P(X)$ polinom mindenegyes együtthatójához rendeljünk hozzá egy $\{a_{i,j}\}_{j=0}^{\infty}$ sorozatot, melyeknek a határértékei az a_i-k. Továbbá minden j-re definiálok egy $G_j(X) = X^n + a_{n-1,j}X^{n-1} + \cdots + a_{0,j}$ polinomot, és ezen polinom gyökeit jelöljünk $r_{i,j}$-el. Továbbá legyen $\{r_{i_j,j}\}_{j=0}^{\infty}$ egy olyan sorozat, melynél az $i_j \in \{1, 2, \ldots, n\}$, és ezen sorozat elemei legyenek indukciósan megadva, tehát legyen $r_{i_0,0}$ egy tetszőleges gyöke $G_0(X)$-nek. Vegyük a következő szorzatot:

$$\prod_{i=0}^{n-1} |r_{i_j,j} - r_{i,j+1}|_p = |G_{j+1}(r_{i_j,j})|_p = |G_{j+1}(r_{i_j,j}) - G_j(r_{i_j,j})|_p = \tag{3.1}$$

$$= \left| \sum_{i=0}^{n} (a_{i,j+1} - a_{i,j}) r_{i_j,j}^i) \right|_p \leq \max(|a_{i,j+1} - a_{i,j}|_p, |r_{i_j,j}|_p^i) \leq \tag{3.2}$$

$$\leq \max(|a_{i,j+1} - a_{i,j}|_p) \max(1, |r_{i_j,j}|_p^i) \leq \max(|a_{i,j+1} - a_{i,j}|_p) \cdot C, \tag{3.3}$$

ahol $C > 0$ egy megfelelő konstans, amivel minden j-re felülről tudjuk becsülni az $A_j = \max(1, |r_{i_j,j}|_p^i)$-t. Látszik az is, hogy j-ben vett határértéke a $\delta_j = \max(|a_{i,j+1} - a_{i,j}|_p)$-nek 0. Így látszódik, hogy létezik egy olyan i legalább, amire teljesül, hogy

$$|r_{i_j,j} - r_{i,j+1}|_p < \sqrt[n]{\delta_j C}.$$

Ha az $\{r_{i_j,j}\}_{j=0}^{\infty}$ sorozat első j tagját definiáltuk, akkor a sorozat $(j+1)$. tagja legyen $r_{i,j+1}$. Az így definiált $\{r_{i_j,j}\}_{j=0}^{\infty}$ sorozat Cauchy lesz, mivel teljesül a 3.3 egyenlőtlenség. Ez által, ha vesszük ezen $\{r_{i_j,j}\}_{j=0}^{\infty}$ sorozatot, melynek legyen r a határértéke, akkor $P(r) = \lim_{j\to\infty} P(r_{i_j,j}) = \lim_{j\to\infty} G_j(r_{i_j,j}) = 0$. □

Az Ω-n is tudjuk definiálni az értékelési gyűrűt, és ezen gyűrű maximális ideálját, mint ahogy $\mathbb{Q}_p$-n, és $\mathbb{Q}_p$ véges bővítésein is tettük.

3.2.19. Definíció. Legyen $\mathfrak{O}$ értékelési gyűrűje Ω-nak, ahol $\mathfrak{O}$ definiáljuk úgy, mint

$$\mathfrak{O} = \{x \in \Omega : |x|_p \leq 1\}$$

Továbbá legyen $\mathfrak{P}$ maximális ideál $\mathfrak{O}$-ban, ahol $\mathfrak{P}$ definiáljuk úgy, mint

$$\mathfrak{P} = \{x \in \Omega : |x|_p < 1\}$$

3.2.20. Észrevétel. *Ha $x \in \Omega$, akkor előáll $x = p^r\omega(x_1)\{x_1\}$, ahol $x = p^r x_1$, $\omega(x_1)$ egységgyök, és $\{x_1\}$ egységkörbeli elem.*

4. fejezet

Analízis az Ω-n

4.1. Alapfüggvények és a Dwork-lemma

$\mathbb{Q}_p$ felett definiáltunk sok mindent, mely megmarad Ω felett is, továbbá ezen definíciók segítségével bizonyítottunk jó pár állítás, lemmát, tételt és ezen tételek következményeit, így szintúgy mint a definíciók a megfelelő kontextusba helyezéssel közel hasonló gondolatmenettel bizonyíthatóak. Így csak felsoroljuk a fontosabb állításokat, tételeket:

4.1.1. Állítás. *Legyen $\{a_n\}_{n=0}^{\infty}$ Ω-beli sorozat, ami akkor, és csak akkor Cauchy, ha*

$$|a_{n+1} - a_n|_p \to 0.$$

4.1.2. Állítás. $\sum_{n=0}^{\infty} a_n$ *sor akkor, és csak akkor konvergens ha $a_n \to 0$, ahol $\{a_n\}_{n=0}^{\infty} \in \Omega$.*

4.1.3. Állítás. *Legyen $f(X) = \sum_{n=0}^{\infty} a_n X^n$ Ω-beli hatványsor, amely meghatároz egy folytonos függvényt az $r = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|a_n|_p}}$ sugarú nulla középpontú gömbön. Ha $\lim_{n\to\infty} |a_n|_p r^n = 0$, akkor az $f(X)$ kiterjed a $\overline{B(0,r)}$ zárt gömbre.*

4.1.4. Tétel. *Legyen $f(X) = \sum_{n=0}^{\infty} a_n X^n$ Ω-beli hatványsor, mely konvergenciasugara r, akkor tetszőleges $\alpha \in \overline{B(0,r)}$ esetén teljesül, hogy*

$$g(X) = \sum_{n=0}^{\infty} a_n (X-\alpha)^n$$

hatványsor konvergenciasugara r és minden $\beta \in \overline{B(0,r)}$ teljesül, hogy $f(\beta) = g(\beta)$.

4.1.5. Tétel (Unicitás tétele)**.** *Legyenek $f(X) = \sum_{n=0}^{\infty} a_n X^n$ és $g(X) = \sum_{n=0}^{\infty} b_n X^n$ Ω-beli hatványsorok. Ha létezik egy x_n nem-stacionárius sorozat, mely mentén a két hatványsor értékei megegyeznek, akkor $f(X) = g(X)$.*

4.1.6. Állítás. *p-adikus logaritmus függvény legyen a $\log_p : U_1 \to \Omega$ függvény, ahol $U_1 = \{x \in \mathfrak{O} : |x-1|_p < 1\} = B(1,1) = 1+\mathfrak{P}$. A p-adikus logaritmus függvényre teljesül, hogy $\log_p(xy) = \log_p(x)+\log_p(y)$ minden $x, y \in U_1$.*

4.1.7. Állítás. *Legyen p-adikus exponenciális függvény, mely*

$$\exp_p : B\left(0, p^{\frac{-1}{p-1}}\right) \to \Omega,$$

akkor ezen függvény kielégíti a következő egyenletet, hogy $\forall x, y \in B\left(0, p^{\frac{-1}{p-1}}\right)$ $\exp_p(x+y) = \exp_p(x) \cdot \exp_p(y)$.

4.1.8. Állítás. *Legyen* $x \in B\left(0, p^{\frac{-1}{p-1}}\right)$ *tetszőleges, akkor teljesülni fog, hogy*

$$|\exp_p(x) - 1|_p < 1,$$

tehát $\exp_p(x)$ *benne van* $\log_p$ *értelmezési tartományában, és* x*-re igaz, hogy* $\log_p\left(\exp_p(x)\right) = x$*. Legyen továbbá* $x \in B\left(0, p^{\frac{-1}{p-1}}\right)$*, akkor*

$$|\log_p(1+x)|_p < p^{\frac{-1}{p-1}},$$

tehát $\log_p(1+x)$ *eleme* $\exp_p$ *értelmezési tartományának, és* $\exp_p\left(\log_p(1+x)\right) = 1+x$*.*

4.1.9. Állítás. *Legyen* $\alpha \in \mathbb{Z}_p$*, és legyen* $(1+x)^\alpha = B_\alpha(X)$ *binomiális sor, akkor ezen hatványsor konvergens minden* $x \in \mathfrak{P}$*-re.*

A következő lemma a segítségünket fogja szolgálni a p-adikus zeta függvény racionalitásának igazolásában. Ezen lemma Dwork nevéhez fűződik, tehát nagy valószínűséggel az első Weil sejtés igazásakor bizonyította ezen lemmát.

4.1.10. Lemma (Dwork-lemma)**.** *Legyen* $F(X) = \sum_{i=0}^{\infty} a_i X^i \in 1 + X\mathbb{Q}_p[[X]]$*.* $F(X) \in 1 + X\mathbb{Z}_p[[X]]$ *akkor, és csak akkor ha*

$$\frac{F(X^p)}{F(X)^p} \in 1 + X\mathbb{Z}_p[[X]].$$

Bizonyítás. Tegyük fel, hogy $F(X) \in 1 + X\mathbb{Z}_p[[X]]$, mivel tudjuk, hogy tagonként lehet p-adik hatványra emelni és tudjuk a kis-Fermat tételét, így teljesül, hogy $F(X)^p = F(X^p) + pG(X)$, ahol $G(X) \in \mathbb{Z}_p[[X]]$. Továbbá, mivel $\mathbb{Z}_p$ kommutatív gyűrű, így teljesül, hogy

$$1 - \frac{pG(X)}{F(X)^p} = \frac{F(X^p)}{F(X)^p},$$

ahol $\frac{pG(X)}{F(X)^p} \in pX\mathbb{Z}_p[[X]]$, akkor $\frac{F(X^p)}{F(X)^p} \in 1 + X\mathbb{Z}_p$.

A másik irány bizonyítását teljes indukcióval tesszük. Tegyük fel, hogy $F(X^p) = F(X)^p G(X)$, ahol $G(X) = \sum_{i=0}^{\infty} b_i X^i \in 1 + pX\mathbb{Z}_p[[X]]$. Ha $i = 0$, akkor $a_0 = 1$, tehát $i = 0$-ra teljesül az állítás. Továbbá tegyük fel, hogy n-ig teljesül az indukció. Az $(n+1)$. együttható megkapásához a két hatványsort elég az n. tagig nézni, tehát

$$\left(\sum_{i=0}^{n} a_i X^i\right)^p + \sum_{i=0}^{n} \left(a_i b_{\lceil \frac{i}{p} \rceil}\right) X^{i(p+1)},$$

akkor így két esetre módosul, mivel ha $n+1$ osztható p-vel, akkor az $n+1$ együtthatóra teljesül, hogy $a_{\frac{n+1}{p}} + a_{\lceil \frac{n+1}{p+1} \rceil} b_{\lceil \frac{n+1}{p^2+p} \rceil} \in \mathbb{Z}_p + p\mathbb{Z}_p$, tehát $a_{n+1} \in \mathbb{Z}_p$. Különben ha $n+1$ nem osztható p-vel, akkor $a_{n+1} = 0$. □

4.1.11. Következmény. *Legyen*

$$F(X_1, X_2, \ldots, X_n) = \sum_{i_1, i_2, \ldots, i_n}^{\infty} a_{i_1, i_2, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}$$

n *változós* 1 *konstans tagú,* $\mathbb{Q}_p$ *együtthatós hatványsor.* $F(X_1, X_2, \ldots, X_n) \in \mathbb{Z}_p[[X_1, \ldots, X_n]]$ *akkor, és csak akkor ha*

$$\frac{F(X_1^p, X_2^p, \ldots, X_n^p)}{(F(X_1, X_2, \ldots, X_n))^p} \in 1 + pX_1\mathbb{Z}_p[[X_1, \ldots, X_n]] + \cdots + pX_n\mathbb{Z}_p[[X_1, \ldots, X_n]].$$

A következmény bizonyítása megegyezik a Dwork-lemma bizonyításával csak itt n változós a hatványsor. Például $n = 2$ esetén ezen következményt lehet használni a következő hatványsor együtthatóinak $\mathbb{Z}_p$-beliségének eldöntésére.

$$\begin{aligned} F(X,Y) &= B_{X,p}(Y) \cdot \prod_{n=1}^{\infty} B_{\frac{X^{p^n}-X^{p^{n-1}}}{p^n},p}(Y^{p^n}) = \\ &= (1+Y)^X \cdot \prod_{n=1}^{\infty} (1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^n}} = \\ &= \sum_{k=0}^{\infty} \left(\frac{\prod_{l=0}^{k-1}(X-l)}{k!} Y^k \right) \cdot \prod_{n=1}^{\infty} \left(\sum_{k=0}^{\infty} \frac{\prod_{l=0}^{k-1} \left(\frac{X^{p^n}-X^{p^{n-1}}}{p^n} - l \right)}{k!} Y^{kp^n} \right). \end{aligned}$$

Az látszódik, hogy $F(X,Y) \in 1 + X\mathbb{Q}_p[[X,y]] + Y\mathbb{Q}_p[[X,Y]]$, mivel minden X^nY^m tagnak az együtthatói csak véges sok elem szorzataként kaphatók meg, és mivel egy tetszőleges $i \in \mathbb{N}$ esetén

$$B_{\frac{X^{p^i}-X^{p^{i-1}}}{p^i},p}(Y^{p^i})$$

együtthatói $\mathbb{Q}_p$-beliek. Továbbá ha vizsgáljuk a

$$\frac{F(X^p,Y^p)}{(F(X,Y))^p} = \frac{(1+Y^p)^{X^p} \cdot \prod_{n=1}^{\infty}(1+Y^{p^{n+1}})^{\frac{X^{p^{n+1}}-X^{p^n}}{p^n}}}{(1+Y)^{pX} \cdot \prod_{n=1}^{\infty}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}}} = \frac{(1+Y^p)^X}{(1+Y)^{pX}},$$

adódik. Innentől elég csak belátni, hogy $\frac{(1+Y^p)^X}{(1+Y)^{pX}} \in 1 + pX\mathbb{Z}_p[[X,Y]] + pY\mathbb{Z}_p[[X,Y]]$, és mivel $1+Y \in 1 + Y\mathbb{Z}_p[[Y]]$, így az előző következmény miatt

$$\frac{1+Y^p}{(1+Y)^p} = 1 + pY(G(Y)),$$

ahol $G(Y) \in \mathbb{Z}_p[[X]]$. Így adódik, hogy

$$\frac{(1+Y^p)^X}{(1+Y)^{pX}} = (1+pYG(Y))^X = \sum_{n=0}^{\infty} \left(\frac{\prod_{k=0}^{n-1}(X-k)}{n!} (pYG(Y))^k \right),$$

amely eleme az $1 + pX\mathbb{Z}_p[[X,Y]] + pY\mathbb{Z}_p[[X,Y]]$-nak, tehát $F(X,Y) \in Z_p[[X,Y]]$.

4.2. Lineáris leképezések a hatványsorok vektorterén

Az n változós Ω együtthatós hatványsorok gyűrűjét jelöljük R-rel ebben az alfejezetben. R-re továbbá lehet gondolni, mint Ω feletti végtelen dimenziós vektortérként is.

Legyen $G \in R$ hatványsor, akkor egy R feletti lineáris leképezésnek nevezzük a G hatványsorral való szorzást, mint leképezést. R feletti lineáris leképezére egy példa például egy nem negatív q elemmel való szorzás (jelöljük T_q-vel), tehát

$$r = \sum_{u \in U} a_u X^u \longmapsto T_q(r) = \sum_{u \in U} a_{uq} X^u,$$

ahol $U = \{(X_1, \ldots, X_n) \in \mathbb{Z}^n | \quad X_i \geq 0, \forall i\}$. Továbbá még példa: $\Psi_{q,G} = T_q \circ G : R \to R$, ahol

$$G(X) = \sum_{w \in U} g_w X^w, \quad \Psi_{q,G}(X^u) = T_q \left(\sum_{w \in U} g_w X^{w+u} \right) = \sum_{v \in U} g_{qv-u} X^v.$$

4.2.1. Állítás. *Legyen* $G(X) = \sum_{w\in U} g_w X^w$, *és*

$$G_q(X) = G(X^q) = \sum_{w\in U} g_w X^{qw},$$

akkor teljesül, hogy

$$G \circ T_q = T_q \circ G_q = \Psi_{q,Gq}.$$

Bizonyítás. Az egyenlet bal oldalára teljesül, hogy

$$G \circ T_q(X^u) = \sum_{w\in U} g_w X^{w+\frac{u}{q}} = \sum_{w\in U} g_{w-\frac{u}{q}} X^w,$$

az egyenlet jobb oldalára teljesül, hogy

$$\Psi_{q,Gq} = T_q \circ G_q(X^u) = \sum_{w\in U} g_{qw} X^{w+qu} = \sum_{w\in U} g_{w-\frac{u}{q}} X^w,$$

tehát teljesül az egyenlőség. □

4.2.2. Definíció. Legyen $|\cdot| : U \mapsto \mathbb{Z}^\times$ függvény, mely $u \in U$-ra $|u| = \sum_{i=1}^{n} u_i$ teljesül, akkor azon R_0 halmazt, amelyre igaz, hogy

$$R_0 = \left\{ G = \sum_{w\in U} g_w X^w \in R |\ \exists M > 0, \mathrm{ord}_p(g_w) \geq M|w|\ \forall w \in U \right\}$$

túl-konvergált hatványsorok halmazának nevezzük.

4.2.3. Állítás. R_0 *zárt a szorzásra, és azon leképezésre, hogy* $G \mapsto G_q$.

Bizonyítás. A a szorzásra való zártság következik a p-adikus értékelés tulajdonságából. Legyen $G = \sum_{w\in U} g_w X^w$, akkor $G_q = \sum_{w\in U} g_w X^{qw}$ hatványsor lesz. Ha $q \nmid w$, akkor adódik, hogy G_q-beli együtthatója 0, azonban ha $q|w$, akkor

$$\mathrm{ord}_p(g_w) \geq M|w| = M|qw'| = M'|w'|,$$

ahol $w = qw'$ és $M' = M|q|$. Ezen egyenlőtlenséggel beláttuk, hogy minden együtthatójához megfelelő választás M', tehát $G_q \in R_0$. □

4.2.4. Állítás (Dwork Nyom Formula)**.** *Legyen* $G \in R_0$, *és legyen* $\Psi = \Psi_{q,G}$, *akkor* $Tr(\Psi^s)$ *konvergens minden* s*-re, és*

$$(q^s - 1)^n \mathrm{Tr}(\Psi^s) = \sum_{\substack{x\in\Omega^n \\ x^{q^s-1}=1}} \prod_{i=1}^{s-1} G\left(x^{q^i}\right).$$

Tr-rel jelöljük a mátrix nyomát, amelyet tudunk, hogy $\mathrm{Tr}(M) = \sum_{i}^{n} m_{ii}$, ahol $M \in V^{n\times n}$, ha $n = \infty$, akkor ha a sor konvergens, akkor létezik csak a nyom.

Bizonyítás. A bizonyítás s szerinti teljes indukcióval fog menni, így $\Psi(X^u) = \sum_{v\in U} g_{qv-u} X^v$, akkor $\mathrm{Tr}(\Psi) = \sum_{u\in U} g_{(q-1)u}$, amelyről látszik, hogy konvergens, mivel $\Psi \in R_0$.

Továbbá tudjuk azt is, hogy minden $i \in \{1, \ldots, n\}$-re

$$\sum_{\substack{x_i\in\Omega \\ x_i^{q-1}=1}} x_i^{w_i} = \begin{cases} q-1, & q-1|w_i, \\ 0, & \text{különben.} \end{cases}$$

Ez által ha $x = (x_1, \dots, x_n)$-re, akkor adódik, hogy

$$\sum_{\substack{x\in\Omega\\ x^{q-1}=1}} x^w = \prod_{i=0}^{n}\left(\sum_{\substack{x_i\in\Omega\\ x_i^{q-1}=1}} x_i^{w_i}\right) = \begin{cases}(q-1)^n, & q-1|w,\\ 0, & \text{különben.}\end{cases}$$

Az állítás jobb oldalát nézve adódik, hogy

$$\sum_{\substack{x\in\Omega\\ x^{q-1}=1}} x^w = \sum_{w\in U} g_w \sum_{\substack{x\in\Omega\\ x^{q-1}=1}} x^w = (q-1)^n \sum_{u\in U} g_{(q-1)u} = (q-1)^n \mathrm{Tr}(\Psi),$$

amelyből kapjuk az állítást s=1 esetén. Ha $s > 1$, akkor az állítást, abból kapjuk, hogy

$$\begin{aligned}\Psi^s &= T_q \circ G \circ T_q \circ G \circ \Psi^{s-2} = T_q \circ T_q \circ G_q \circ G \circ \Psi^{s-2} = T_{q^2} \circ G \cdot G_q \circ \Psi^{s-2} = \\ &= T_{q^2} \circ T_q \circ (G \cdot G_q)_q \circ G \circ \Psi^{s-3} = T_{q^3} \circ G \cdot G_q \cdot G_{q^2} \circ \Psi^{s-2} = \cdots = \\ &= T_{q^s} \circ \prod_{i=0}^{s-1} G_{q^i} = \Psi_{q^s, \prod_{i=0}^{s-1} G_{q^i}}.\end{aligned}$$

Ezen egyenlőség miatt lehet használni az $s = 1$ esetben használt gondolatmenetet, tehát teljesül a Nyom formula. □

Továbbiakban mátrixfüggvények determinánsának egy tulajdonságát fogjuk belátni, amely arról szól, hogy tetszőleges nagyságú A mátrixhoz, ahol tegyük fel, hogy a mátrixnyoma konvergens sor, akkor

$$\det(1 - AT) = \exp_p\left(-\sum_{s=1}^{\infty} \mathrm{Tr}(A^s)\frac{T^s}{s}\right).$$

Tetszőleges véges mátrixfüggvény esetén tudjuk, hogy

$$\det(1 - AT) = \sum_{i=1}^{n} b_i T^i,$$

ahol

$$b_i = (-1)^i \sum_{\substack{1\le j_1,\dots,j_i\le n\\ \sigma:\text{permutáció}}} \mathrm{sgn}(\sigma) \prod_{l=1}^{i} a_{j_l,\sigma(j_l)}.$$

Továbbá végtelen mátrix esetén is teljesül ezen felírás, mivel tetszőleges n esetén tudjuk, hogy igaz a felírás, ez által b_i-k konvergensek lesznek.

Vegyük most egy konkrét végtelen dimenziós mátrixot, amely legyen az $A = \{g_{qv-u}\}_{u,v=1}^{\infty}$ mátrix, amely az előbb definiált $\Psi_{q,G}$ lineáris leképezés mátrixa. A $\Psi_{q,G} = T_q \circ G$, ahol $G \in R_0$, tehát létezik egy olyan $M > 0$, hogy $\mathrm{ord}_p(g_w) \ge M|w|$. Ez alapján becsüljük b_m nagyságát, hogy tudjunk a konvergenciáról valamit mondani:

$$\begin{aligned}\mathrm{ord}_p(b_m) = \mathrm{ord}_p\left(\prod_{i=1}^{m} g_{q\sigma(u_i)-u_i}\right) &\ge M\left(\prod_{i=1}^{m} |g_{q\sigma(u_i)-u_i}|\right) \ge \\ &\ge M\left(\sum_{i=1}^{n} q|\sigma(u_i) - \sum_{i=1}^{n} |u_i|\right) = M(q-1)\sum_{i=1}^{n} |u_i|.\end{aligned}$$

Ebből látszódik, hogy a $\mathrm{ord}_p(b_m) \to \infty$, ha $m \to \infty$, és ez által a $\det(1 - AT)$ hatványsor jól-definiált, továbbá, mivel $\frac{1}{m} \cdot \mathrm{ord}_p(b_m) \to \infty$, ez által a konvergencia tartománya az egész Ω.

4.2.5. Állítás. *Legyen $A = \{g_{qv-u}\}_{u,v=1}^{\infty}$ mátrix, amely az előbb definiált $\Psi_{q,G}$ lineáris leképezés mátrixa, akkor*

$$\det(1 - AT) = \exp_p\left(-\sum_{s=1}^{\infty} \mathrm{Tr}(A^s)\frac{T^s}{s}\right),$$

és továbbá a konvergenciasugara végtelen és jól-definiált.

Bizonyítás. A jól-definiáltságot, és a végtelen konvergenciasugarat az előbb láttuk. Feltehető, hogy az A mátrixunk felsőháromszögmátrix, mivel tudunk olyan invertálható mátrixot találni, mely nem változtatja meg a mátrix determinánsát, és nyomát se. Ezen mátrixokat hívjuk az A mátrix konjugáltjának. Legyen először A mátrix csak véges $m \times m$-es mátrix, akkor tudjuk, hogy

$$\det(1 - AT) = \prod_{i=1}^{m}(1 - g_{i(q-1)}T).$$

Belátjuk, hogyha kiindulunk a jobboldalból, akkor megkapható a baloldal.

$$\begin{aligned}
\exp_p\left(-\sum_{s=1}^{\infty} \mathrm{Tr}(A^s)\frac{T^s}{s}\right) &= \exp_p\left(-\sum_{s=1}^{\infty}\sum_{i=1}^{m} g_{i(q-1)}^s\frac{T^s}{s}\right) = \\
&= \prod_{i=1}^{m}\exp_p\left(-\sum_{s=1}^{\infty} g_{i(q-1)}^s\frac{T^s}{s}\right) = \\
&= \prod_{i=1}^{m}\exp_p(\log_p\left(1 - g_{i(q-1)}T\right) = \\
&= \prod_{i=1}^{m}(1 - g_{i(q-1)}T).
\end{aligned}$$

Így véges m-re kijött az állítás. Legyen most $m = \infty$.

Azt tudjuk, hogy véges mátrixokra teljesül az állítás, tehát ha definiáljuk az egyenlet jobboldalát minden m-re, akkor kapunk egy sorozatot. Legyen

$$\begin{aligned}
F_m &= \exp_p\left(-\sum_{s=1}^{\infty} \mathrm{Tr}(A_m^s)\frac{T^s}{s}\right) \\
F &= \exp_p\left(-\sum_{s=1}^{\infty} \mathrm{Tr}(A^s)\frac{T^s}{s}\right),
\end{aligned}$$

akkor azt kéne belátni, hogy $F_m \to F$, ha $m \to \infty$. Ez teljesül, mivel tudjuk, hogy a végtelen dimenziós mátrix nyoma és a determinánsa létezik, és továbbá a hatványsor együtthatói megfelelően konvergálnak, mivel minden véges esetben teljesül az egyenlőség. □

Az előző bizonyításból látszik, hogy a

$$\det(1 - AT) = \exp_p\left(-\sum_{s=1}^{\infty} \mathrm{Tr}(A^s)\frac{T^s}{s}\right)$$

egyenlőség tetszőleges mátrix esetén teljesül.

4.3. Ω-beli karakterek felemelései

Legyen F egy testszőleges test, és legyen K az F test egy véges bővítése.

4.3.1. Definíció. Legyen F egy tetszőleges test, és legyen K az F test egy véges bővítése, akkor azon homomorfizmusokat nevezzük K-beli karakternek, amelyek egy G véges csoportból, K multiplikatív csoportjába mennek.

A definícióból és Lagrange tételéből adódik, hogy a G csoport karakterének képe a $K^\times$-beli egységgyökök lesznek.

4.3.2. Definíció. Legyen K test az F test Galois-bővítése, amelyre $G = \mathrm{Gal}(K/F)$. Nyomnak nevezzük azon függvényt, amely tetszőleges $a \in K$-ra teljesül, hogy

$$\mathrm{Tr}_{K/F}(a) = \sum_{\sigma \in G} \sigma(a).$$

A következő esetekben F csak olyan bővítéseire vizsgáljuk a nyomot, amikor a bővítés Galois, így ezért elég volt ilyen alakban kimondani.

Legyen $F = \mathbb{F}_p$, és $K = \mathbb{F}_{p^s}$, ahol $s \in \mathbb{N}$, akkor adódik, hogy $G = \mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$. A Galois-csoportjáról tudjuk azt, hogy az $\mathbb{F}_{p^s}$ test egy nem nulla (a) eleméhez a Galois-csoport egy (σ) eleme hozzárendeli az a egy megfelelő i hatványát. Ez alapján adódik, hogy

$$\mathrm{Tr}_s(a) = \sum_{i=0}^{s-1} a^{p^i}$$

alakban is írható.

4.3.3. Állítás. *Legyen $\epsilon \in \Omega^\times$ p-edik egységgyök, akkor*

$$\begin{aligned} \theta : \mathbb{F}_{p^s} &\to \Omega^\times \\ a &\to \epsilon^{\mathrm{Tr}_s(a)} \end{aligned}$$

a θ egy Ω-beli karakter.

Bizonyítás. Ha belátjuk, hogy teljesül a

$$\mathrm{Tr}_s(a)^p = \mathrm{Tr}_s(a), \text{ és } \quad \mathrm{Tr}_s(a+b) = \mathrm{Tr}_s(a) + \mathrm{Tr}_s(b),$$

akkor ez által adódik, hogy θ egy Ω karakter. Először lássuk be, hogy teljesül $\mathrm{Tr}_s(a)^p$=$\mathrm{Tr}_s(a)$. A tagonkénti szorzás miatt $\mathbb{F}_p$ felett igaz az első állítás, mivel

$$\mathrm{Tr}_s(a)^p = \left(\sum_{i=0}^{s-1} a^{p^i}\right)^p = \sum_{i=0}^{s-1} a^{p^{i+1}} = \sum_{i=0}^{s-1} a^{p^i} = \mathrm{Tr}_s(a).$$

Az előző tulajdonság miatt teljesül a $\mathrm{Tr}_s(a+b) = \mathrm{Tr}_s(a) + \mathrm{Tr}_s(b)$ is, mivel $(a+b)^{p^i} = a^{p^i} + b^{p^i}$. □

Legyen $a \in \mathbb{F}_{p^s}^\times$ tetszőleges elem, és jelöljük az a elem Teichmüller reprezentánsát $\tau_s(a)$, ahol $\tau_s(a)$ eleme a $\mathbb{Q}_p$ (p^s-1) rendű nem-elágazó bővítésének. A p^s. szimmetrikus polinom gyöktényezős alakra bomlása miatt a $K/\mathbb{Q}_p$ Galois-bővítés, tehát a nyom írható úgy, hogy

$$\mathrm{Tr}_{K/\mathbb{Q}_p}(a) = \sum_{\sigma \in G} \sigma(a).$$

Továbbá az is teljesül, hogy

$$\mathrm{Tr}_{K/\mathbb{Q}_p}(a) \equiv \mathrm{Tr}_s(a) \pmod{p\mathcal{O}_K},$$

ebből következik, hogy tetszőleges $\epsilon \in K$ p. egységgyök esetén teljesül, hogy

$$\epsilon^{\mathrm{Tr}_{K/\mathbb{Q}_p}(a)} = \epsilon^{\mathrm{Tr}_s(a)}.$$

A következő feladatunk az, hogy találjuk egy olyan (Θ) függvényt, amely segít a karakterek felemelésében, tehát azt szeretnénk, hogy teljesüljön tetszőleges $a \in \mathbb{F}_{p^s}$-re, hogy

$$\Theta(\tau_s(a)) = \epsilon^{\mathrm{Tr}a}.$$

4.3.4. Állítás. *Legyen ϵ p. egységgyök és legyen $\lambda = \epsilon - 1$. Továbbá legyen $\mathbb{F}_{p^s}$ feletti karakter:*

$$\theta : \mathbb{F}_{p^s} \to \Omega^\times,$$
$$a \to \epsilon^{\mathrm{Tr}_s(a)},$$

akkor

$$\Theta(T) = F(T,\lambda) = B_{T,p}(\lambda) \cdot \prod_{n=1}^{\infty} B_{\frac{T^{p^n} - T^{p^{n-1}}}{p^n},p}(\lambda^{p^n})$$

függvény megfelelő a θ karakter felemelésére Ω-n.

Bizonyítás. Az előző részben láttuk, hogy $F(T,\theta) \in \mathbb{Z}_p[[X,Y]]$. Ezen kétváltozós függvény írható olyan alakba, hogy

$$F(X,Y) = \sum_{n=0}^{\infty} X^n \left(\sum_{m=n}^{\infty} a_{n,m} Y^m \right).$$

A bizonyítás első lépéseként be kellene látni, hogy legalább a $\overline{B\left(0, p^{\frac{-1}{p-1}}\right)}$ konvergens, ehhez meg azt kéne belátni, hogy $a_n = \sum_{m=n}^{\infty} a_{n,m}\lambda^m$ p-adikus értékelése legalább $\frac{n}{p-1}$, ehhez meg elég látni, hogy $\mathrm{ord}_p(\lambda) = \frac{1}{p-1}$.

4.3.5. Lemma. *Ha ϵ p. primitív egységgyök és legyen $\lambda = \epsilon - 1$, akkor* $\mathrm{ord}_p(\lambda) = \frac{1}{p-1}$

Ezen állítás bizonyításához Mustata ((2011)) online elérhető jegyzetének 8.7-es lemmájának bizonyításán fog alapulni.

Bizonyítás. Azt tudjuk, hogy $(\lambda+1)^p = 1$, abból következik, hogy ϵ gyöke a p-edik körosztási polinomnak, tehát

$$\Phi(X) = \sum_{i=0}^{p-1} \binom{p}{i} X^{p-1-i}\text{-nek.}$$

Az ϵ p-edik primitív egységgyök, így a körosztási polinom irreducibilis $\mathbb{Q}_p$ felett, így Φ előáll $\mathbb{Q}_p(\epsilon)$ felett, mint

$$\Phi(X) = \prod_{i=1}^{p-1} (\epsilon^i - x).$$

Ez által

$$|\epsilon - 1|_p = \left| \prod_{i=1}^{p-1} (\epsilon^i - 1) \right|_p^{\frac{1}{p-1}} = |p|_p^{\frac{1}{p-1}} = p^{\frac{1}{p-1}}.$$

□

Így kapjuk, hogy

$$\mathrm{ord}_p(a_n) = \mathrm{ord}_p\left(\sum_{m=n}^{\infty} a_{n,m}\lambda^m \right) \geq \mathrm{ord}_p(\lambda^n) = \frac{n}{p-1}.$$

A bizonyítás következő lépése, hogy belássuk

$$\epsilon^{\mathrm{Tr}_s(a)} = \prod_{i=0}^{s-1} \Theta\left(\tau_s(a)^{p^i}\right).$$

Fejezzük ki az egyenlet jobboldalát:

$$\prod_{i=0}^{s-1} \Theta\left(\tau_s(a)^{p^i}\right) = \prod_{i=0}^{s-1} \left(B_{\tau_s(a)^{p^i},p}(\lambda) \cdot \prod_{n=1}^{\infty} B_{\frac{\tau_s(a)p^{n+i} - \tau_s(a)p^{n-1+i}}{p^n},p}\left(\lambda^{p^n}\right) \right),$$

mivel $\tau_s(a)^{p^s} = \tau_s(a)$, így adódik, hogy

$$\prod_{i=0}^{s-1} \Theta\left(\tau_s(a)^i\right) = (1+\lambda)^{\prod_{i=0}^{s-1} \tau_s(a)^i} = \epsilon^{\mathrm{Tr}_s(a)}.$$

Ez által beláttuk, hogy Θ a θ karakter felemelése az Ω-ra. □

A felemelések, azért fontosak számunkra, mert ha van egy problémánk, amit véges testek felett kellene megoldani, akkor egy felemelés által képesek vagyunk p-adikus testek feletti analízissel megpróbálni megoldani, és így ez által jóval több eszköz áll rendelkezésünkre. Az első Weil sejtés bizonyításakor is Dworknak valami hasonló érvelés miatt juthatott eszébe, hogy a véges testekről térjünk át a p-adikus testek felé, ahol már képesek vagyunk analízist végezni, és ezzel sikerült is bizonyítania a sejtést.

4.4. p-adikus Weierstrass approximációs tétel

A szakasz címében megadott tételhez szükségünk lesz egy jó pár lemmára, hogy képesek legyünk belátni. Ezen lemmák polinomokhoz, hatványsorokhoz definiált poligonokról szólnak. Ezen poligonokat Newton nevéhez szoktuk fűzni. A szakasz Koblitz ((2012)) könyvének 4. fejezetének 3. alfejezete alapján fogjuk vizsgálni a Newton-poligonokat.

4.4.1. Definíció (Polinomhoz tartozó Newton-poligon)**.** Legyen $f(X) = 1 + \sum_{i=1}^{n} a_i X^i$ egy n-ed fokú Ω-beli együtthatós polinom, és legyen $(0,0)$, $(i, \mathrm{ord}_p(a_i))$ minden i-re a sík pontjai, akkor az $f(X)$ polinom Newton-poligonján a sík ezen pontok általi zárt konvex burkának alsó töröttvonalát értjük, ahol az alsó töröttvonal a zárt konvex burok határának azon része, amely az origót és a legutolsó pontot összekötő töröttvonal.

Ezen poligon megalkotását elképzelhetjük, úgy is, hogy vesszük az origóból kiinduló függőleges félegyenest, majd elkezdjük az óra járásával ellentétesen forgatni addig míg rajta nem lesz a félegyenesen egy $(i, \mathrm{ord}_p(a_i))$ pont. Ha ezen egyenesen egyszerre több pont is rajta lesz, akkor a legtávolabbi ponttal kötjük össze az origót. Ez után vegyük azon félegyenest, amelynek a végpontja az előzőleg hozzávett pont és az origó is rajta van, és ezzel a félegyenessel is elvégezzük ugyancsak azt a menetet, mint az elsőnek hozzávett pontnál. Ezt a folyamatot végezzük addig, amíg az n. pontig nem jutunk.

A Newton-poligon csúcsainak azon $(i, \mathrm{ord}_p(a_i))$ pontokat értjük, melyeknél változik a meredekség. A meredekséget meghatározható, ha például legyen (x_1, y_1) és (x_2, y_2) pontok, akkor a meredekség megadható, mint $\frac{y_2 - y_1}{x_2 - x_1}$.

4.4.2. Lemma. *Legyen*

$$f(X) = 1 + \sum_{i=1}^{n} a_i X^i = \left(1 - \frac{X}{\alpha_1}\right) \cdots \left(1 - \frac{X}{\alpha_n}\right)$$

Ω-beli együtthatós polinom, és legyen $\mathrm{ord}_p\left(\frac{1}{\alpha_i}\right) = \lambda_i$ *a gyökök p-adikus értéke, akkor ha létezik egy* λ *meredekségű szakasza az* $f(X)$ *Newton-poligonjának, melynek hossza legyen* h*, akkor létezik egy olyan* i*, melyre teljesül, hogy* λ_i*-hez tartozó hossz* h *és* $\lambda = \lambda_i$*. Másképpen az* $f(X)$ *Newton-poligonjának meredekségei a p-adikus értékelései az* $f(X)$ *gyökeinek reciprokának.*

Bizonyítás. Az általánosság elvesztése nélkül feltehetjük, hogy monoton növekvő sorrendben vannak az λ-k. Továbbá még feltehető, hogy létezik egy olyan i, melyre teljesül, hogy $\lambda_1 = \lambda_2 = \cdots = \lambda_i < \lambda_{i+1}$, tehát azt szeretnénk belátni először $(i, \mathrm{ord}_p(a_i))$ pontot és az origót összekötő szakasz megegyezik a Newton-poligon első szakaszával, tehát az origót és a $(i, i\lambda_1)$ pontot összekötő szakasszal. Ha ezt belátjuk, akkor ezen gondolatmenet mentén végig belátható a Newton-poligon többi szakaszairól is, hogy ezek megegyeznek.

Az $f(X)$ polinom együtthatói megkaphatók, mint az $\frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_n}$ szimmetrikus polinomjaként, így tetszőleges $j \leq i$-re teljesül, hogy a_j értéke legalább $\frac{1}{\alpha_1 \cdots \alpha_j} = \frac{1}{\alpha_1^j}$. Így $(j, \mathrm{ord}_p(a_j))$ megegyezik a

$(j, j\lambda_1)$, vagy $(j, j\lambda_1)$ felette helyezkedik el, mivel i-ig megegyeznek a λ-k értéke. Az előző elmondható úgy is, hogy rajta van az origót és a $(i, i\lambda_1)$-et összekötő szakaszon, vagy felette helyezkedik el. Ez alapján tudjuk, hogy a_i esetén teljesül, hogy $(i, \mathrm{ord}_p(a_i)) = (i, i\lambda_1)$, mivel

$$a_i = \sum_{k_1,k_2,\ldots,k_i=1}^{n} (-1)^i \cdot \left(\prod_{l=1}^{i} \frac{1}{\alpha_{k_l}} \right) \Rightarrow \mathrm{ord}_p(a_i) = \min_{k_1,k_2,\ldots,k_i=1}^{n} \left(\sum_{l=1}^{i} \lambda_{k_l} \right) = i\lambda_1,$$

mivel i-nel nagyobb indexre $\lambda_{i+1} > \lambda_i$. Így tényleg megegyezik a két szakasz. Ezen gondolatot a többi indexre is belátható, mivel legyen $s > i+1$ és teljesüljön, hogy $\lambda_i < \lambda_{i+1} = \lambda_{i+2} = \cdots = \lambda_{s-1} < \lambda_s$, akkor az origót kicserélve $(i, \mathrm{ord}_p(a_i))$-re elvégezhető ugyanezen gondolatmenet. □

A következő feladatunk, hogy a polinomokhoz tartozó Newton-poligonok segítségével definiáljuk a hatványsorokhoz tartozó Newton-poligonokat.

4.4.3. Definíció. Legyen $f(X) = 1 + \sum_{n=1}^{\infty} a_n X^n \in 1 + X\Omega[[X]]$ hatványsor, és legyen $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i$ polinom az n. részletösszege $f(X)$-nek, akkor az $f(X)$ hatványsor Newton-poligonján az $f_n(X)$-ek Newton-poligonjainak határértékét értjük.

Egy hatványsor Newton-poligonjának elkészítésének metódusa megegyezik egy polinomhoz tartozó Newton-poligon elkészítésével. Azonban hatványsor esetben akadhatnak gondok, mint például ha végtelen sok véges hosszú részből áll a Newton-poligon, vagy ha az utolsó szakasz végtelen hosszúságú, vagy csak olyan pontot képes a félegyenesünk forgatás közben tartalmazni, amelynek kisebb az indexe. Az első esetre példa, ha

$$f_1(X) = 1 + \sum_{i=1}^{\infty} p^{i^2} X^i,$$

második esetre például megfelelő az

$$f_2(X) = \sum_{n=0}^{\infty} X^n,$$

az utolsóra meg az

$$f_3(X) = 1 + \sum_{j=1}^{\infty} pX^j$$

hatványsor megfelelő példa.

Egy hatványsor konvergenciájának meghatározásában segítségünkre lesz a következő lemma, amely Newton-poligonok egy tulajdonságát fogja segítségül venni.

4.4.4. Lemma. *Legyen $f(X) = 1 + \sum_{n=1}^{\infty} a_n X^n \in 1 + X\Omega[[X]]$ hatványsor, és legyen b azon legkisebb érték, amely felsőkorlátja az $f(X)$ Newton-poligonjának, tehát minden szakasz meredekségének felsőkorlátja b, akkor $f(X)$ konvergenciasugara p^b.*

Bizonyítás. Az egyenlőség bizonyítását két részre fogjuk bontatni. Először belátjuk, hogyha $|x|_p < p^b$, akkor konvergens a hatványsor, másodszor meg azt látjuk be, hogyha $|x|_p > p^b$, akkor a hatványsor divergens.

Tegyük fel, hogy $|x|_p < p^b$, tehát $\mathrm{ord}_p(x) > -b$. Továbbá tegyük fel, hogy $\mathrm{ord}_p(x) = -b'$, ahol $b' < b$, akkor $\mathrm{ord}_p(a_n x^n) = \mathrm{ord}_p(a_n) - nb'$, ebből adódik, hogy végtelen sok olyan n létezik, melyre teljesül, hogy $\mathrm{ord}_p(a_n) > \mathrm{ord}_p(x^n)$, így $\mathrm{ord}_p(a_n x^n) \to \infty$, tehát $|a_n x^n|_p \to 0$. Így $f(X)$ konvergens.

Tegyük fel, hogy $|x|_p > p^b$, akkor $\mathrm{ord}_p(a_n) < \mathrm{ord}_p(x^n)$ végtelen sok n-re, így $\mathrm{ord}_p(a_n x^n) \to -\infty$, tehát $|a_n x^n|_p \not\to 0$. Így $f(X)$ nem konvergens. □

4.4.5. Észrevétel. *Az előző lemma abban az esetben, hogy $|x|_p = p^b$ nem mond semmit, tehát a konvergenciasugár határán nem tudjuk az $f(X)$ konvergenciáját.*

4.4.6. Észrevétel. *Ha $c \in \Omega$, akkor $f\left(\frac{X}{c}\right)$ Newton-poligonja megkapható, mint $f(X)$ Newtoni poligonjából elhagyjuk az $y = \lambda x$ origóból induló félegyenest, ahol* $\mathrm{ord}_p(c) = \lambda$.

4.4.7. Lemma. *Legyen $f(X) = 1 + \sum_{n=1}^{\infty} a_n X^n \in 1 + X\Omega[[X]]$ hatványsor, melynek Newton-poligonjának első meredeksége legyen λ_1, és legyen $c \in \Omega$ egy olyan érték, melyre teljesül, hogy* $\mathrm{ord}_p(c) = \lambda \leq \lambda_1$. *Továbbá tegyük fel még, hogy $f(X)$ a $\overline{B(0, p^{\lambda})}$ zárt gömbön konvergens.*

Legyen $g(X) = (1 - cX)f(X)$ hatványsor, akkor $g(X)$ Newton-poligonja megkapható, mint $(1 - cX)$ polinom Newton-poligonjához hozzáillesztjük az $f(X)$ Newton-poligonját. Továbbá $f(X)$-nek és $g(X)$-nek a konvergencia tartománya megegyezik.

Bizonyítás. Tegyük fel, hogy $c = 1$, $\lambda = 0$, akkor adódik, ha $g(X) = \sum_{n=1}^{\infty} b_n X^n$, hogy $b_n = a_n - a_{n-1}$ minden $n \geq 1$, és teljesül, hogy

$$\mathrm{ord}_p(b_n) \geq \min(\mathrm{ord}_p(a_n), \mathrm{ord}_p(a_{n-1}))$$

minden $n \geq 1$-re. Ha $(n, \mathrm{ord}_p(a_n))$, és $(n-1, \mathrm{ord}_p(a_{n-1}))$ rajta, vagy felette van az $f(X)$ Newton-poligonjának, akkor ebből következik, hogy $(n, \mathrm{ord}_p(b_n))$ rajta lesz $g(X)$ Newton-poligonján, vagy felette helyeszkedik el. Továbbá ha $(n-1, \mathrm{ord}_p(a_{n-1}))$ csúcsa az $f(X)$ Newton-poligonjának, akkor $(n, \mathrm{ord}_p(b_n))$ csúcsa lesz $g(X)$ Newton-poligonjának, mivel $\mathrm{ord}_p(b_n) = \mathrm{ord}_p(a_{n-1})$. Ebből következik, hogy $f(X)$-nek és $g(X)$-nek a Newton-poligonjai az utolsó szakasz kívételével megegyeznek.

Egy hatványsor Newton-poligonjának utolsó szakasza meghatározza a hatványsor konvergenciasugarát, és ezen állítás megfordítása is igaz, tehát ha a konvergenciasugara adott, akkor az meghatározza a Newton-poligon utolsó szakaszát.

Ha $f(X)$ Newton-poligonjának utolsó szakasza végtelen hosszú, akkor $g(X)$-é is ilyen, mivel teljesül

$$\mathrm{ord}_p(b_n) \geq \min(\mathrm{ord}_p(a_n), \mathrm{ord}_p(a_{n-1}))$$

egyenlőtlenség. Indirekten fogjuk belátni, hogyha $f(X)$ konvergenciasugara $p^{\lambda_f} < \infty$, akkor $g(X)$ konvergenciasugara is p^{λ_f}, tehát tegyük fel, hogy $g(X)$ kovergenciasugara nagyobb, mint $f(X)$-nek. Ez azt jelenti, hogy létezik egy olyan i index, melyre teljesül, hogy $(i+1, \mathrm{ord}_p(a_i))$ pont $g(X)$ Newton-poligonja alatt van, tehát ebből következik, hogy $\mathrm{ord}_p(a_j) = \mathrm{ord}_p(a_i)$ teljesül minden $j > i$-re, mivel $b_{i+1} = a_{i+1} - a_i$ egyenlőség, és az előző egyenlőtlenség is teljesül. Azonban ez ellentmondás, mivel $f(X)$-nek a konvergens az egységgömbön, tehát $g(X)$ konvergenciasugara megegyezik $f(X)$-évél, és a két Newton-poligon a lemmában leírt azonossággal néz ki. A fordított felállás, tehát $f(X)$ konvergenciasugara megegyezik $g(X)$-évél ugyanezen levezetéssel bizonyítható.

Előbb beláttuk konkrét c-re, és λ-ra a lemmát, most meg belátjuk tetszőleges c-re, és λ-ra. Legyen $f_1(X) = f\left(\frac{X}{c}\right)$, akkor így visszatértünk az előző esetre, mivel így $c = 1$, $\lambda = 0$, és a Newton-poligon első szakaszának meredeksége $\lambda_1 - \lambda$. Ez által tovább legyen $g_1(X) = (1 - X)f_1(X)$, és így $g(X) = g_1(cX)$. Ezen felosztában az előbb beláttak miatt teljesül $g_1(X)$-re, és $f_1(X)$-re az állítás, így akkor $f(X)$-re, és $g(X)$-re is teljesül. □

4.4.8. Lemma. *Legyen $f(X) = 1 + \sum_{n=1}^{\infty} a_n X^n \in 1 + X\Omega[[X]]$ hatványsor, melynek Newton-poligonjának első meredeksége legyen λ_1. Tegyük fel, hogy $f(X)$ konvergens a $\overline{B(0, p^{\lambda_1})}$ zárt gömbön, továbbá ha vesszük az origóból induló $\lambda_1 x$ félegyenest, akkor létezik egy olyan i index, melyre teljesül, hogy a félegyenesen rajta van a $(i, \mathrm{ord}_p(a_i))$ pont. Ekkor teljesülni fog, hogy létezik egy olyan $x \in \Omega$, amelyre* $\mathrm{ord}_p(x) = -\lambda_1$, *és $f(x) = 0$.*

Bizonyítás. Ennek a lemmának a bizonyítását is, úgy fogjuk végezni, mint az előzőt, mivel belátjuk, hogy az általános esetet vissza lehet vezetni arra amikor $\lambda_1 = 0$.

Ha $\lambda_1 \neq 0$, akkor ezen esetet visszavezetjük $\lambda_1 = 0$ esetre. Legyen $\alpha \in \Omega$ olyan elem, amelyre igaz, hogy $\mathrm{ord}_p(\alpha) = \lambda_1$, akkor vegyük azon $f_1(X)$ hatványsort, mely legyen egyenlő $f\left(\frac{X}{\alpha}\right)$-val, így már f_1-re $\lambda_1 = 0$. Így ha belátjuk $\lambda_1 = 0$-s esetet, akkor létezik olyan $x = \frac{x_1}{\alpha}$, ahol x_1 $f_1(X)$ megfelelő gyöke. Ekkor x gyöke lesz $f(X)$-nek, és $\mathrm{ord}_p(x) = -\lambda_1$.

Most lássuk be az $\lambda_1 = 0$ esetet. Legyenek minden n-re definiálva $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i$ polinomok. Ha minden n-re $\mathrm{ord}_p(a_n) = 0$, akkor tényleg teljesül az állítás. Másrészt ha $\mathrm{ord}_p(a_n) \geq 0$ minden n-re, és $\mathrm{ord}_p(a_n) \to \infty$, ha $n \to \infty$. Legyen $N \geq 1$ a legnagyobb index, amelyre teljesül, hogy $\mathrm{ord}_p(a_N) = 0$, akkor a 4.4.2 lemma miatt ha $n \geq N$ legfeljebb N darab olyan gyöke van, melyre teljesül, hogy $\mathrm{ord}_p(x_{n,i}) = 0$, ahol $f_n(X)$-nek az i. ilyen gyökére gondolunk. Legyen $x_N = x_{N,1}$, és minden $n \geq N$-re meg x_n legyen azon gyöke $f_n(X)$-nek, melyre teljesül, hogy $|x_{n,i} - x_{n-1}|_p$ minimális. Ezen választások miatt az $\{x_n\}_{n=1}^{\infty}$ sorozat Cauchy tulajdonságú, és mivel Ω teljes, így a határértéke legyen $\hat{x}$, akkor ezen $\hat{x}$ gyöke $f(X)$-nek. Az $\hat{x}$-re, és $\{x_n\}_{n=1}^{\infty}$ sorozatra vonatkozó állítások azért teljesülnek, mivel vegyük $n \geq N$, akkor

$$|f_{n+1}(x_n) - f_n(x_n)|_p = |f_{n+1}(x_n)|_p = \left| \prod_{i=1}^{N} \left(1 - \frac{x_n}{x_{n+1,i}}\right) \right|_p =$$
$$= \prod_{i=1}^{N} |x_{n+1,i} - x_n|_p \geq |x_{n+1} - x_n|_p^N.$$

Így adódik, hogy

$$|x_{n+1} - x_n|_p^N \leq |f_{n+1}(x_n) - f_n(x_n)|_p = |a_{n+1} x_n^{n+1}|_p = |a_{n+1}|_p,$$

így teljesül, hogy $\{x_n\}_{n=1}^{\infty}$ sorozat Cauchy. Továbbá

$$|f(\hat{x})|_p = |f_n(\hat{x}) - f_n(x_n)|_p = |\hat{x} - x_n|_p \cdot \left| \sum_{i=1}^{n} a_i \cdot \frac{\hat{x}^i - x_n^i}{\hat{x} - x_n} \right|_p =$$
$$= |\hat{x} - x_n|_p \cdot \left| \sum_{i=1}^{n} a_i \cdot \left(\sum_{k=1}^{i} \hat{x}^{i-k} x_n^k \right) \right|_p \leq |\hat{x} - x_n|_p,$$

tehát $f(\hat{x}) = \lim_{n\to\infty} f_n(\hat{x}) = 0$. Ezzel beláttuk a lemmát. □

4.4.9. Lemma. *Legyen $f(X) = 1 + \sum_{n=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ hatványsor, mely konvergens és α gyöke. Továbbá legyen*

$$g(X) = 1 + \sum_{n=1}^{\infty} b_i X^i = f(X) \cdot \left(\sum_{n=0}^{\infty} \left(\frac{X}{\alpha} \right)^n \right),$$

akkor $g(X)$ konvergens $\overline{B(0, |\alpha|_p)}$ gömbön.

Bizonyítás. Legyen $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i$ az n. részletösszege $f(X)$-nek, akkor látszik, hogy minden n-re $g(\alpha)$ együtthatója egyenlő, mint

$$b_n = \sum_{i=0}^{n} \frac{a_i}{\alpha^i},$$

tehát $b_n \cdot \alpha^n = f_n(\alpha)$. Ebből adódik, hogy

$$\lim_{n\to\infty} |b_n \alpha^n|_p = \lim_{n\to\infty} |f_n(\alpha)|_p = 0,$$

mivel α gyöke $f(X)$-nek. □

4.4.10. Tétel (p-adikus Weierstrass approximációs tétele)**.** *Legyen $f(X) = 1 + \sum_{n=1}^{\infty} a_n X^n \in 1 + X\Omega[[X]]$, és legyen konvergens a $\overline{B(0, p^{\lambda})}$ zárt egységgömbön. Továbbá $N < \infty$ érték legyen a Newton-poligon összes legfeljebb λ meredekségű szakaszainak függőleges hossza. Másrészt ha az $f(X)$ Newton-poligonjának utolsó szakaszának meredeksége λ, akkor legyen N azon legnagyobb i, melyre teljesül, hogy*

$(i, \mathrm{ord}_p(a_i))$ az utolsó szakaszon van rajta. Ekkor egyértelműen létezik egy olyan $h(X) \in 1 + X\Omega[[X]]$ N-ed fokú polinom, és $g(X) = 1 + \sum_{n=1}^{\infty} b_n X^n$ hatványsor, melyre teljesül, hogy konvergens, és nem nulla a $\overline{B(0, p^\lambda)}$ zárt gömbön. Továbbá még teljesül, hogy $h(X) = f(X) \cdot g(X)$, és ezen $h(X)$ megkapható, mint az $f(X)$ első N együtthatójához tartozó Newton-poligon.

Bizonyítás. A bizonyítás N szerinti indukcióval fog történni, továbbá még feltehető az előző lemmák (4.4.8, 4.4.7) bizonyítása által, hogy $\lambda = 0$.

Így az adódik $N = 0$ esetben, hogy $f(X)$ és $g(X)$ egymás inverzei. Továbbá $\lambda = 0$ miatt feltehető, hogy $f(X)$ együtthatóira teljesül $i \to \infty$ esetén, hogy $\mathrm{ord}_p(a_i) \to \infty$, és minden i-re teljesül, hogy $\mathrm{ord}_p(a_i) > 0$. Így i szerinti teljes indukcióval látszik, hogy $g(X)$ együtthatóira is teljesül, hogyha $f(X)g(X) = 1$, hogy $\mathrm{ord}_p(b_i) > 0$ minden $i > 0$-ra, mivel

$$b_i = \sum_{j=1}^{i} -(b_{i-j}a_j).$$

Legyen $M > 0$ egy olyan elég nagy valós szám, melyhez létezik olyan m, hogy $i \geq m$-re teljesül, hogy $\mathrm{ord}_p(a_i) > M$, és legyen $\epsilon = \min_{j=1}^{m}(\mathrm{ord}_p(a_j))$. A $\mathrm{ord}_p(b_i) \to \infty$ $(i \to \infty)$, ekvivalens azzal, hogy $i > n \cdot m$-re teljesül, hogy

$$\mathrm{ord}_p(b_i) > \min(M, n\epsilon),$$

tehát elég belátni $i > n \cdot m$-re, hogy $\mathrm{ord}_p(b_i) > \min(M, n\epsilon)$ teljesül.

Ezen állítást n szerinti indukcióval fogjuk megtenni. $n = 0$ esetén az állítás egyértelmű, tegyük fel, hogy $(n-1)$-ig teljesül az állítás. Ekkor n esetén vegyünk b_n összegének egy tagját, melyre teljesül, hogy $j > m$, akkor

$$\mathrm{ord}_p(b_{i-j}a_j) \geq \mathrm{ord}_p(a_j) > M,$$

azonban ha $j \leq m$, akkor

$$\mathrm{ord}_p(b_{i-j}a_j) > \epsilon + \min(M, (n-1)\epsilon),$$

így b_n-re teljesül, hogy $\mathrm{ord}_p(b_n) \geq \min(M, n\epsilon)$. Ezzel beláttuk $N = 0$ estén az állítást.

$N \geq 1$ esetén használni fogjuk a 4.4.9, 4.4.8, 4.4.7 lemmákat, továbbá tegyük fel, hogy a N szerinti indukció teljesül $(N-1)$-ig. Legyen az $f(X)$ Newton-poligonjának az első szakaszának meredeksége $\lambda_1 \leq \lambda$, akkor a 4.4.8 lemma miatt létezik egy olyan α gyöke $f(X)$-nek, melyre igaz, hogy $\mathrm{ord}_p(\alpha) = -\lambda_1$. Ez alapján vegyük az $f_1(X)$ hatványsort, mely megkapható, mint

$$f_1(X) = f(X) \cdot \left(\sum_{n=0}^{\infty} \left(\frac{X}{\alpha} \right)^n \right).$$

A 4.4.9 lemma miatt így teljesül, hogy $f_1(X)$ konvergencia tartománya megegyezik $f(X)$ konvergencia tartományával. Azonban $f(X)$ ebből kifejezhető úgy, mint

$$f_1(X) = \frac{f(X)}{1 - \frac{X}{\alpha}} \Rightarrow f(X) = \left(1 - \frac{X}{\alpha}\right) f_1(X),$$

a mértani sor összegképlete miatt. Az $f_1(X)$ Newton-poligonjának az első szakaszának meredeksége λ_1'. Ha $\lambda_1' < \lambda_1$ teljesülne, akkor 4.4.8 lemma miatt létezne egy olyan α' gyöke $f_1(X)$-nek, hogy $\mathrm{ord}_p(\alpha') = -\lambda_1'$. Azonban ez meg ellentmondás, mivel $f(X)$-nek is gyöke kell legyen, de ez nem lehetséges. Így teljesül, hogy $\lambda_1' \geq \lambda_1$. Ez által teljesülnek a 4.4.7 lemma feltételei, így $f(X)$ Newton-poligon megkapható, mint $f_1(X)$ Newton-poligonja kivéve az első szakaszt. Továbbá a 4.4.7 lemma miatt teljesül, hogy $f(X)$ és $f_1(X)$ hatványsoroknak megegyezik a konvergencia tartománya. Ez által és az indukciós feltétel által $f_1(X)$-hez létezik $h_1(X)$ $(N-1)$-ed fokú polinom, melyre teljesül, hogy $\overline{B(0, p^\lambda)}$ zárt gömbön konvergens, és nem nulla ezen a tartományon, továbbá

$$h_1(X) = f_1(X)g(X).$$

Így $\left(1-\frac{X}{\alpha}\right)$-gyel beszorozva az egyenlet mindkét oldalát kapjuk, hogy

$$f(X)g(X) = \left(1-\frac{X}{\alpha}\right)h_1(X),$$

ahol a jobb oldal egy N-ed fokú polinom, melyre teljesülnek már a tétel állításai.

Már csak az egyértelműséget kell belátni. Indirekten fogjuk bebizonyítani az egyértelműséget, tehát legyen $H(X)$, $h(X)$ polinomok melyekre teljesülnek a tétel állításai, és továbbá $G(X)$, $g(X)$ hatványsorok. Ekkor igaz lesz, hogy

$$H(X)g(X) = f(X)G(X)g(X) = h(X)G(X),$$

mivel a két polinom gyökei multiplicitással azonosak, így a két polinom megegyezik, tehát akkor $g(X)$, és $G(X)$ hatványsorok is azonosak, tehát ellentmondásra jutottunk, így teljesül az egyértelműség. □

4.4.11. Következmény. *Az $f(X) \in 1 + X\Omega[[X]]$ hatványsor Newton-poligonjának egy szakaszának hossza $N < \infty$, meredeksége λ, akkor ezen szakaszán pontosan multiplicitással számolva N darab gyök van, melyre teljesül, hogy $\mathrm{ord}_p(x) = -\lambda$.*

4.4.12. Észrevétel. *Ha vesszük egy hatványsor, mely az egész Ω-n konvergens, és nincs gyöke Ω-ban, akkor ezen hatványsor konstans.*

Bizonyítás. Az előző p-adikus Weierstrass approximációs tétel miatt ezen hatványsorhoz tartozó polinom egy konstans polinom, így a hatványsor egy konstans függvény. □

A p-adikus Weierstrass approximációs tétel egy hatványsor gyökeivel kapcsolatban sok segítséget tud adni, és továbbá hatványsorral megadott függvények érdekes tulajdonságaira is rá tud világítani. A Strassmann tétele is például ilyen, mely hatványsor gyökeinek adja meg bizonyos tulajdonságait. Ezen tétel bizonyítása következik az előző approximációs tételből, de lehetséges egyszerű eszközökkel is bizonyítani, most csak az előző tétel következményeként hivatkozunk rá. Az egyszerű bizonyítás megtalálható Gouvea ((2003)) könyvének 5.6-os alfejezetében, ahol 5.6.1-es tétel pont a Strassmann tétele, és a következőkben kimondott következmények is ebben az alfejezetben találhatóak meg.

4.4.13. Tétel (Strassmann tétele)**.** *Legyen $f(X) = \sum_{n=0}^{\infty} a_n X^n$, ahol nem nulla Ω-beli együtthatós hatványsor, és $\lim_{n\to\infty} a_n = 0$, tehát $f(x)$ minden $x \in \mathfrak{O}$-re konvergens. Továbbá legyen $N \in \mathbb{N}$ azon szám, melyre teljesül, hogy $|a_N|_p = \max(|a_n|_p)$ és $|a_n|_p < |a_N|_p$ minden $n > N$, akkor $f : \mathfrak{O} \to \Omega$, mint függvénynek legfeljebb N nullhelye van.*

Bizonyítás. A p-adikus Weierstrass tétel miatt tudjuk, hogy $f(X) \cdot g(X) = h(X)$ egyenlőség teljesül, ahol $h(X)$ egy N-ed fokú polinom, $g(X)$ meg $\mathfrak{O}$-n konvergens hatványsor. Továbbá tudjuk a 4.4.2 lemma miatt, hogy $h(X)$-nek pontosan N darab gyöke van $\mathfrak{O}$-ben. Ez által teljesül Strassmann tétele. □

4.4.14. Következmény. *Legyen $f(X) = \sum_{n=0}^{\infty} a_n X^n$, ahol nem azonosan nulla Ω-beli együtthatós hatványsor, és $\lim_{n\to\infty} a_n = 0$, tehát $f(x)$ minden $x \in \mathfrak{O}$-re konvergens. Továbbá legyen $\alpha_1, \ldots, \alpha_m$ az $f(X)$ gyökei $\mathfrak{O}$-ban, akkor létezik egy olyan $g(X)$ hatványsor, melynek nincs gyöke $\mathfrak{O}$-ban, de nem azonosan nulla $\mathfrak{O}$-ban, és előállítja $f(X)$-et, mint*

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)g(x)$$

Az előző tétel és a 2.3.6 tétel Ω-n kimondott változata, melynek bizonyítása megegyezik az eredetivel, bizonyítja a következményt.

4.4.15. Következmény. *Legyen $f(X) = \sum_{n=0}^{\infty} a_n X^n$, ahol nem nulla Ω-beli együtthatós hatványsor, és legyen konvergens $p^m\mathfrak{P}$-n valamely m-re, akkor $f(X)$-nek véges sok gyöke van $p^m\mathfrak{P}$-ban.*

Ha vesszük a $g(X) = f(p^m X)$ hatványsort, és a Strassmann tételét, akkor ezek bizonyítják ezen következményt.

4.4.16. Következmény. *Legyen* $f(X) = \sum_{n=0}^{\infty} a_n X^n$ *és* $g(X) = \sum_{n=0}^{\infty} b_n X^n$, *melyek legyenek konvergensek egy* $p^m\mathfrak{P}$*-beli gömbön valamely* m*-re. Ha létezik megszámlálhatóan sok* $\alpha \in p^m\mathfrak{P}$, *melyre* $f(\alpha) = g(\alpha)$, *akkor* $a_n = b_n$ *minden* n*-re.*

Az előző következményt ha alkalmazzuk a $h(X) = f(X) - g(X)$ hatványsorra, akkor ebből következik ezen következmény.

4.4.17. Következmény. *Legyen* $f(X) = \sum_{n=0}^{\infty} a_n X^n$, *mely legyen konvergens egy* $p^m\mathfrak{P}$*-beli gömbön valamely* m*-re. Ha mint függvény periódikus, tehát létezik egy olyan* $\pi \in p^m\mathfrak{P}$, *melyre* $f(\pi + x) = f(x)$ *minden* $x \in p^m\mathfrak{P}$*-re, akkor* $f(X)$ *konstans.*

Vegyük az $f(X) - f(0)$ hatványsort, akkor ennek a hatványsornak megszámlálhatóan sok gyöke van ($n\pi$, ahol $n \in \mathbb{Z}$), akkor alkalmazható az előző következmény, amellyel beláttuk ezen következményt is, mivel $f(X) - f(0)$ azonosan 0, tehát $f(X)$ konstans.

4.4.18. Definíció. Egy függvény teljesnek nevezük, ha Ω minden elemére konvergens, és hatványsorba fejtehető.

4.4.19. Következmény. *Legyen* $f(X) = \sum_{n=0}^{\infty} a_n X^n$ *teljes,* Ω *együtthatós hatványsor, akkor* $f(X)$*-nek legfeljebb megszámlálhatóan sok nullhelye van. Továbbá ha nem véges sok nullhelye van, akkor a nullhelyekből álló sorozat* p*-adikus értéke végtelenhez konvergál.*

Ezen következmény, abból látszik, hogyha vesszük minden m-re a $p^{-m}\mathfrak{P}$ halmazokat, akkor ezen halmazokban mindig csak véges sok gyöke van $f(X)$-nek, tehát Ω-n is csak véges sok nullhelye van, mivel

$$\Omega = \cup_{m=0}^{\infty}(p^{-m}\mathfrak{P}).$$

5. fejezet

Dwork tétele

5.1. Borel-tétele

5.1.1. Tétel (Borel-tétele)**.** *Legyen* $F(X) = \sum_{i=0}^{\infty} a_i X^i \in K[[X]]$*, ahol* K *tetszőleges test. Továbbá legyen* $m, s \geq 0$*, és* $A_{s,m}$ *egy olyan mátrix, amely úgy néz ki, hogy*

$$A_{s,m} = \begin{pmatrix} a_s & a_{s+1} & a_{s+2} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & a_{s+3} & \cdots & a_{s+m+1} \\ a_{s+2} & a_{s+3} & a_{s+4} & \cdots & a_{s+m+2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m} \end{pmatrix},$$

és legyen $N_{s,m} = \det(A_{s,m})$*. Ez által* $F(X)$ *hatványsor akkor, és csak akkor áll elő*

$$F(X) = \frac{P(X)}{Q(X)},$$

ahol $P(X), Q(X) \in K[X]$ *polinomok, ha létezik egy olyan* S*,* $m \in \mathbb{N}$*, melyre teljesül, hogy minden* $s \geq S$ *igaz, hogy* $N_{s,m} = 0$*.*

Bizonyítás. Tegyük fel, hogy $F(X)$ előáll, mint két polinom hányadosa, és legyen ezen két polinom $P(X) = \sum_{i=0}^{N} b_i X^i$, és $Q(X) = \sum_{i=0}^{M} c_i X^i$, akkor $F(X) \cdot Q(X) = P(X)$. Ha $i > \max(M, N)$, akkor T^i együtthatója nulla lesz, tehát

$$\sum_{j=0}^{M} a_{i-M+j} c_{M-j} = 0.$$

Legyen $S = \max(1, N - M + 1)$, és $m = M$. Ha $s \geq S$, akkor felírható $2M$ darab egyenlet, hogy

$$\sum_{j=0}^{M} a_{s+j} c_{M-j} = 0.$$

$$\sum_{j=0}^{M} a_{(s+1)+j} c_{M-j} = 0.$$

$$\vdots$$

$$\sum_{j=0}^{M} a_{(s+M)+j} c_{M-j} = 0.$$

Ha c_j-kre változóként gondolunk, akkor ezen egyenletek sora c_j-khez tartozó lineáris egyenletrendszer, melynek a hozzátartozó mátrix $A_{s,M}$. Ez által adódik, hogy $A_{s,M}$ determinánsa 0. A másik irány belátásához s szerinti teljes idukciót használunk. Először m minimalitását kellene belátni tehát, hogy $\det(A_{s,m-1}) \neq 0$, ha $s \geq S$. Ezen állítást indirekten fogjuk belátni.

Tegyük fel, hogy $\det(A_{s,m-1}) = 0$, akkor ez azt jelenti, hogy a mátrix sorai összefüggőek. Jelöljük a mátrix sorait r_i-vel, akkor legyen r_{i_0} azon legelső sor, melynek az együtthatója nem nulla, akkor r_{i_0} kifejezhető, mint

$$r_{i_0} = \alpha_1 r_{i_0+1} + \alpha_2 r_{i_0+2} + \cdots + \alpha_{m-i_0-1} r_{m-1}.$$

Ha a mátrix r_{i_0}. sorát kicseréljük

$$r_{i_0} - (\alpha_1 r_{i_0+1} + \alpha_2 r_{i_0+2} + \cdots + \alpha_{m-i_0-1} r_{m-1})\text{-re},$$

akkor két esetre bomlik az $A_{s,m}$ mátrix a kinézete alapján. A két eset ha $i_0 = 0$ vagy ha $i_0 \neq 0$.

Ha $i_0 \neq 0$, akkor

$$\left(\begin{array}{ccccc} a_s & a_{s+1} & a_{s+2} & \cdots & a_{s+m} \\ \hline a_{s+1} & a_{s+2} & a_{s+3} & \cdots & a_{s+m+1} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{s+i_0-1} & a_{s+i_0} & a_{s+i_0+1} & \cdots & a_{s+i_0+m-1} \\ 0 & 0 & \cdots & 0 & \beta \\ a_{s+i_0+1} & a_{s+i_0+2} & a_{s+i_0+3} & \cdots & a_{s+i_0+m+1} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m} \end{array}\right)$$

ahol $\beta \neq 0$, akkor látszódik, hogy $A_{s+1,m-1}$ részmátrix determinánsa nulla. Ha $i_0 = 0$, akkor

$$\left(\begin{array}{ccccc} 0 & 0 & \cdots & 0 & \beta \\ \hline a_{s+1} & a_{s+2} & a_{s3} & \cdots & a_{s+m} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m} \end{array}\right),$$

mivel tudjuk, hogy $N_{s,m} = 0$, így vagy $\beta = 0$, vagy $\det(A_{s+1,m-1}) = 0$. Ha $\beta = 0$, akkor van olyan $(m-1)\times(m-1)$-es részmátrixa $A_{s,m}$-nek, melynek determinánsa nulla, ez látszik a mátrix alakjából, mivel a következő mátrix jobb felső részmátrixának determinánsa nulla:

$$\left(\begin{array}{c|cccc} 0 & 0 & \cdots & 0 & \beta = 0 \\ a_{s+1} & a_{s+2} & a_{s3} & \cdots & a_{s+m} \\ \vdots & \vdots & \vdots & & \vdots \\ \hline a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m} \end{array}\right).$$

A három esetből mindig adódott egy olyan $(m-1)\times(m-1)$-es részmátrix, melynek a determinánsa 0, és továbbá ez tetszőleges $s' > s \geq S$-re is teljesül az indukciós feltétel miatt, tehát m nem minimális, így ellentmondásra jutottunk.

Így adódik, hogy $N_{s,m-1} \neq 0$ minden $s \geq S$-re és $N_{s,m} = 0$, tehát a mátrix sorai összefüggőek, de ha egyel kevesebb sort veszünk, akkor lineárisan függetlenek. Feltehető, hogy a mátrix sorai közül az utolsónak legyen nem nulla együtthatója. Így ebből következik, hogyha $u = (u_1, \ldots, u_M)$ megoldása a

következő egyenleteknek

$$\sum_{j=0}^{M} a_{s+j}u_{M-j} = 0$$
$$\sum_{j=0}^{M} a_{(s+1)+j}u_{M-j} = 0$$
$$\vdots$$
$$\sum_{j=0}^{M} a_{(s+M-1)+j}u_{M-1-j} = 0,$$

akkor ezen $u = (u_1, \ldots, u_M)$ megoldása a

$$\sum_{j=0}^{M} a_{(s+M)+j}u_{M-j} = 0$$

is, és az indukciós feltevés által minden $s \geq S$-re teljesül, hogy

$$\sum_{j=0}^{M} a_{s+j}u_{M-j} = 0.$$

Ezzel be is láttuk az állítás, mivel

$$\left(\sum_{j=0}^{\infty} a_j X^j\right) \cdot \left(\sum_{j=0}^{m} u_j X^j\right)$$

szorzatként előáll egy legfeljebb $(S+m)$-ed fokú polinom. □

5.2. A zeta-függvény

A rész elején megemlítjük az affin és projektív tér számunkra szükséges tulajdonságait, hogy tudjuk definiálni a zeta-függvényt. Legyen F tetszőleges test, akkor $\mathbb{A}_F^n$-et n dimenziós affin térnek nevezzük, amelynek pontjai rendezett szám n-esek, tehát $(x_1, \ldots, x_n) \in \mathbb{A}_F^n$, ahol $x_i \in F$ minden i-re. Egy n dimenziós affin térben egy hiperfelületet $f(X_1, \ldots, X_n)$ n változós F feletti polinommal adhatjuk meg, úgyhogy

$$H_f = \{(x_1, \ldots, x_n) \in \mathbb{A}_F^n | f(x_1, \ldots, x_n) = 0\}$$

halmaz pontjai az affin hiperfelület.

Geometriából tudjuk, hogy a projektív tér megadható, mint

$$\mathbb{A}_F^{n+1} - \{(0, \ldots, 0)\}$$

halmaz ekvivalenciaosztályainak halmaza, ahol az ekvivalenciareláció, úgy definiáljuk, hogy

$$(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n) \iff \exists \lambda \in F, \quad x_i = \lambda y_i \quad \forall i \in \{0, 1, \ldots, n\}.$$

Továbbá tudjuk azt is, hogy az n dimenziós F feletti projektív tér előáll, mint

$$\mathbb{P}_F^n = \text{"végtelen pont"} \sqcup \left(\sqcup_{i=1}^{n} \mathbb{A}_F^i\right).$$

Legyen $f(X_1, \ldots, X_n)$ n vátozós, d-ed fokú polinom, akkor ezen polinomot, úgy homogenizáljuk, hogy vegyünk egy $\hat{f}[X_0, X_1, \ldots, X_n]$ $n+1$ változós d-ed fokú polinomot, mely úgy áll elő, hogy

$$\hat{f}[X_0, X_1, \ldots, X_n] = X_0^d \cdot f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right),$$

akkor ezen $\hat{f}[X_0, X_1, \ldots, X_n]$ polinomot nevezzük az $f(X_1, \ldots, X_n)$ polinom homogenizáltjának. Ez alapján tudjuk definiálni a projektív terek hiperfelületeit, mivel legyen $f(X_1, \ldots, X_n)$ n-változós polinom, melynek $\hat{f}[X_0, X_1, \ldots, X_n]$ a homogenizáltja, akkor

$$H_{\hat{f}} = \{(x_0, x_1, \ldots, x_n) \in P_F^n | \quad f(x_0, x_1, \ldots, x_n) = 0, \quad \exists i \quad x_i \neq 0\}.$$

Térjünk át arra az esetre, ahol $F = \mathbb{F}_q$, ahol $q = p^s$ valamely $s \geq 1$-re, akkor tetszőleges $f(X_1, \ldots, X_n)$ inhomogén, és $\hat{f}(X_0, X_1, \ldots, X_n)$ homogén polinomhoz tartozó H_f és $H_{\hat{f}}$ hiperfelületek elemszáma véges minden s-re $\mathbb{F}_q$ felett. Továbbá jelőljük ezen pontok számát

$$N_s = \#(H_f(\mathbb{F}_q)) \quad , \quad \hat{N}_s = \#(H_{\hat{f}}(\mathbb{F}_q)).$$

Ez által tudjuk definiálni a zeta-függvényt.

5.2.1. Definíció. Legyen $f(X_1, \ldots, X_n)$ n változós polinom $\mathbb{F}_q$ test felett, és H_f a hozzá tartozó affin hiperfelület, akkor az f polinomhoz tartozó zeta-függvényt a következő hatványsorral definiáljuk:

$$Z(H_f/\mathbb{F}_q, T) = \exp\left(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}\right).$$

5.2.2. Állítás. *A $Z(H_f/\mathbb{F}_q, T)$ hatványsor T^j változó együtthatója legfeljebb q^{nj}.*

Bizonyítás. Az n dimenziós affin térnek $\mathbb{F}_{q^k}$ felett legfeljebb q^{nk}, tehát ez által a N_k is legfeljebb ennyi lehet, így adódik az állítás, mivel

$$\exp\left(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}\right) \leq \exp\left(\sum_{s=1}^{\infty} q^{ns} \frac{T^s}{s}\right) = \exp\left(-\log(1 - q^n T)\right) =$$
$$= \frac{1}{1 - q^n T} = \sum_{s=0}^{\infty} q^{ns} T^s.$$

□

5.2.3. Állítás. *A $Z(H_f/\mathbb{F}_q, T)$ hatványsor együtthatói $\mathbb{Z}$-beliek és a konstans tag 1.*

Bizonyítás. Legyen $P = (x_1, \ldots, x_n)$ eleme $H_f(K)$-nak, ahol K véges bővítése $\mathbb{F}_q$-nek, akkor létezik egy olyan legkisebb s_0, melyre teljesül, hogy mindegyik $x_i \in \mathbb{F}_{q^{s_0}}$. Ha $P \in \mathbb{F}_{q^{s_0}}$, akkor P-nek van s_0 darab különböző konjugáltja, amelyek valamely $\mathbb{F}_{q^s}$-nak ($s < s_0$) elemei. Így ezen $P_1, \ldots, P_{s_0}$ pontok feletti zeta-függvény egyenlő lesz, mint

$$\exp\left(\sum_{j=1}^{\infty} s_0 \frac{T^{js_0}}{js_0}\right) = \exp\left(-\log(1 - T^{s_0})\right) = \frac{1}{1 - T^{s_0}} = \sum_{j=0}^{\infty} T^{js_0}.$$

Az f szerinti zeta-függvény ilyen $\sum_{j=0}^{\infty} T^{js_0}$ hatványsorok végtelen szorzataként áll elő, azonban mivel csak véges sok szorzatából kapható meg egy tetszőleges T^i hatvány ($i \in \mathbb{N}$) együtthatója, akkor ebből következik, hogy $Z(H_f/\mathbb{F}_q, T)$ együtthatói egészek és a konstans tag 1 lesz. □

Ireland and Rosen ((2013)) könyvének 11. fejezete tartalmaz az előző állítás bizonyításának végét egy kicsit különböző, de lényegében azonos elmondását, azért írom le azon bizonyítás befejezését is, mivel abból jobban látszik a Riemann-zeta függvénnyel való azonossága.

Ezen bizonyítás során is szükségünk lesz egy V halmazra, mely n változós polinomok gyökeit tartalmazza egy $\mathbb{F}_q$ test felett, ahol tetszőleges $\alpha \in V$-re teljesül, és legyen F_{q^s} azon legkisebb véges test, amelyre $\alpha_i \in F_{q^s}$.

5.2.4. Definíció. Egy V algebrai halmaz α d-ed ($d|s$) rendű eleméhez tartozó prímosztónak nevezzük azon halmazt, melynek alakja

$$\left\{\alpha^{p^j} | \quad j = 0, 1, \ldots, s-1\right\}.$$

Ezen definíció alapján V algebrai halmazt particionálják a prímosztók halmazai. Továbbá V-re lehet gondolni, mint egy n dimenziós affin tér egy részhalmaza, amelyben az α-k pontok, és ezen α-khoz tudunk definiálni egyedi d-ed rendű $\mathfrak{P}$ prímosztót. Ha a_d-vel jelöljük a V d-ed rendű prímosztóinak számát, akkor adódik, hogy

$$N_s = \sum_{d|s} da_d.$$

N_s-sel jelöljük V halmaz elemszámát $\mathbb{F}_{q^s}$ felett.

5.2.5. Állítás. *V feletti zeta-függvény egyenlő lesz, mint*

$$Z_V(T) = \prod_{\mathfrak{P}} \frac{1}{1-u^{\deg(\mathfrak{P})}}.$$

Bizonyítás. A jobboldal formálásával bizonyítjuk, hogy tényleg ilyen alakú $Z_V(T)$.

$$\prod_{\mathfrak{P}} \frac{1}{1-u^{\deg(\mathfrak{P})}} = \prod_{n=1}^{\infty} \left(\frac{1}{1-T^n}\right)^{a_n},$$

ekkor vesszük a logaritmusát és formálisan deriváljuk, akkor adódik, hogy

$$\frac{1}{T}\sum_{n=1}^{\infty} \frac{na_nT^n}{1-T^n}.$$

Ezen kifejezés látszódik, hogy egyenlő, mint

$$\frac{1}{T}\sum_{m=1}^{\infty}\left(\sum_{d|m} da_d\right)T^m,$$

mivel $\frac{1}{1-T^n}$ mértani sorba fejthető így kapjuk, hogy

$$\frac{1}{T}\sum_{n=1}^{\infty} \frac{na_nT^n}{1-T^n} = \frac{1}{T}\sum_{n=1}^{\infty}\sum_{m=0}^{\infty} na_nT^{nm},$$

továbbá a két szummát felcserélve adódik, hogy

$$\frac{1}{T}\sum_{n=1}^{\infty}\sum_{m=0}^{\infty} na_nT^{nm} = \frac{1}{T}\sum_{m=1}^{\infty}\left(\sum_{d|m} da_d\right)T^m.$$

Behelyettesítve azt, hogy $N_s = \sum_{d|s} da_d$ teljesül, hogy

$$\sum_{m=0}^{\infty} N_mT^{m-1},$$

ha vesszük a formális integrálját, és vesszük az exponenciálját megkapjuk a $Z_V(T)$. □

Az analógia a Riemann-zeta függvénnyel tisztán látszik, ha $T = q^{-s}$ helyettesítünk, mivel

$$Z(q^{-s}) = \prod_{\mathfrak{P}} \frac{1}{1-q^{-sdeg(\mathfrak{P})}} = \prod_{\mathfrak{P}} \frac{1}{1-\left(\frac{1}{N(\mathfrak{P})}\right)^s}.$$

5.2.6. Tétel (Dwork tétele)**.** *Tetszőleges affin hiperfelület feletti zeta-függvény előáll, mint két polinom hányadosa, melynek együtthatói $\mathbb{Q}$-beliek.*

5.2.7. Észrevétel. *Tetszőleges algebrai varietásra is teljesül Dwork tétele.*

Bizonyítás. Legyen tetszőleges m darab polinom

$$f_1(X_1,\dots,X_n), f_2(X_1,\dots,X_n),\dots,f_m(X_1,\dots,X_n)\in\mathbb{F}_p[X_1,\dots,X_n],$$

továbbá legyen ezen algebrai varietáshoz tartozó affin hiperfelület

$$H_{(f_1,\dots,f_i)}(\mathbb{F}_{p^s})=\{(x_1,\dots,x_n)\in\mathbb{A}^n_{\mathbb{F}_{p^s}}|f_1(X_1,\dots,X_n)=0,$$
$$f_2(X_1,\dots,X_n)=0,\dots,f_i(X_1,\dots,X_n)=0\}$$

tetszőleges $i\in\{1,\dots,m\}$-ig, ahol ezen $H_{(f_1,\dots,f_j)}(\mathbb{F}_{p^s})$ halmazra gondolhatunk, mint az i darab polinom közös gyökeinek halmaza. Ez alapján minden $H_{(f_1,\dots,f_i)}(\mathbb{F}_{p^s})$ halmaz pontjainak számát jelöljük

$$N_s^{(f_1,\dots,f_i)}\text{-vel.}$$

Továbbá definiáljuk minden $i\in\{1,\dots,m\}$-re i darab polinom szorzatának gyökeinek halmazát. Legyen

$$N_s^{(f_1,\dots,f_i)}=\#H_{(f_1,\dots,f_i)}(\mathbb{F}_{p^s})=\{(x_1,\dots,x_n)\in\mathbb{A}^n_{\mathbb{F}_{p^s}}|f_1(X_1,\dots,X_n)=0,\dots,f_i(X_1,\dots,X_n)=0).$$

A szitaformula segítségével

$$N_s^{(f_1,\dots,f_m)}=\sum_{i=1}^{m}(-1)^{i+1}\sum_{\substack{J=\{1,2,\dots,m\}\\|J|=i}}N_s^{f_{j_1},\dots,f_{j_1}}.$$

A szitaformulát használva írjuk be zeta-függvénybe ezen dupla szummát, akkor kapjuk, hogy

$$Z(H_{(f_1,\dots,f_m)}/\mathbb{F}_q,T)=\exp\left(\sum_{s=1}^{\infty}N_s^{(f_1,\dots,f_m)}\frac{T^s}{s}\right)=$$
$$=\exp\left(\sum_{s=1}^{\infty}\left(\sum_{i=1}^{m}(-1)^{i+1}\sum_{\substack{J=\{1,2,\dots,m\}\\|J|=i}}N_s^{f_{j_1},\dots,f_{j_1}}\right)\frac{T^s}{s}\right).$$

a véges szummákat a végtelen szummával, és az exponenciális függvénnyel felcserélve kapjuk, hogy

$$Z(H_{(f_1,\dots,f_m)}/\mathbb{F}_q,T)=\dots=\frac{\prod\limits_{\substack{i=1\\i\equiv0(2)}}^{m}\prod\limits_{\substack{J=\{1,2,\dots,m\}\\|J|=i}}\exp\left(N_s^{f_{j_1},\dots,f_{j_1}}\frac{T^s}{s}\right)}{\prod\limits_{\substack{i=1\\i\equiv1(2)}}^{m}\prod\limits_{\substack{J=\{1,2,\dots,m\}\\|J|=i}}\exp\left(N_s^{f_{j_1},\dots,f_{j_1}}\frac{T^s}{s}\right)}.$$

Ebből már következik is az észrevételünk, mivel a dupla szorzat minden tagjára lehet alkalmazni a Dwork tételét, és mivel véges sok racionális együtthatós polinom szorzata is racionális együtthatós polinom, így teljesül az észrevétel. □

Az előző állítás bizonyításánál használt szitaformula segítségével mutatni fogok konkrét függvényekkel megadott hiperfelület feletti zeta-függvényt.

A példánk legyen az $f(X_1,X_2)=X_1X_2(X_1+X_2+1)$ függvény. A $N_s^f=\#H_f(\mathbb{F}_p^s)$ halmaz pontjai a szitaformula miatt megadható, mint

$$N_s^f=N_s^{X_1=0}+N_s^{X_2=0}+N_s^{X_1+X_2+1=0}-$$
$$-\left(N_s^{X_1=0,X_2=0}+N_s^{X_1=0,X_1+X_2+1=0}+N_s^{X_2=0,X_1+X_2+1=0}\right)+$$
$$+N_s^{X_1=0,X_2=0,X_1+X_2+1=0},$$

ez alapján látszódik, hogy $N_s^{X_1=0,X_2=0,X_1+X_2+1=0}=0$ minden s-re. Az

$$N_s^{X_1=0}=p^s,\ N_s^{X_2=0}=p^s$$

minden s-re, mivel az egyik változó fix, a másik meg tetszőleges lehet. A $N_s^{X_1+X_2+1=0}$ szám meg p^s-vel lesz egyenlő minden s-re, mivel tetszőleges $i\in\{1,2,\dots,p^s-1\}$-hez egyértelműen létezik egy i', melyre teljesül, hogy az összegük 1. A $N_s^{X_1=0,X_2=0}=1$, $N_s^{X_1=0,X_1+X_2+1=0}=1$, és $N_s^{X_1=0,X_1+X_2+1=0}=1$ minden s-re, mivel az első esetben csak a $(0,0)$ pont a megfelelő, a másik két esetben meg a $(0,1)$ és az $(1,0)$ pontok. Így a zeta-függvényre adódik, hogy

$$\begin{aligned}
Z(H_f/\mathbb{F}_p,T)&=\exp\left(\sum_{s=1}^{\infty}N_s^f\frac{T^s}{s}\right)=\\
&=\exp\left(\sum_{s=1}^{\infty}(2\cdot p^s+p^s-3)\cdot\frac{T^s}{s}\right)=\\
&=\exp\left(2\cdot\sum_{s=1}^{\infty}\frac{(pT)^s}{s}\right)\cdot\exp\left(\sum_{s=1}^{\infty}\frac{(pT)^s}{s}\right)\cdot\exp\left(-3\cdot\sum_{s=1}^{\infty}\frac{T^s}{s}\right)=\\
&=\exp\left(-2\log(1-pX)\right)\exp\left(-\log(1-pX)\right)\exp\left(3\log(1-X)\right)=\\
&=\frac{(1-X)^3}{(1-pX)^3}.
\end{aligned}$$

5.2.8. Észrevétel. *Dwork tétele teljesül projektív hiperfelület felett is.*

Bizonyítás. Dimenzió szerinti indukcióval bizonyítjuk az észrevételt.

$n=1$ esetén a projektív egyenes felbontható egy affin egyenes, és egy "végtelen pont" disztjunkt uniójára. Ez által $\hat{N}_s^1$ felírható, mint

$$\begin{aligned}
\hat{N}_s^1=\#H_{\hat{f}}(\mathbb{F}_p^s)&=|\{(x_0,x_1)\in\mathbb{P}_F^1|\quad f(x_0,x_1)=0,\quad \exists i\quad x_i\neq 0\}|=\\
&=|\{(x_0,x_1)\in\mathbb{P}_{\mathbb{F}}^1|\quad f(x_0,x_1)=0,\quad x_0\neq 0\}|+\\
&+|\{(x_0,x_1)\in\mathbb{P}_{\mathbb{F}}^1|\quad f(x_0,x_1)=0,\quad x_0=0\}|=N_s^1+N_s^*,
\end{aligned}$$

ahol N_s^1 az egy-dimenziós affin egyenesen lévő pontok számát jelöljük, N_s^* a "végtelen pont"-hoz tartozó pontok. Ez által a zeta-függvény felírható, mint

$$\exp\left(\sum_{s=1}^{\infty}N_s^1\frac{T^s}{s}\right)\cdot\exp\left(\sum_{s=1}^{\infty}N_s^*\frac{T^s}{s}\right),$$

a Dwork-tétel miatt tudjuk, hogy a szorzat első része előáll két racionális együtthatós polinom hányadosaként, a szorzat második tagja $\frac{1}{1-T}$ lesz, mivel $N_s^*=1$. Ezzel $n=1$ esetén teljesül az észrevétel.

Tegyük fel, hogy $(n-1)$-ig teljesül az állítás, akkor

$$\begin{aligned}
\hat{N_s^n}=\#H_{\hat{f}}(\mathbb{F}_p^s)&=|\{(x_0,x_1,\dots,x_n)\in\mathbb{P}_{\mathbb{F}}^n|\ f(x_0,x_1,\dots,x_n)=0,\ \exists i\ x_i\neq 0\}|=\\
&=|\{(x_0,x_1,\dots,x_n)\in\mathbb{P}_{\mathbb{F}}^n|\quad f(x_0,x_1,\dots,x_n)=0,\quad x_0\neq 0\}|+\\
&+|\{(x_0,x_1,\dots,x_n)\in\mathbb{P}_{\mathbb{F}}^n|\quad f(x_0,x_1,\dots,x_n)=0,\quad x_0=0,\ \exists i\ x_i\neq 0\}|=\\
&=N_s^n+\hat{N}_s^{n-1},
\end{aligned}$$

ahol N_s^n-sel jelöljük az n dimenziós affin téren lévő pontokat, és $\hat{N}_s^{n-1}$-nel jelöljük az $(n-1)$ dimenziós projektív téren lévő pontokat. Így az $n=1$ esethez hasonlóan, a zeta-függvény egyenlő lesz, mint

$$\exp\left(\sum_{s=1}^{\infty}N_s^n\frac{T^s}{s}\right)\cdot\exp\left(\sum_{s=1}^{\infty}\hat{N}_s^{n-1}\frac{T^s}{s}\right).$$

Az szorzat első tagja Dwork-tétele miatt lesz két racionális együtthatós polinom hányadosa, a második része meg az indukciós feltevés miatt lesz, ez által teljes indukcióval beláttuk az észrevételt. □

5.2.9. Lemma. *Legyen $g(X) = \frac{h(X)}{f(X)}$, ahol $g(X) \in 1 + X\Omega[[X]]$ hatványsor, melynek az összes együtthatója $\overline{B(0,1)}$-ben van. Ha $h(X) \in 1 + X\Omega[X]$, és $f(X) \in 1 + X\Omega[X]$ polinomok, amelyeknek nincsen közös gyöke, akkor $h(X)$, és $f(X)$ összes együtthatóija $\overline{B(0,1)}$-ben van.*

Bizonyítás. Írjuk át ezt az egyenletet olyan alakra, hogy $f(X)g(X) = h(X)$. Tegyük fel, hogy $f(X)$ valamelyik a_i együtthatójára teljesül, hogy $\mathrm{ord}_p(a_i) < 0$, akkor 4.4.2 lemma miatt létezik egy α gyöke a $\overline{B(0,1)}$-ben, azonban ez ellentmondás, mivel $f(X)$-nek és $h(X)$-nek nincsen közös gyöke. Ezen indirekten feltett gondolatmenet a másik irányra is megfelel így beláttuk, hogy $f(X)$, és $h(X)$ együtthatói $\overline{B(0,1)}$-ben vannak. □

Ezen lemma, azért volt szükséges, hogy bebizonyítsunk egy újabb állítást a zeta-függvényről.

5.2.10. Állítás. *Tetszőleges affin hiperfelület feletti zeta-függvény előáll, mint két polinom hányadosa, melynek együtthatói $\mathbb{Z}$-beliek, és konstans tagjuk* 1.

Bizonyítás. A 5.2.3 állítás miatt tudjuk, hogy a zeta-függvény együtthatói egészek és a konstans tagja 1. A Dwork tétele miatt továbbá tudjuk, hogy a zeta-függvény előáll két racionális együtthatós polinom hányadosaként. Legyen ezen két polinom $f(X)$ és $h(X)$, akkor ezen polinomok közös gyökeikkel egyszerűsítve kaphatunk két olyan $f'(X)$, és $h'(X)$ polinomokat, amelyek gyökei különbözőek. Továbbá $f'(X)$, és $h'(X)$ olyan alakra is hozhatóak, hogy 1 legyen a konstans tagjuk. Ez által alkalmazható az előző lemma, így a zeta-függvény előáll, mint két egész együtthatós, 1 konstans tagú polinom hányadosa. □

A következő állítás Dwork tételére ad egy

5.2.11. Állítás. *Dwork tétele ekvivalens azzal, hogy léteznek olyan algebrai komplex számok*

$$(\alpha_1, \dots, \alpha_t; \beta_1, \dots, \beta_u),$$

ahol az α_t-k az α konjugáltjai, a β_u-k a β konjugáltjai, akkor teljesül, hogy

$$N_s = \sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s.$$

Bizonyítás. $\Longrightarrow$:

Tegyük fel, hogy teljesül Dwork tétele, akkor

$$Z(H_f/\mathbb{F}_q, T) = \frac{P(T)}{Q(T)} = \frac{\prod_{i=1}^{\nu}(1-\lambda_i T)}{\prod_{j=1}^{\gamma}(1-\mu_j T)}.$$

Vegyük mindkét oldal logaritmusát, akkor adódik, hogy

$$\sum_{s=1}^{\infty} N_s \frac{T^s}{s} = \sum_{i=1}^{\nu} \log(1-\lambda_i T) - \sum_{j=1}^{\gamma} \log(1-\mu_j T) =$$
$$= -\sum_{i=1}^{\nu} -\log(1-\lambda_i T) + \sum_{j=1}^{\gamma} -\log(1-\mu_j T).$$

Ez után vegyük a logaritmus hatványsorát, akkor kapjuk a következő egyenlőséget, hogy

$$\sum_{s=1}^{\infty} N_s \frac{T^s}{s} = \cdots = \sum_{j=1}^{\gamma}\sum_{s=1}^{\infty} \mu_j^s \frac{T^s}{s} - \sum_{i=1}^{\nu}\sum_{s=1}^{\infty} \lambda_i^s \frac{T^s}{s} = \sum_{s=1}^{\infty} \left(\sum_{j=1}^{\gamma} \mu_j^s - \sum_{i=1}^{\nu} \lambda_i^s \right) \frac{T^s}{s},$$

és mivel a hatványsor együtthatói meg kell, hogy egyezzenek, így

$$N_s = \sum_{j=1}^{\gamma} \mu_j^s - \sum_{i=1}^{\nu} \lambda_i^s.$$

$\Longleftarrow$: Ekkor tegyük fel, hogy

$$Z(H_f/\mathbb{F}_q, T) = \exp\left(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}\right) = \exp\left(\sum_{s=1}^{\infty}\left(\sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s\right)\frac{T^s}{s}\right).$$

A két véges összeget megcserélve a végtelen összeggel és az exponenciális függvényen kívül véve megkapjuk, hogy

$$Z(H_f/\mathbb{F}_q, T) = \cdots = \frac{\prod_{i=1}^{t} \exp\left(\sum_{s=1}^{\infty} \alpha_i^s \frac{T^s}{s}\right)}{\prod_{j=1}^{u} \exp\left(\sum_{s=1}^{\infty} \beta_j^s \frac{T^s}{s}\right)}.$$

A logaritmus hatványsorát használva kapjuk, hogy

$$Z(H_f/\mathbb{F}_q, T) = \cdots = \frac{\prod_{i=1}^{t} \exp(-\log(1-\alpha_i T))}{\prod_{j=1}^{u} \exp(-\log(1-\beta_j T))} = \frac{\prod_{i=1}^{t} (1-\alpha_i T)}{\prod_{j=1}^{u} (1-\beta_j T)} = \frac{P(T)}{Q(T)},$$

így adódik, hogy a zeta-függvény előáll két racionális együtthatós polinom hányadosaként. □

5.3. p-adikus meromorfizmus

5.3.1. Definíció. Egy tetszőleges $F(X) \in \Omega[[X]]$ hatványsort p-adikusan meromorfnak nevezük, ha előáll két olyan hatványsor hányadosaként, melyek konvergenciasugara végtelen.

A következő lemmában megmutatjuk, hogy tetszőleges hiperfelület felett a zeta-függvény p-adikusan meromorf, amely segítségével belátható Dwork-tétele.

5.3.2. Lemma. *Legyen $f(X_1, X_2, \ldots, X_n) \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ polinom, és legyen $Z(H_f/\mathbb{F}_q; T)$ a H_f hiperfelület feletti zeta-függvény, akkor a zeta-függvény p-adikusan meromorf.*

A következő állítás segítségünkre a lemma bizonyításában.

5.3.3. Állítás. *Legyen $a \in \overline{B(0,1)}$, és X^ω, ahol $X^\Omega = X_0^{\omega_0} \cdots X_n^{\omega_n}$, akkor $\Theta(aX^\omega) \in R_0$.*

Bizonyítás. Azt tudjuk, hogy $\Theta(X) = F(T, \lambda) = \sum_{i=0}^{\infty} \theta_i X^i$, ahol

$$\theta_i = \sum_{j=i}^{\infty} \theta_{i,j} \lambda^j,$$

amelyről tudjuk a 4.3.5 állítás miatt, hogy

$$\operatorname{ord}_p(\theta_i) = \operatorname{ord}_p\left(\sum_{j=i}^{\infty} \theta_{i,j}\lambda^j\right) \geq \min_{j=i}^{\infty}\left(\operatorname{ord}_p(\theta_{i,j}) + \operatorname{ord}_p(\lambda^j)\right) \geq \min_{j=i}^{\infty}\left(\operatorname{ord}_p(\lambda^j)\right) = \frac{i}{p-1}.$$

Ez által teljesül, hogy

$$\operatorname{ord}_p(a^i\theta_i) = i\operatorname{ord}_p(a) + \operatorname{ord}_p(\theta_i) \geq \operatorname{ord}_p(\theta_i) \geq \frac{i}{p-1} = \frac{i|\omega|}{|\omega|(p-1)}.$$

Ha $M = \frac{1}{|\omega|(p-1)}$, akkor adódik, hogy $\Theta(aX^\omega) \in R_0$. □

Bizonyítás. A bizonyítás n szerinti teljes indukcióval fog menni, ahol n a változók száma, akkor $n = 0$ esetén egyértelműen adódik, hogy p-adikusan meromorf, mivel H_f az üres halmaz. Tegyük fel, hogy $(n-1)$-ig teljesül a lemma. Továbbá nem az eredeti függvényre fogjuk direkten belátni, hogy p-adikusan meromorf, hanem felbontjuk két olyan függvény szorzatára, amelyek p-adikusan meromorfak.

A zeta-függvényhez hasonlóan definiáljuk a szorzat egyik tagját. Legyen

$$N'_s = \#H'_f(\mathbb{F}_{q^s}) = \{(x_1, \dots, x_n) \in \mathbb{A}^n_{\mathbb{F}_{q^s}} | f(x_1, \dots, x_n) = 0, \quad \forall x_i \neq 0\},$$

ez által legyen

$$Z'(H_f/\mathbb{F}_q; T) = \exp\left(\sum_{s=0}^{\infty} N'_s \frac{T^s}{s}\right).$$

Ez az eredeti zeta-függvénytől n darab hiperfelület uniójával tér el, tehát így a zeta-függvény felírtható, mint

$$Z(H_f/\mathbb{F}_q; T) = Z'(H'_f/\mathbb{F}_q; T) \cdot \exp\left(\sum_{s=0}^{\infty} (N_s - N'_s) \frac{T^s}{s}\right).$$

Az exponenciális tag azon H_i ($i \in \{1, \dots, n\}$) hiperfelületek uniója, amelyek az

$$f(X_1, \dots, X_n) = 0 \qquad , \text{ és} \qquad X_i = 0$$

által vannak meghatározva. Ez alapján két féle típusa lehet H_i-knek. Az első eset, hogy H_i egy affin $(n-1)$ dimenziós hipersík, vagy a második eset, hogy $(n-2)$ dimenziós affin hiperfelület.

Ha H_i $(n-1)$ dimenziós affin hipersík, akkor

$$Z(H_i/\mathbb{F}_q; T) = \exp\left(\sum_{s=0}^{\infty} q^{s(n-1)} \frac{T^s}{s}\right) = \exp(-\log(1 - q^{n-1}T)) = \frac{1}{1 - q^{n-1}T},$$

tehát a H_i p-adikusan meromorf minden i-re. A második eset p-adikus meromorfizmusa a teljes indukciós feltételből következik.

Az unió meghatározására használjuk a szita-formulát, amely jelen esetben arra módosul, hogy vesszük H_i-khoz tartozó zeta-függvények szorzatát, majd leosztjuk a $H_{i,j}$-knek a szorzatával, ahol $H_{i,j}$-k azon hiperfelületek, amelyeket

$$f(X_1, \dots, X_n) = 0 \qquad , \text{ és} \qquad X_i = X_j = 0$$

határoz meg, majd szorozzuk a hármas szorzatokkal, és így tovább n-ig. Azonban, mivel tudjuk, hogy ezen hányados minden tagja p-adikusan meromorf, így az egész is p-adikusan meromorf, tehát az exponenciális tagról beláttuk, hogy p-adikusan meromorf. Ebből adódik, hogyha belátjuk, hogy $Z'(H'_f/\mathbb{F}_q; T)$ p-adikusan meromorf, akkor az eredeti zeta-függvény is p-adikusan meromorf.

Legyen $s \geq 1$, akkor adódik, hogy

$$\sum_{x \in \mathbb{F}_{q^s}} \epsilon^{\mathrm{Tr}(xu)} = \begin{cases} 0, & \text{ha } u \in \mathbb{F}^{\times}_{q^s}, \\ q^s, & \text{ha } u = 0. \end{cases}$$

Így ha feltesszük, hogy $x \in \mathbb{F}^{\times}_{q^s}$, akkor kapjuk, hogy

$$\sum_{x \in \mathbb{F}^{\times}_{q^s}} \epsilon^{\mathrm{Tr}(xu)} = \begin{cases} -1, & \text{ha } u \in \mathbb{F}^{\times}_{q^s}, \\ q^s - 1, & \text{ha } u = 0. \end{cases}$$

Továbbá még az is adódik, ha $u = f(x_1, \dots, x_n)$, hogy

$$\sum_{\substack{x_i \in \mathbb{F}^{\times}_{q^s}, \\ \forall i \in \{0,1,\dots,n\}}} \epsilon^{\mathrm{Tr}(x_0 f(x_1,\dots,x_n))} = q^s N'_s - (q^s - 1)^n.$$

A bizonyításunkban eljutottunk ahhoz a lépéshez, hogy segítségül vegyük Dwork Nyom Formuláját (4.2.4 állítás), és nyomhoz tartozó Ω-beli karakter előállítását (4.3.4 állítás). Használjuk a Teichmüller felemelést az $X_0 \cdot f(X_1, \dots, X_n) \in \mathbb{F}_{q^s}[X_0, \dots, X_n]$-ra, akkor $X_0 \cdot f(X_1, \dots, X_n)$-hoz megadható egy $F[X_0, \dots, X_n] = \sum_{i=1}^{N} a_i X^{\omega_i}$ Ω-beli polinom, ahol $X^{\omega_i} = X_0^{\omega_{0,i}} \cdots X_n^{\omega_{n,i}}$. Ez által használva 4.3.4 állítást kapjuk, hogy

$$q^s N'_s = (q^s - 1)^n + \sum_{\substack{x_i \in \mathbb{F}_{q^s}^{\times}, \\ x_i^{q^s-1}=1, \\ \forall i \in \{0,1,\dots,n\}}} \prod_{i=1}^{N} \prod_{j=0}^{s-1} \Theta\left(a_i^{q^j} x^{q^j \omega_i}\right).$$

Definiáljuk egy hatványsort úgy, hogy

$$G(X_0, \dots, X_n) = \prod_{i=1}^{N} \prod_{j=0}^{s-1} \Theta\left(a_i^{q^j} X^{q^j \omega_i}\right),$$

és legyen $\Delta(T) = \det(1 - AT)$, ahol A a $\Psi_{q,G}$ lineáris leképezés mátrixa, és

$$\det(1 - AT) = \exp_p\left(-\sum_{s=1}^{\infty} \mathrm{Tr}\left(\Psi_{q,G}^s\right) \frac{T^s}{s}\right).$$

A 5.3.3 állítást használva látszik, hogy $G \in R_0$, mivel a szorzat minden tagja R_0-ban van. Ez által adódik, hogy

$$q^s N'_s = (q^s - 1)^n + (q^s - 1)^{n+1} \mathrm{Tr}\left(\Psi_{q,G}^s\right),$$

a q^s átvéve a másik oldalra kapjuk, hogy

$$N'_s = \sum_{i=0}^{n} \binom{n}{i} (-1)^i q^{s(n-i-1)} + \sum_{i=0}^{n+1} \binom{n+1}{i} (-1)^i q^{s(n-i)} \left(\Psi_{q,G}^s\right).$$

Ezen N'_s-t behelyettesítve a $Z'(H'_f/\mathbb{F}_q; T)$-be kapjuk, hogy

$$\begin{aligned}
Z'(H'_f/\mathbb{F}_q; T) &= \exp_p\left(\sum_{s=0}^{\infty} N'_s \frac{T^s}{s}\right) = \\
&= \left(\prod_{i=0}^{n} \exp_p\left(\sum_{s=1}^{\infty} q^{s(n-i-1)} \frac{T^s}{s}\right)^{\binom{n}{i}(-1)^i}\right) \cdot \\
&\cdot \left(\prod_{i=0}^{n+1} \exp_p\left(\sum_{s=1}^{\infty} q^{s(n-i)} \cdot \mathrm{Tr}\left(\Psi_{q,G}^s\right) \cdot \frac{T^s}{s}\right)^{\binom{n+1}{i}(-1)^i}\right) = \\
&= \left(\prod_{i=0}^{n} \exp_p\left(\log(1 - q^{n-i-1}T)^{\binom{n}{i}(-1)^{i+1}}\right)\right) \cdot \\
&\cdot \left(\prod_{i=0}^{n+1} \Delta\left(q^{n-i}T\right)^{\binom{n+1}{i}(-1)^{i+1}}\right) = \\
&= \left(\prod_{i=0}^{n} \left(1 - q^{n-i-1}T\right)^{\binom{n}{i}(-1)^{i+1}}\right) \cdot \left(\prod_{i=0}^{n} \Delta\left(q^{n-i}T\right)^{\binom{n+1}{i}(-1)^{i+1}}\right).
\end{aligned}$$

Ez által beláttuk, hogy $Z'(H'_f/\mathbb{F}_q; T)$, hogy p-adikusan meromorf, mivel a szorzat minden tagjának konvergenciasugara végtelen, tehát teljes függvény, azért végtelen, mivel teljesül a 4.2.5 állítás. $\square$

5.4. Dwork tételének bizonyítása

Dwork tételét kimondjuk ezen részben is, mivel a bizonyítás előkészületeit az előbb elvégeztük. Ezen részben a legáltalánosabban mondjuk ki Dwork tételét, hogy az előzekben bebizonyított állításokat is használjuk.

5.4.1. Tétel (Dwork általánosan kimondott tétele)**.** *Legyen*

$$f_1 \in \mathbb{F}_q[X_0, \dots, X_n],\ \dots,\ f_n \in \mathbb{F}_q[X_0, \dots, X_n]$$

homogén $(n+1)$ *változós polinomok, akkor ezen homogén polinomok által definiált algebrai varietáshoz tartozó projektív hiperfelület felett definiált zeta-függvény előáll két* 1 *konstans tagú, egész együtthatós polinom hányadosaként.*

A bizonyítás az először kimondott alakra fogjuk belátni, mivel az általánosításokat beláttuk a tétel először kimondása után.

Bizonyítás. A 5.3.2 lemma miatt tudjuk, hogy

$$Z(H_f/\mathbb{F}_q; T) = \frac{\zeta_1(T)}{\zeta_2(T)},$$

ahol $\zeta_1(T)$, és $\zeta_2(T)$ is teljes függvények, tehát a konvergenciasugaruk végtelen. Legyen $R > q^n$ valós szám, amely fixáljuk $R = q^{2n}$-nel, akkor p-adikus Weierstrass tétele miatt (4.4.10 tétel) tudjuk, hogy $\zeta_2(T)$ előll egy $P(T) = 1 + \sum_{i=1}^{N} c_i T^i \in 1 + T\Omega[T]$ polinom, és $\zeta_3(T)$ hátványsor hányadosként, amely $\overline{B(0,R)}$-en konvergens, ez azért tehető fel, mivel ζ_2 teljes függvény, tehát $\overline{B(0,R)}$-en konvergens. Továbbá jelöljük $H(T) = 1 + \sum_{i=1}^{\infty} b_i T^i \in 1 + T\Omega[[T]]$-t $\overline{B(0,R)}$-en konvergens hatványsorként a $\zeta_3(T)$ és $\zeta_1(T)$ szorzatát, akkor ebből adódik, hogy

$$Z(H_f/\mathbb{F}_q; T) \cdot P(T) = H(T).$$

A 5.2.3 állítás miatt tudjuk, hogyha $Z(H_f/\mathbb{F}_q; T) = \sum_{s=0}^{\infty} a_i T^i \in 1+T\mathbb{Z}[[T]]$, és 5.2.2 állítás miatt tudjuk, hogy $|a_i|_p \leq p^{-in}$. A $H(T)$ hatványsor, mivel konvergens $\overline{B(0,R)}$-n, így tudjuk, hogy $|b_i|_p \leq q^{-i2n}$.

A bizonytás folytatásához, és befejezéséhez a Borel-tétel (5.1.1 tétel) feltételeit kéne igazolni. Legyen $m > 2N$ fix, akkor legyen $A_{s,m} = \{a_{i,j}\}_{i,j=0}^{m}$ azon mátrix, ahol s kellően nagy, továbbá legyen a determinánsa $N_{s,m}$.

A $Z(T) \cdot P(T) = H(T)$ egyenlőség miatt, minden $(j+N)$ együttható megadható, úgy mint

$$b_{j+N} = \sum_{i=0}^{N} c_{N-i} a_{N+j-i}.$$

Az $A_{s,m}$ mátrixot egy kicsit módosítjuk úgy, hogy a determinánst ne változtassuk. Először vegyük a mátrix m-edik oszlopát adjuk ehhez hozzá az előző N oszlop lineáris kombinációját a megfelelő c_i együtthatóval, tehát az $(m-i)$ oszlopnak legyen az együtthatója c_i. Ezen gondolatmenetet csináljuk végig az összes oszlopon m-től $(N+1)$-ig. Az előbbi egyenlőség miatt a determinánson nem változtattunk.

Ez a mátrix tehát úgy fog kinézni, hogy

$$A'_{s,m} = \begin{pmatrix} a_s & \cdots & a_{N-1} & b_N & \cdots & b_{s+m} \\ a_{s+1} & \cdots & a_N & b_{N+1} & \cdots & b_{s+m+1} \\ a_{s+2} & \cdots & a_{N+1} & b_{N+2} & \cdots & b_{s+m+2} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{s+m-2} & \cdots & a_{N+m-2} & b_{N+m-2} & \cdots & b_{s+2m-2} \\ a_{s+m-1} & \cdots & a_{N+m-1} & b_{N+m-1} & \cdots & b_{s+2m-1} \\ a_{s+m} & \cdots & a_{N+m} & b_{N+m} & \cdots & b_{s+2m} \end{pmatrix}$$

Azt az egyszerű állítást ismerjük az egész számokról, hogy

$$\prod_{p\in\{2,3,5,\dots\}\cup\{\infty\}} |z|_p = 1,$$

ahol $z \neq 0 \in \mathbb{Z}$, akkor adódik, hogy akkor, és csak akkor lesz $|z|_p \cdot |z|_\infty < 1$, ha $z = 0$. Azt tudjuk, hogy a $N_{s,m} \in \mathbb{Z}$, tehát lássuk be, hogy $|N_{s,m}|_p \cdot |N_{s,m}|_\infty < 1$. Először lássuk be, hogy $|N_{s,m}|_p \leq q^{-sn(m+2)}$, mivel $a_i \in \mathbb{Z}$, így $|a_i|_p < 1$, tehát

$$|N_{s,m}|_p \leq \max_{j\geq s+m} (|b_j|_p) < R^{-s(m+1-N)},$$

és, mivel $R = q^{2n}$, és $m > 2N$, akkor kapjuk az állítást, hogy

$$|N_{s,m}|_p \leq R^{-s(m+1-N)} = q^{2n-s(m+1-N)} < q^{-sn(2m-m+2)} = q^{-sn(m+2)}.$$

Vizsgáljuk az $|N_{s,m}|_\infty$ értékét, mivel tudjuk, hogy $A_{s,m}$ minden eleme legfeljebb $q^{n(s+2m)}$ nagyságú, így adódik $|N_{s,m}|_\infty$-re, hogy

$$|N_{s,m}|_\infty = \left| \sum_{\sigma:\text{permutáció}} \operatorname{sgn}(\sigma) \prod_{i=0}^{m} a_{i,\sigma(i)} \right|_\infty \leq (m+1)! q^{n(s+2m)(m+1)} = \\ = (m+1)! q^{2nm(m+1)} q^{ns(m+1)}.$$

Ebből adódik, hogy

$$|N_{s,m}|_p \cdot |N_{s,m}|_\infty < \left(q^{-sn(m+2)}\right) \cdot \left((m+1)! q^{2nm(m+1)} q^{ns(m+1)}\right) = \\ = (m+1)! \cdot \frac{q^{2nm(m+1)}}{q^{sn}},$$

ha s-et kellően nagynak választottuk meg az elején, akkor ebből adódik, hogy

$$(m+1)! \cdot \frac{q^{2nm(m+1)}}{q^{sn}} < 1,$$

tehát $N_{s,m} = 0$. Így a Borel-tétel miatt adódik, hogy $Z(H_f/\mathbb{F}_q; T)$ előáll két racionális együtthatós polinom hányadosaként, tehát beláttuk az első Weil-sejtést. □

Irodalomjegyzék

F. Gouvea. *p-adic Numbers: An Introduction*. Universitext. Springer Berlin Heidelberg, 2003.

I. Herstein. *TOPICS IN ALGEBRA, 2ND ED*. Wiley India Pvt. Limited, 2006.

K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer New York, 2013.

N. M. Katz and J. Tate. Bernard dwork (1923-1998), 1998. Notices of the AMS, volume 46 no. 3, Elérhető: `http://www.ams.org/notices/199903/mem-dwork.pdf?fbclid=IwAR1UsoiqSTjhDS6DGT7_D2EakcVfyXakllGAucv0lvc0oTNw2pdQZhcPBAg`.

E. Kiss. *Bevezetés az algebrába*. Elméleti matematika. Typotex, 2007.

N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Graduate Texts in Mathematics. Springer New York, 2012.

M. Mustata. Zeta functions in algebraic geometry, 2011. Elérhető: `http://www-personal.umich.edu/mmustata/zetabook.pdf`.

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

J. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 1995.

G. Zábrádi. Algebrai számelmélet, 2020. Elérhető: `https://zabradi.web.elte.hu/Jegyzetek/algszamjegyzet.pdf`.

NYILATKOZAT

Név: ANDERLIK CSABA

ELTE Természettudományi Kar, szak: Matematika BSc-matematikus szakirány

NEPTUN azonosító: NOK1EJ

Szakdolgozat címe:

Az első Weil-sejtés Dwork-féle bizonyítása.

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2022.05.26

Anderlik Csaba

a hallgató aláírása