NYILATKOZAT

Név: Gáspár Attila

ELTE Természettudományi Kar, szak: matematika

NEPTUN azonosító: ZX7NAM

Szakdolgozat címe:
p-adikus Lie-csoportok

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, 2021.05.29.

Gáspár Attila

a hallgató aláírása

Eötvös Loránd Tudományegyetem
Természettudományi Kar

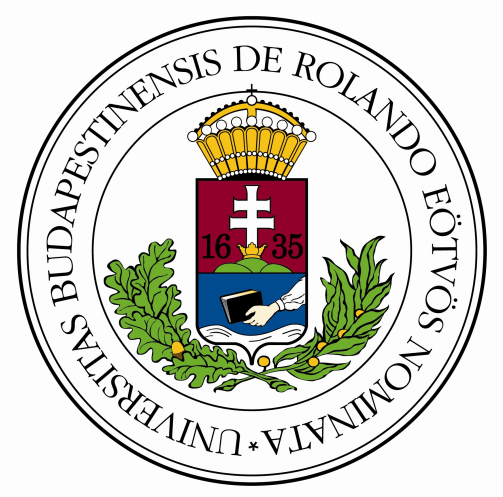
---

p-adikus Lie-csoportok

Gáspár Attila

Témavezető:
Zábrádi Gergely, egyetemi docens

BSc Szakdolgozat
Algebra és Számelmélet Tanszék



Budapest, 2021.

Tartalomjegyzék

Bevezetés

A p-adikus Lie-csoportoknak számos alkalmazása van a számelméletben. Például a Langlands-programban központi szerepe van a p-adikus Lie-csoportok reprezentációelméletének, a téma alapjai megtalálhatóak az [1]-ben. A p-adikus Lie-csoportok elméletében kulcsfontosságúak a pro-p-csoportok, amik a véges p-csoportok provéges megfelelői. A provéges csoportok a testbővítések elméletben is megjelennek: egy végtelen Galois-bővítés Galois-csoportja provéges ([5]). A pro-p-csoportoknak egy másik fontos alkalmazása a véges p-csoportokra vonatkozó „coclass conjecture" bizonyítása: Leedham-Green ([3]) és Shalev ([6]) egymástól függetlenül, a pro-p-csoportok elméletét felhasználva igazolta a sejtést.

A dolgozat a [2] alapján készült. A [4] egy másik, hasonló megközelítése a témának.

Az első fejezetben bemutatom a p-adikus számokat, valamint a p-adikus analízis alapjait, különösen a hatványsorok elméletét. Bár a [2] olyan hatványsorokkal is foglalkozik, ahol a változók nem felcserélhetőek, itt csak a felcserélhető változójú hatványsorokra lesz szükség.

A második fejezetben először a provéges, illetve a pro-p-csoportok tulajdonságairól lesz szó. Ezután bevezetem a hatványteljes pro-p-csoport fogalmát, ami a p-adikus Lie-csoportok mellett a véges rangú pro-p-csoportok jellemzésére is alkalmas ([2], §3.2). A hatványteljes csoportoknak fontos speciális esetei az egyenletes pro-p-csoportok, amiket a 3.3. szakaszban definiált csoportalgebrához fogunk felhasználni.

A harmadik fejezet elején a p-adikus analitikus sokaságokat, valamint a p-adikus Lie-csoportokat definiálom, felhasználva a hatványsorok elméletét. Ezután bizonyítom a dolgozat fő tételét, miszerint egy topologikus csoport pontosan akkor p-adikus Lie-csoport, ha tartalmaz nyílt, egyenletes pro-p-csoportot.

1. Normált gyűrűk

1.1. Teljessé tétel

1.1.1. Definíció. Legyen R egységelemes gyűrű. A $\|\cdot\| : R \to \mathbb{R}_{\geq 0}$ függvény *norma*, ha kielégíti az alábbi feltételeket:

- $\|x\| = 0$ pontosan akkor, ha $x = 0$;
- $\|1\| = 1$, és szubmultiplikatív, azaz $\|xy\| \leq \|x\|\|y\|$;
- teljesül az *ultrametrikus egyenlőtlenség*: $\|x \pm y\| \leq \max\{\|x\|, \|y\|\}$.

Az $(R, \|\cdot\|)$ párt *normált gyűrűnek* nevezzük.

Könnyen ellenőrizhető, hogy egy normált gyűrűben $\|-x\| = \|x\|$ és $\|x_1 + \cdots + x_n\| \leq \max\{\|x_1\|, \ldots, \|x_n\|\}$. Az ultrametrikus egyenlőtlenségből nyilvánvalóan következik a háromszög-egyenlőtlenség, ezért a $d(x, y) = \|x - y\|$ képlettel egy metrikát kapunk R-en.

1.1.2. Lemma. *Normált gyűrűben a Cauchy-sorozatok zártak az elemenkénti összeadásra, szorzásra és ellentettképzésre.*

Bizonyítás. Az ellentettképzésre triviális az állítás.

Legyen (x_n) és (y_n) két Cauchy-sorozat, és legyen $\varepsilon > 0$ tetszőleges. Ha n és m elég nagy, akkor $\|x_n - x_m\| < \varepsilon$ és $\|y_n - y_m\| < \varepsilon$. Ekkor

$$\|(x_n + y_n) - (x_m + y_m)\| = \|(x_n - x_m) + (y_n - y_m)\| \leq \max\{\|x_n - x_m\|, \|y_n - y_m\|\} < \varepsilon,$$

tehát az $(x_n + y_n)$ sorozat Cauchy.

A Cauchy-sorozatok korlátosak, ezért van olyan $K > 0$, hogy $\|x_n\|, \|y_n\| \leq K$ minden n-re. Emiatt

$$\|x_n y_n - x_m y_m\| = \|x_n(y_n - y_m) + (x_n - x_m)y_m\| \leq$$
$$\leq \max\{\|x_n\|\|y_n - y_m\|, \|x_n - x_m\|\|y_m\|\} \leq K \max\{\|y_n - y_m\|, \|x_n - x_m\|\}.$$

Ha n és m elég nagy, akkor $\max\{\|y_n - y_m\|, \|x_n - x_m\|\} < \frac{\varepsilon}{K}$, amiből $\|x_n y_n - x_m y_m\| < \varepsilon$. Tehát az $(x_n y_n)$ is Cauchy-sorozat. □

1.1.3. Állítás. *Normált gyűrűben az összeadás, szorzás, ellentettképzés és a norma folytonosak.*

Bizonyítás. Az $R \times R$ M_1-tér, ezért elég az összeadás sorozatfolytonosságát igazolni. Tegyük fel, hogy $x_n \to x$ és $y_n \to y$. Legyen (x'_n) az a sorozat, amit úgy kapunk, hogy (x_n) minden eleme után beszúrjuk az x-et, ekkor nyilván $x'_n \to x$. Az (y'_n)-et hasonlóan definiáljuk. Az 1.1.2. lemma szerint az $(x'_n + y'_n)$ sorozat Cauchy-sorozat. Minden második eleme $x + y$, ezért az $x + y$-hoz konvergál. Emiatt $x_n + y_n \to x + y$, tehát az összeadás folytonos.

A szorzás és ellentettképzés folytonossága hasonlóan látható. A norma folytonossága pedig következik a metrika folytonosságából, mert $\|x\| = d(x, 0)$. □

1.1.4. Definíció. Az R normált gyűrű *teljes*, ha teljes metrikus tér, vagyis minden R-beli Cauchy-sorozat konvergens.

1.1.5. Definíció. Az $\hat{R}$ teljes normált gyűrű az R normált gyűrű *teljessé tétele*, ha $R \leq \hat{R}$ sűrű részgyűrű.

1.1.6. Állítás. *Bármely R normált gyűrűhöz létezik $\hat{R}$.*

Bizonyítás. Legyen C az R-beli álló Cauchy-sorozatok halmaza. A $\varphi : R \to C, \varphi(x) = (x, x, \dots)$ injektív leképezés. Az 1.1.2. lemma miatt C az elemenkénti műveletekkel C egységelemes gyűrű. Legyen $(x_n) \in C$-re $\|(x_n)\| = \lim_{n\to\infty} \|x_n\|$ (ez Cauchy-sorozat $\mathbb{R}$-ben, mert a háromszög-egyenlőtlenségből $\big|\|x_n\| - \|x_m\|\big| \leq \|x_n - x_m\|$). A norma folytonosságából látható, hogy C-ben a normált gyűrű axiómái az $\|x\| = 0 \Rightarrow x = 0$ kivételével teljesülnek (tehát a $\|\cdot\|$ úgynevezett *félnorma*).

Legyen $N = \big\{ x \in C \;\big|\; \|x\| = 0 \big\}$. Ellenőrizhető, hogy a szubmultiplikativitás és a háromszög-egyenlőtlenség következtében $N \lhd C$, és a $\|\cdot\|$ konstans N mellékosztályain. Emiatt az $\hat{R} = C/N$-en jóldefiniált a $\|\cdot\|$, így az $(\hat{R}, \|\cdot\|)$ normált gyűrű. $\varphi(R) \cap N = 0$, ezért a φ által indukált $\tilde{\varphi} : R \to \hat{R}$ normatartó beágyazás. Tetszőleges $(x_n) \in C$-re ellenőrizhető, hogy $\lim_{k\to\infty} \|\varphi(x_k) - (x_n)\| = 0$. Ebből következik, hogy $\hat{R}$ minden eleme előáll $\tilde{\varphi}(x_n)$ alakú elemek határértékeként, tehát $\tilde{\varphi}(R)$ sűrű $\hat{R}$-ban.

Már csak azt kell ellenőriznünk, hogy $\hat{R}$ teljes. Legyen $(x_n)_{n\geq 1} = \big((x_{n,m})_{m\geq 1}\big)_{n\geq 1}$ egy C-beli elemekből álló Cauchy-sorozat a félnorma szerint. Tetszőleges $n > 0$-ra válasszunk olyan $y_n \in R$-et, amelyre $\|x_n - \varphi(y_n)\| \leq \frac{1}{n}$. Világos, hogy a $\varphi(y_n)$-ek Cauchy-sorozatot alkotnak, ezért φ normatartása miatt $(y_n) \in C$. Ekkor

$$\begin{aligned}
\lim_{k\to\infty} \|x_k - (y_n)\| &= \lim_{k\to\infty} \lim_{n\to\infty} \|x_{k,n} - y_n\| = \\
&= \lim_{k\to\infty} \lim_{n\to\infty} \lim_{m\to\infty} \max\big\{ \|x_{k,n} - x_{k,m}\|, \|x_{k,m} - x_{n,m}\|, \|x_{n,m} - y_n\| \big\} = \\
&= \max\Big\{ \lim_{k\to\infty} \lim_{n,m\to\infty} \|x_{k,n} - x_{k,m}\|, \lim_{k,n\to\infty} \|x_k - x_n\|, \lim_{n\to\infty} \|x_n - \varphi(y_n)\| \Big\} = \\
&= 0.
\end{aligned}$$

A határértékek létezése onnan látható, hogy egy Cauchy-sorozat elemenkénti normái konvergálnak. Ezzel beláttuk, hogy $x_k \to (y_n)$, amiből triviálisan következik $\hat{R}$ teljessége. □

1.1.7. Állítás. *Legyen $f : R \to S$ folytonos homomorfizmus az R és S normált gyűrűk között. Ekkor f egyértelműen kiterjed egy $\hat{f} : \hat{R} \to \hat{S}$ folytonos homomorfizmussá.*

Bizonyítás. Először megmutatjuk, hogy ha (x_n) Cauchy-sorozat R-ben, akkor $(f(x_n))$ is Cauchy-sorozat. Legyen $\varepsilon > 0$ tetszőleges. f folytonos a 0-ban, így van olyan $\delta > 0$, hogy ha $\|x\| < \delta$, akkor $\|f(x)\| < \varepsilon$. Ha n és k elég nagy, akkor $\|x_n - x_k\| < \delta$, ezért $\|f(x_n) - f(x_k)\| = \|f(x_n - x_k)\| < \varepsilon$, vagyis az $(f(x_n))$ Cauchy-sorozat.

Legyen $x \in \hat{R}$ tetszőleges. Ha $x_n \in R$, $x_n \to x$, és $\hat{f}$ létezik, akkor $\hat{f}(x) = \lim_{n\to\infty} f(x_n)$, amiből az egyértelműség világos. Most belátjuk, hogy az előző képlettel definiált $\hat{f}$ jó lesz. Ha $x_n \to x$, akkor $(f(x_n))$ Cauchy-sorozat, ezért konvergens $\hat{S}$-ban. Ha $x_n \to x$ és $y_n \to x$, akkor a két sorozat összefésülésével kapott (z_n) sorozat is x-hez tart. Ekkor $f(z_n)$ konvergens, emiatt $\lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} f(y_n)$, tehát $\hat{f}(x)$ nem függ a sorozat választásától.

Legyen $x, y \in \hat{R}$ tetszőleges. Ekkor választható $x_n, y_n \in R$, amelyre $x_n \to x$ és $y_n \to y$. Az összeadás folytonossága miatt

$$\hat{f}(x) + \hat{f}(y) = \lim_{n\to\infty} f(x_n) + \lim_{n\to\infty} f(y_n) = \lim_{n\to\infty} (f(x_n) + f(y_n)) = \lim_{n\to\infty} f(x_n + y_n) = \hat{f}(x + y).$$

Hasonlóan látható, hogy $\hat{f}$ szorzattartó, ezért homomorfizmus.

Legyen $\varepsilon > 0$ tetszőleges. Az f folytonossága miatt van olyan $\delta > 0$, hogy $\|x\| < \varepsilon$, ha $x \in R$ és $\|x\| < \delta$. Tegyük fel, hogy $x, y \in \hat{R}$, és $\|x - y\| < \delta$. Válasszunk R-ben olyan (x_n) és (y_m) sorozatot, amelyre $x_n \to x$ és $y_m \to y$. $f(x_n) \to \hat{f}(x)$, ezért ha n elég nagy, akkor $\|x_n - x\| < \delta$ és $\|f(x_n) - \hat{f}(x)\| < \varepsilon$. Hasonlóan található olyan m, amelyre $\|y_m - y\| < \delta$ és $\|f(y_m) - \hat{f}(y)\| < \varepsilon$. Ekkor az ultrametrikus egyenlőtlenség miatt $\|x_n - y_m\| < \delta$, így $\|f(x_n) - f(y_m)\| < \varepsilon$. Az ultrametrikus egyenlőtlenséget ismét alkalmazva adódik, hogy $\|\hat{f}(x) - \hat{f}(y)\| < \varepsilon$. Ezzel megmutattuk $\hat{f}$ folytonosságát. □

1.1.8. Következmény. *A teljessé tétel egyértelmű: ha $\hat{R}_1$ és $\hat{R}_2$ két teljessé tétele R-nek, akkor van köztük olyan normatartó izomorfizmus, ami R-re megszorítva az identitás.*

Bizonyítás. Legyen $f : R \to R$ az identitás. Az 1.1.7. állítás miatt f kiterjed egy $\hat{f} : \hat{R}_1 \to \hat{R}_2$ folytonos homomorfizmussá. f^{-1} hasonlóan kiterjed egy $\hat{R}_2 \to \hat{R}_1$ folytonos homomorfizmussá. Az $\widehat{f^{-1}} \circ \hat{f}$ olyan folytonos endomorfizmusa $\hat{R}_1$-nek, ami az identitás R-en, így az egyértelműség miatt maga is az identitás. Ebből következik, hogy $\hat{f}$ izomorfizmus. $\hat{f}$ normatartó R-en, így a norma folytonossága miatt az $\hat{R}_1$-en is. □

Megjegyzés. Az egyértelműségből következik, hogy $\widehat{\mathrm{id}} = \mathrm{id}$, illetve $\widehat{f \circ g} = \hat{f} \circ \hat{g}$, tehát a teljessé tétel a normált gyűrűk kategóriájának egy endofunktora.

1.2. Sorok

Legyen R normált gyűrű. A sorösszeget a $\sum_{i=0}^{\infty} a_i = \lim_{n\to\infty} \sum_{i=0}^{n} a_i$ képlettel definiáljuk, ha $a_i \in R$ minden i-re.

1.2.1. Állítás. *Ha $\sum_{i=0}^{\infty} a_i$ konvergens, akkor $\lim_{i\to\infty} a_i = 0$. Ha R teljes, akkor a fordított irány is igaz: a $\lim_{i\to\infty} a_i = 0$ feltételből következik a $\sum_{i=0}^{\infty} a_i$ konvergenciája.*

Bizonyítás. Legyen $s_n = \sum_{i=0}^{n} a_i$. Tegyük fel, hogy $s_n \to s = \sum_{i=0}^{\infty} a_i$. Ekkor

$$a_i = s_{i+1} - s_i \to s - s = 0,$$

ha $i \to \infty$.

Ha $\lim_{i\to\infty} a_i = 0$, akkor tetszőleges $\varepsilon > 0$ esetén elég nagy n-re $\|a_i\| \le \varepsilon$. Ha n elég nagy, és $n < m$, akkor az ultrametrikus egyenlőtlenség miatt

$$\|s_m - s_n\| = \left\| \sum_{i=n+1}^{m} a_i \right\| \le \max_{n<i\le m} \|a_i\| \le \varepsilon.$$

Ezzel beláttuk, hogy (s_n) Cauchy-sorozat. A konvergenciája R teljességből következik. □

1.2.2. Állítás. *Legyen π egy permutációja $\mathbb{N} = \{0, 1, 2, \dots\}$-nek. Ha $\sum_{i=0}^{\infty} a_i$ konvergens, akkor $\sum_{i=0}^{\infty} a_{\pi(i)}$ is konvergens, és a két sorösszeg megegyezik.*

Bizonyítás. $\lim_{i\to\infty} a_i$ pontosan akkor, ha minden $\varepsilon > 0$-ra véges sok i kivételével $\|a_i\| \le \varepsilon$. Ebből világos, hogy a határértéket a permutálás nem befolyásolja. Emiatt az 1.2.1. állításból adódik a $\sum_{i=0}^{\infty} a_{\pi(i)}$ konvergenciája.

Vezessük be az $s_n = \sum_{i=0}^{n} a_i$ és $t_m = \sum_{j=0}^{m} a_{\pi(j)}$ jelöléseket, illetve legyen $s = \lim_{n\to\infty} s_n$ és $t = \lim_{m\to\infty} t_m$. Legyen $\varepsilon > 0$, és legyen n olyan nagy, hogy ha $i > n$, akkor $\|s_i - s\| \le \varepsilon$. Ebből következik, hogy

$$\|a_i\| = \|(s_{i+1} - s) - (s_i - s)\| \le \varepsilon$$

minden $i > n$-re. Legyen $m \ge \max_{0\le i\le n} \pi^{-1}(i)$ olyan nagy, hogy $\|t_m - t\| \le \varepsilon$. Látható, hogy

$$t_m - s_n = \sum_{j=0}^{m} a_{\pi(j)} - \sum_{i=0}^{n} a_i = \sum_{j=0}^{m} a_{\pi(j)} - \sum_{\substack{0\le j\le m \\ \pi(j)\le n}} a_{\pi(j)} = \sum_{\substack{0\le j\le m \\ \pi(j)>n}} a_{\pi(j)},$$

emiatt $\|t_m - s_n\| \le \varepsilon$. Ebből következik, hogy

$$\|t - s\| = \|(t - t_m) - (s - s_n) + (t_m - s_n)\| \le \varepsilon.$$

ε tetszőleges volt, ezért $s = t$, vagyis a két sorösszeg megegyezik. □

Ha $I = \{i_0, i_1, \dots\}$ megszámlálhatóan végtelen halmaz, akkor bevezethetjük a $\sum_{i\in I} a_i = \sum_{j=0}^{\infty} a_{i_j}$ jelölést. Az előző állítás szerint a soroknál nem számít a tagok sorrendje, így a $\sum_{i\in I} a_i$ értéke nem függ az I elemeinek felsorolásától. Hasonlóan jelöljük $\lim_{i\in I} a_i$-vel a $\lim_{j\to\infty} a_{i_j}$-t, ez szintén független a felsorolásától.

1.2.3. Állítás. *Legyen I megszámlálható. Ha $\sum_{i\in I} a_i$ konvergens, akkor*

$$\left\| \sum_{i\in I} a_i \right\| \le \sup_{i\in I} \|a_i\|.$$

Bizonyítás. Véges I esetén az ultrametrikus egyenlőtlenségből triviális.

Ha I végtelen, akkor elég $I=\mathbb{N}$-re bizonyítani. Az 1.2.1. állítás miatt a jobb oldal véges. Legyen $s_n = \sum_{i=0}^{n} a_i$, az ultrametrikus egyenlőtlenség miatt

$$\|s_n\| \le \max_{0\le i\le n} \|a_i\| \le \sup_{i\in\mathbb{N}} \|a_i\|.$$

A norma folytonossága miatt

$$\left\|\sum_{i=0}^{\infty} a_i\right\| = \left\|\lim_{n\to\infty} s_n\right\| = \lim_{n\to\infty} \|s_n\| \le \sup_{i\in\mathbb{N}} \|a_i\|.$$

□

1.2.4. Állítás. *Tegyük fel, hogy R teljes, és $\sum_{i\in I} a_i$ konvergens. Legyen $(I_j)_{j\in J}$ egy partíciója I-nek (a J megszámlálható halmaz). Ekkor*

$$\sum_{i\in I} a_i = \sum_{j\in J} \sum_{i\in I_j} a_i.$$

Bizonyítás. Ha I véges, akkor véges sok j kivételével I_j üres, ezért az állítás triviális.

Ha I végtelen, akkor az 1.2.1. állításból adódik, hogy az $s_j = \sum_{i\in I_j} a_i$ minden j-re konvergens. Legyen $\varepsilon > 0$ tetszőleges, és legyen $I' = \{i \in I \mid \|a_i\| > \varepsilon\}$, ez egy véges halmaz. Ekkor

$$\sum_{i\in I} a_i = \sum_{i\in I'} a_i + \sum_{i\in I\setminus I'} a_i,$$

mert az I-nek van olyan felsorolása, aminek az I' az elején van. Az 1.2.3. állítás miatt $\left\|\sum_{i\in I\setminus I'} a_i\right\| \le \varepsilon$, vagyis $\left\|\sum_{i\in I} a_i - \sum_{i\in I'} a_i\right\| \le \varepsilon$. Legyen $I'_j = I_j \cap I'$ és $s'_j = \sum_{i\in I'_j} a_i$. Hasonlóan látható, hogy $\|s_j - s'_j\| \le \varepsilon$. Véges sok j kivételével $s'_j = 0$, ekkor $\|s_j\| \le \varepsilon$. Az ε tetszőleges volt, ezért $\lim_{j\in J} s_j = 0$, így az 1.2.1. állításból következik a $\sum_{j\in J} s_j$ konvergenciája. Emiatt a $\sum_{j\in J}(s_j - s'_j)$ is konvergens. Az összeadás folytonosságából látható, hogy

$$\sum_{j\in J} s_j = \sum_{j\in J} s'_j + \sum_{j\in J} (s_j - s'_j),$$

így az 1.2.3. állítás következtében $\left\|\sum_{j\in J} s_j - \sum_{j\in J} s'_j\right\| \le \varepsilon$. Mivel $\sum_{i\in I'} a_i = \sum_{j\in J} s'_j$, az ultrametrikus egyenlőtlenség miatt $\left\|\sum_{i\in I} a_i - \sum_{j\in J} s_j\right\| \le \varepsilon$. Az ε tetszőleges volt, tehát $\sum_{i\in I} a_i = \sum_{j\in J} s_j$. □

1.2.5. Következmény. *Ha R teljes és $\lim_{(i,j)\in I\times J} a_{i,j} = 0$, akkor*

$$\sum_{i\in I} \sum_{j\in J} a_{i,j} = \sum_{j\in J} \sum_{i\in I} a_{i,j}.$$

1.2.6. Állítás. *Ha $\sum_{i\in I} a_i$ és $\sum_{j\in J} b_j$ konvergens, akkor*

$$\sum_{(i,j)\in I\times J} a_i b_j = \left(\sum_{i\in I} a_i\right)\left(\sum_{j\in J} b_j\right).$$

Bizonyítás. Világos, hogy elég $\hat{R}$-ban bizonyítani az állítást. Először az 1.2.1. állítást felhasználva ellenőrizzük, hogy a $\sum_{(i,j)\in I\times J} a_i b_j$ konvergens. $a_i \to 0$ és $b_j \to 0$, ezért $\|a_i\| \le K$ és $\|b_i\| \le L$ valamilyen $K, L > 0$-ra. Véges sok i kivételével $\|a_i\| \le \frac{\varepsilon}{L}$, így $\|a_i b_j\| \le \|a_i\|\|b_j\| \le \varepsilon$. Hasonlóan, véges sok j kivételével $\|b_j\| \le \frac{\varepsilon}{K}$, emiatt $\|a_i b_j\| \le \varepsilon$. Tehát véges sok (i,j) kivételével $\|a_i b_j\| \le \varepsilon$, amiből következik a konvergencia.

Az 1.2.4. állítás, illetve a szorzás folytonossága miatt

$$\sum_{(i,j)\in I\times J} a_i b_j = \sum_{i\in I}\sum_{j\in J} a_i b_j = \sum_{i\in I} a_i \left(\sum_{j\in J} b_j\right) = \left(\sum_{i\in I} a_i\right)\left(\sum_{j\in J} b_j\right).$$

□

1.2.7. Állítás. *Legyen R teljes. Tegyük fel, hogy $(x_{i,n})_{n\in\mathbb{N}}$ konvergens minden $i\in\mathbb{N}$-re. Ha van olyan (g_i) sorozat $\mathbb{R}$-ben, amelyre $\lim_{i\to\infty} g_i = 0$, és $\|x_{i,n}\| \le g_i$ minden i,n-re, akkor*

$$\lim_{n\to\infty}\sum_{i=0}^{\infty} x_{i,n} = \sum_{i=0}^{\infty}\lim_{n\to\infty} x_{i,n}.$$

Bizonyítás. Legyen $x_i = \lim_{n\to\infty} x_{i,n}$. A norma folytonossága miatt $\|x_i\| \le g_i$ minden i-re. Így az 1.2.1. állítás miatt az összes sor konvergens. Tetszőleges $\varepsilon > 0$-ra van olyan m, hogy $g_i \le \varepsilon$ minden $i > m$-re. Az 1.2.3. állítás miatt

$$\left\|\sum_{i=0}^{\infty} x_i - \sum_{i=0}^{\infty} x_{i,n}\right\| = \left\|\sum_{i=0}^{\infty}(x_i - x_{i,n})\right\| \le \sup_i \|x_i - x_{i,n}\| \le \max\left\{\varepsilon, \max_{i\le m}\|x_i - x_{i,n}\|\right\} = \varepsilon,$$

ha n olyan nagy, hogy $\|x_i - x_{i,n}\| \le \varepsilon$ minden $i \le m$-re. Az ε tetszőleges volt, ezért $\sum_{i=0}^{\infty} x_{i,n} \to \sum_{i=0}^{\infty} x_i$, amivel az állítást igazoltuk. □

1.3. p-adikus számok

1.3.1. Definíció. Legyen p prím. Egy $q \ne 0$ racionális szám felírható $q = p^n \cdot \frac{a}{b}$ alakban, ahol $a, b \in \mathbb{Z}$, $p \nmid a, b$. Ekkor az n egyértelmű. Definiáljuk a *p-adikus abszolút értékét* a

$$|q|_p = p^{-n}$$

képlettel, illetve legyen $|0|_p = 0$.

Látható, hogy a $(\mathbb{Z}, |\cdot|_p)$, illetve a $(\mathbb{Q}, |\cdot|_p)$ normált gyűrűk. Világos, hogy p-adikus abszolút érték nemcsak szubmultiplikatív, hanem *multiplikatív* is, azaz $|xy|_p = |x|_p|y|_p$ bármely $x, y \in \mathbb{Q}_p$-re.

1.3.2. Definíció. A *p-adikus egészek* gyűrűje a $(\mathbb{Z}, |\cdot|_p)$ teljessé tétele, amit $\mathbb{Z}_p$-vel jelölünk. Hasonlóan definiáljuk a $\mathbb{Q}_p$ gyűrűt a $(\mathbb{Q}, |\cdot|_p)$ teljessé tételeként.

A $\mathbb{Z}$ és $\mathbb{Q}$ kommutatív gyűrűk, ezért a szorzás folytonosságából következik, hogy a $\mathbb{Z}_p$ és $\mathbb{Q}_p$ is kommutatívak. Hasonlóan látható, hogy a norma multiplikativitása $\mathbb{Z}_p$-n és $\mathbb{Q}_p$-n is teljesül.

1.3.3. Állítás. *A $\mathbb{Z}_p$ kompakt.*

Bizonyítás. $\mathbb{Z}_p$ teljes metrikus tér, ezért csak azt kell ellenőrizni, hogy teljesen korlátos. A $p^k\mathbb{Z}$ mellékosztályai a $\mathbb{Z}$-nek p^k darab p^{-k} sugarú zárt gömbbel való fedését alkotják. $\mathbb{Z}$ sűrű $\mathbb{Z}_p$-ben, ezért ezek a gömbök $\mathbb{Z}_p$-t is fedik, emiatt készen vagyunk. □

1.3.4. Állítás. *Legyen $n \ge 0$. Ekkor a $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ természetes homomorfizmus egyértelműen kiterjed egy $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ folytonos homomorfizmussá (a $\mathbb{Z}/p^n\mathbb{Z}$-n a diszkrét topológiát vesszük).*

Bizonyítás. Legyen $x \in \mathbb{Z}/p^n\mathbb{Z}$-re $\|x\| = 1$, ha $x \ne 0$, különben legyen $\|x\| = 0$. Ellenőrizhető, hogy ez valóban norma, és a diszkrét topológiát indukálja. Így az 1.1.7. állítás miatt elég lenne azt megmutatni, hogy a $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ faktorleképezés folytonos. x és y képe akkor és csak akkor egyezik meg, ha $p^n \mid x - y$, ami ekvivalens azzal, hogy $|x-y|_p \le p^{-n}$. Emiatt $\mathbb{Z}/p^n\mathbb{Z}$ bármely elemének ősképe egy p^{-n} sugarú zárt gömb. A végesség miatt bármely halmaz őse zárt, tehát a faktorleképezés folytonos. □

A $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ leképezést $x \bmod p^n$-nel fogjuk jelölni. Látható, hogy a magja $\overline{p^k\mathbb{Z}}$, ami a kompaktság miatt $p^k\mathbb{Z}_p$.

1.3.5. Állítás. *Minden $x \in \mathbb{Z}_p$ egyértelműen előáll*

$$x = \sum_{k=0}^{\infty} a_k p^k$$

alakban, ahol $0 \le a_k < p$ egész.

Bizonyítás. Ha $x\in\mathbb{N}$, akkor az állítás nyilvánvaló a p-s számrendszerbeli alak létezéséből és egyértelműségéből, és világos, hogy az $x \bmod p^{k+1}$ meghatározza a_k-t. A p-adikus topológia szerint $\mathbb{N}$ sűrű $\mathbb{Z}$-ben, mert minden modulo p^k maradékosztály tartalmaz nemnegatív elemet. Ebből következik, hogy $\mathbb{N}$ sűrű a $\mathbb{Z}_p$-ben is. Így minden $x\in\mathbb{Z}_p$-hez van olyan (x_n) sorozat $\mathbb{N}$-ben, amelyre $x_n\to x$. Legyen $x_n=\sum_{k=0}^{\infty} a_{n,k}p^k$, ahol $0\le a_{n,k}<p$. A konvergencia miatt tetszőleges k-ra az $x_n \bmod p^{k+1}$ valahonnan kezdve konstans, ezért van olyan a_k, hogy elég nagy n-re $a_{n,k}=a_k$. $|a_{n,k}p^k|_p\le p^{-k}$, így az 1.2.7. állítás miatt

$$x=\lim_{n\to\infty} x_n=\lim_{n\to\infty}\sum_{k=0}^{\infty} a_{n,k}p^k=\sum_{k=0}^{\infty}\lim_{n\to\infty} a_{n,k}p^k=\sum_{k=0}^{\infty} a_kp^k.$$

Az egyértelműséghez elég azt igazolni, hogy ha $\sum_{k=0}^{\infty} a_kp^k=0$, akkor $a_k=0$ minden k-ra. Tegyük fel, hogy van olyan minimális n, amelyre $a_n\neq 0$. Ekkor $0<a_n<p$, ezért $|a_np^n|_p=p^{-n}$. Az 1.2.3. állítás miatt

$$p^{-n}=|a_np^n|_p=\left|\sum_{k=n+1}^{\infty} a_kp^k\right|_p\le\sup_{k>n}|a_kp^k|_p\le p^{-n-1},$$

ami ellentmondás. □

1.3.6. Állítás. *A $\mathbb{Z}_p$-ben pontosan a $\mathbb{Z}_p\setminus p\mathbb{Z}_p$ elemei invertálhatóak.*

Bizonyítás. Nyilvánvaló, hogy a $p\mathbb{Z}_p$ elemei nem invertálhatóak, mert az $x \bmod p$ magjában vannak.

Legyen $x\notin p\mathbb{Z}_p$. Ekkor $A_k=\{y\in\mathbb{Z}_p\mid xy\equiv 1 \pmod{p^k}\}\neq\emptyset$. A műveletek folytonossága miatt A_k zárt, és $A_1\supseteq A_2\supseteq\dots$, így a kompaktság miatt a metszetük tartalmaz valamilyen $y\in\mathbb{Z}_p$-t. Ekkor $xy-1$ benne van a $\bigcap_{k=1}^{\infty} p^k\mathbb{Z}_p$-ben, ezért a normája legfeljebb p^{-k} minden k-ra, tehát $xy-1=0$. □

1.3.7. Állítás. *Minden $x\in\mathbb{Q}_p\setminus\{0\}$ egyértelműen előáll $x=p^ny$ alakban, ahol n egész, és $y\in\mathbb{Z}_p\setminus p\mathbb{Z}_p$. Ekkor teljesül, hogy $|x|_p=p^{-n}$.*

Bizonyítás. Először az egyértelműséget ellenőrizzük. Ha $y\in\mathbb{Z}_p\setminus p\mathbb{Z}_p$, akkor invertálható $\mathbb{Z}_p$-ben.

$$|y|_p\ge|y|_p|y^{-1}|_p=|1|_p=1,$$

emiatt $|y|_p=1$. Ebből következik, hogy $|p^ny|_p=p^{-n}$, így az n egyértelmű. Ha $p^ny_1=p^ny_2$, akkor $\mathbb{Q}_p$-ben p^{-n}-nel szorozhatunk, ezért $y_1=y_2$.

Ha $\|x\|=p^{-n}$, akkor a norma folytonossága miatt van olyan $(\frac{a_k}{b_k})_{k\ge1}$ sorozat $\mathbb{Q}$-ban, amelyre $a_k,b_k\in\mathbb{Z}\setminus p\mathbb{Z}$, és $p^n\cdot\frac{a_k}{b_k}\to x$. Ekkor $b_k\notin p\mathbb{Z}_p$, ezért invertálható $\mathbb{Z}_p$-ben, így $\frac{a_k}{b_k}\in\mathbb{Z}_p$. Az a_k is invertálható $\mathbb{Z}_p$-ben, ezért $\frac{a_k}{b_k}\in\mathbb{Z}_p\setminus p\mathbb{Z}_p$. A szorzás folytonossága miatt $\frac{a_k}{b_k}\to p^{-n}x$, tehát $y=p^{-n}x\in\mathbb{Z}_p\setminus p\mathbb{Z}_p$. □

1.3.8. Következmény. *Tetszőleges $n\in\mathbb{Z}$-re $\mathbb{Q}_p$-ben a legfeljebb p^{-n} abszolút értékű elemek pontosan a $p^n\mathbb{Z}_p$ elemei.*

Mivel $p^ny\cdot p^{-n}y^{-1}=1$, a $\mathbb{Q}_p$ test. Emiatt a *p-adikus számok testének* nevezzük.

1.4. Hatványsorok

Legyen $\mathbf{x}\in\mathbb{Q}_p^r$ és $\alpha\in\mathbb{N}^r$. Vezessük be az

$$\mathbf{x}^\alpha=x_1^{\alpha_1}\cdots x_r^{\alpha_r},$$

az $\langle\alpha\rangle=\alpha_1+\dots+\alpha_r$, illetve az $\|\mathbf{x}\|=\max_i|x_i|_p$ jelölést. Ellenőrizhető, hogy $|\mathbf{x}^\alpha|_p\le\|\mathbf{x}\|^{\langle\alpha\rangle}$.

1.4.1. Definíció. $\mathbb{Q}_p$ feletti r-változós *formális hatványsornak* nevezzük az

$$F(\mathbf{x})=\sum_{\alpha\in\mathbb{N}^r} a_\alpha\mathbf{x}^\alpha$$

alakú formális sorokat, ahol $a_\alpha\in\mathbb{Q}_p$ minden α-ra. A formális hatványsorok halmazát $\mathbb{Q}_p[[\mathbf{x}]]$-szel jelöljük. $\mathbb{Z}_p[[\mathbf{x}]]$-szel jelöljük azoknak a hatványsoroknak a halmazát, ahol az együtthatók $\mathbb{Z}_p$-beliek.

Egy F formális hatványsor *konvergens* az $\mathbf{x}\in\mathbb{Q}_p^r$ pontban, ha $\mathbf{x}$-et behelyettesítve a sor konvergens. A helyettesítési értéket $F(\mathbf{x})$-szel jelöljük.

1.4.2. Lemma. *Legyen $F(\mathbf{x})=\sum_{\alpha\in\mathbb{N}^r} a_\alpha \mathbf{x}^\alpha$ olyan r-változós formális hatványsor, ami a $\mathbf{0}$-nak egy környezetében konvergens. Ekkor van olyan $K>0$, amelyre $|a_\alpha|_p \le K^{\langle\alpha\rangle+1}$ minden α-ra.*

Bizonyítás. Legyen $\mathbf{x}=(p^k,\dots,p^k)$. $p^k\to 0$, ezért ha k elég nagy, akkor $F(\mathbf{x})$ konvergens. Az 1.2.1. állítás miatt

$$0=\lim_{\alpha\in\mathbb{N}^r} a_\alpha \mathbf{x}^\alpha = \lim_{\alpha\in\mathbb{N}^r} a_\alpha p^{k\langle\alpha\rangle}.$$

Így van olyan $K\ge p^k$, hogy $|a_\alpha p^{k\langle\alpha\rangle}|_p \le K$ minden α-ra. Ekkor

$$|a_\alpha|_p = \left|a_\alpha p^{k\langle\alpha\rangle}\right|_p \cdot p^{k\langle\alpha\rangle} \le K\cdot K^{\langle\alpha\rangle} = K^{\langle\alpha\rangle+1}.$$

□

1.4.3. Állítás. *Legyen $F(\mathbf{x})=\sum_{\alpha\in\mathbb{N}^r} a_\alpha\mathbf{x}^\alpha$, és tegyük fel, hogy elég kicsi $\mathbf{x}$-re $F(\mathbf{x})=0$. Ekkor $a_\alpha=0$ minden α-ra.*

Bizonyítás. Először az $r=1$ esetet vizsgáljuk. Legyen $F(x)=\sum_{n=0}^\infty a_n x^n$ egyváltozós hatványsor, amelyre teljesül, hogy elég kicsi x-re $F(x)=0$, és tegyük fel, hogy van olyan n, amelyre $a_n\ne 0$. Feltehető, hogy n minimális. Az 1.4.2. lemma szerint van olyan $K>0$, hogy $|a_m|_p\le K^{m+1}$ minden m-re. Ha k elég nagy, akkor az $x=p^k$ olyan kicsi, hogy $K^{n+2}|x|_p<|a_n|_p$ és $K|x|_p\le 1$, továbbá az $F(x)$ konvergens. Az 1.2.3. állítás miatt

$$|a_n|_p|x|_p^n = |-a_n x^n|_p = \left|\sum_{m=n+1}^\infty a_m x^m\right|_p \le \sup_{m>n}|a_m x^m|_p \le \sup_{m>n} K^{n+2}|x|_p^{n+1}(K|x|_p)^{m-n-1} \le K^{n+2}|x|_p^{n+1}.$$

$|x|_p^n$-nel leosztva adódik, hogy $|a_n|_p\le K^{n+2}|x|_p$, ami ellentmondás.

Az általános esetet r szerinti indukcióval bizonyítjuk. Legyen $F\in\mathbb{Q}_p[[\mathbf{x},y]]$ egy $r+1$ változós hatványsor. Ekkor az 1.2.4. állítás miatt

$$F(\mathbf{x},y)=\sum_{\substack{\alpha\in\mathbb{N}^r\\ n\in\mathbb{N}}} a_{\alpha,n}\mathbf{x}^\alpha y^n = \sum_{n=0}^\infty\sum_{\alpha\in\mathbb{N}^r} a_{\alpha,n}\mathbf{x}^\alpha y^n = \sum_{n=0}^\infty\left(\sum_{\alpha\in\mathbb{N}^r} a_{\alpha,n}\mathbf{x}^\alpha\right)y^n.$$

A $\sum_{\alpha\in\mathbb{N}^r} a_{\alpha,n}\mathbf{x}^\alpha$ konvergenciája onnan látható, hogy elég kicsi $\mathbf{x}$ esetén van olyan $y\ne 0$, amit behelyettesítve F konvergens. Ha $\mathbf{x}$-et rögzítjük, akkor $F(\mathbf{x},y)$ egyváltozós lesz, így az $r=1$ eset miatt $\sum_{\alpha\in\mathbb{N}^r} a_{\alpha,n}\mathbf{x}^\alpha=0$ minden n-re. Ez minden elég kicsi $\mathbf{x}$-re igaz, ezért az indukciós feltevés szerint $a_{\alpha,n}=0$ minden α,n-re. □

1.4.4. Definíció. Legyen $F(\mathbf{x})=\sum_{\alpha\in\mathbb{N}^r} a_\alpha\mathbf{x}^\alpha$ és $G(\mathbf{x})=\sum_{\alpha\in\mathbb{N}^r} b_\alpha\mathbf{x}^\alpha$ két r-változós formális hatványsor. Az F és G *szorzata* az

$$(F\cdot G)(\mathbf{x})=\sum_{\alpha\in\mathbb{N}^r}\left(\sum_{\beta+\gamma=\alpha} a_\beta b_\gamma\right)\mathbf{x}^\alpha$$

formális hatványsor. Ez értelmes, mert minden együttható egy véges sok tagú összegként áll elő.

Ha F formális hatványsor, akkor ismételt szorzással definiálható az F^n, illetve $\mathbf{F}=(F_1,\dots,F_s)$ és $\alpha\in\mathbb{N}^s$ esetén az

$$\mathbf{F}^\alpha = F_1^{\alpha_1}\cdots F_s^{\alpha_s}.$$

Ellenőrizhető, hogy a hatványsorok szorzása kommutatív és asszociatív, emiatt a zárójelezés nem számít.

1.4.5. Állítás. *Ha az $F,G\in\mathbb{Q}_p[[x_1,\dots,x_r]]$ formális hatványsorok konvergensek a $\mathbf{0}$-nak egy környezetében, akkor elég kicsi $\mathbf{x}$-re $(F\cdot G)(\mathbf{x})=F(\mathbf{x})\cdot G(\mathbf{x})$.*

Bizonyítás. Legyen $F(\mathbf{x})=\sum_{\alpha\in\mathbb{N}^r} a_\alpha\mathbf{x}^\alpha$ és $G(\mathbf{x})=\sum_{\alpha\in\mathbb{N}^r} b_\alpha\mathbf{x}^\alpha$. Az 1.4.2. lemma miatt választható olyan K, hogy $|a_\alpha|_p\le K^{\langle\alpha\rangle+1}$ és $|a_\alpha|_p\le K^{\langle\alpha\rangle_1+1}$ minden α-ra. Legyen $\|\mathbf{x}\|<K^{-1}$, az ilyen $\mathbf{x}$-ek a $\mathbf{0}$-nak egy környezetét alkotják. Ha $\beta+\gamma=\alpha$, akkor

$$|a_\beta b_\gamma\mathbf{x}^\alpha|_p \le K^{\langle\beta\rangle+1}K^{\langle\beta\rangle+1}\|x\|^{\langle\alpha\rangle} = (K\|\mathbf{x}\|)^{\langle\alpha\rangle}K^2.$$

Adott α-hoz véges sok (β,γ) tartozik, ezért $\lim_{\alpha\in\mathbb{N}^r} a_\beta b_\gamma \mathbf{x}^\alpha = 0$. Így alkalmazható az 1.2.6., majd az 1.2.4 állítás:

$$F(\mathbf{x})\cdot G(\mathbf{x}) = \left(\sum_{\beta\in\mathbb{N}^r} a_\beta \mathbf{x}^\beta\right)\left(\sum_{\gamma\in\mathbb{N}^r} b_\gamma \mathbf{x}^\gamma\right) = \sum_{\beta,\gamma\in\mathbb{N}^r} a_\beta b_\gamma \mathbf{x}^{\beta+\gamma} = \sum_{\alpha\in\mathbb{N}^r}\sum_{\beta+\gamma=\alpha} a_\beta b_\gamma \mathbf{x}^\alpha = (F\cdot G)(\mathbf{x}).$$

□

1.4.6. Következmény. *Legyen $\mathbf{F}=(F_1,\dots,F_s)$, $F_i\in\mathbb{Q}_p[[x_1,\dots,x_r]]$ és $\alpha\in\mathbb{N}^s$. Ha minden F_i konvergens a $\mathbf{0}$-nak egy környezetében, akkor elég kicsi $\mathbf{x}$-re $\mathbf{F}^\alpha(\mathbf{x}) = \mathbf{F}(\mathbf{x})^\alpha$.*

1.4.7. Definíció. Legyen $F(\mathbf{x}) = \sum_{\alpha\in\mathbb{N}^r} a_\alpha \mathbf{x}^\alpha$ egy r-változós formális hatványsor, és legyen $\mathbf{G}$ egy r-elemű vektor, amelynek minden eleme $\mathbb{Q}_p[[y_1,\dots,y_s]]$-beli. Legyen $\mathbf{G}^\alpha(\mathbf{y}) = \sum_{\beta\in\mathbb{N}^s} b_{\alpha,\beta}\mathbf{y}^\beta$ minden $\alpha\in\mathbb{N}^s$-re. Tegyük fel, hogy az összes G_i konstans tagja nulla. Ekkor F és $\mathbf{G}$ *kompozíciója* az

$$(F\circ\mathbf{G})(\mathbf{y}) = \sum_{\beta\in\mathbb{N}^s}\left(\sum_{\alpha\in\mathbb{N}^r} a_\alpha b_{\alpha,\beta}\right)\mathbf{y}^\beta$$

formális hatványsor.

Mivel a G_i-k konstans tagja nulla, könnyen ellenőrizhető, hogy $\langle\beta\rangle < \langle\alpha\rangle$ esetén $b_{\alpha,\beta}=0$. Ebből nyilvánvaló az $F\circ\mathbf{G}$ együtthatóinak konvergenciája, hiszen véges sok kivétellel minden tag nulla.

1.4.8. Állítás. *Ha $F\in\mathbb{Q}_p[[x_1,\dots,x_r]]$, $\mathbf{G}=(G_1,\dots,G_r)$, $G_i\in\mathbb{Q}_p[[y_1,\dots,y_s]]$, és minden G_i konstans tagja nulla, továbbá F és $\mathbf{G}$ konvergensek a $\mathbf{0}$-nak egy környezetében, akkor elég kicsi $\mathbf{y}$-ra $(F\circ\mathbf{G})(\mathbf{y}) = F(\mathbf{G}(\mathbf{y}))$.*

Bizonyítás. Legyen $F(\mathbf{x}) = \sum_{\alpha\in\mathbb{N}^r} a_\alpha\mathbf{x}^\alpha$, $\mathbf{G}^\alpha(\mathbf{y}) = \sum_{\beta\in\mathbb{N}^s} b_{\alpha,\beta}\mathbf{y}^\beta$ és $G_i(\mathbf{y}) = \sum_{\beta\in\mathbb{N}^s} c_{i,\beta}\mathbf{x}^\beta$. Az 1.4.2. lemma miatt van olyan $K>1$, hogy $|a_\alpha|_p \le K^{\langle\alpha\rangle+1}$ és $|c_{i,\beta}|_p \le K^{\langle\beta\rangle+1}$ minden α-ra és i-re. Minden $b_{\alpha,\beta}$ felírható véges sok $c_{i_1,\beta_1}\cdots c_{i_n,\beta_n}$ alakú tag összegeként, ahol $n=\langle\alpha\rangle$ és $\beta_1+\dots+\beta_n=\beta$.

$$|c_{i_1,\beta_1}\cdots c_{i_n,\beta_n}|_p \le K^{\langle\beta_1\rangle+1}\cdots K^{\langle\beta_n\rangle+1} = K^{\langle\alpha\rangle+\langle\beta\rangle},$$

ezért az ultrametrikus egyenlőtlenség miatt $|b_{\alpha,\beta}|_p \le K^{\langle\alpha\rangle+\langle\beta\rangle}$. $b_{\alpha,\beta}\neq 0$ csak $\langle\alpha\rangle\le\langle\beta\rangle$ esetén lehet, elég ezekkel foglalkozni. Ha $\|\mathbf{y}\| < K^{-3}$, akkor

$$|a_\alpha b_{\alpha,\beta}\mathbf{y}^\beta|_p \le K^{\langle\alpha\rangle+1}K^{\langle\alpha\rangle+\langle\beta\rangle}\|\mathbf{y}\|^{\langle\beta\rangle} \le K^{3\langle\beta\rangle+1}\|\mathbf{y}\|^{\langle\beta\rangle} = (K^3\|\mathbf{y}\|)^{\langle\beta\rangle}K.$$

Rögzített β esetén véges sok α-ra teljesül, hogy $\langle\alpha\rangle\le\langle\beta\rangle$, tehát

$$\lim_{\substack{\alpha\in\mathbb{N}^r\\ \beta\in\mathbb{N}^s}} a_\alpha b_{\alpha,\beta}\mathbf{y}^\beta = 0.$$

Ha $\|\mathbf{y}\|$ elég kicsi, akkor $\mathbf{G}(\mathbf{y})$ konvergens, ezért az 1.4.6., majd az 1.2.5. állítást alkalmazva

$$F(\mathbf{G}(\mathbf{y})) = \sum_{\alpha\in\mathbb{N}^r} a_\alpha \mathbf{G}(\mathbf{y})^\alpha = \sum_{\alpha\in\mathbb{N}^r} a_\alpha \mathbf{G}^\alpha(\mathbf{y}) = \sum_{\alpha\in\mathbb{N}^r} a_\alpha \sum_{\beta\in\mathbb{N}^s} b_{\alpha,\beta}\mathbf{y}^\beta =$$
$$= \sum_{\alpha\in\mathbb{N}^r}\sum_{\beta\in\mathbb{N}^s} a_\alpha b_{\alpha,\beta}\mathbf{y}^\beta = \sum_{\beta\in\mathbb{N}^s}\sum_{\alpha\in\mathbb{N}^r} a_\alpha b_{\alpha,\beta}\mathbf{y}^\beta = (F\circ\mathbf{G})(\mathbf{y}).$$

□

1.4.9. Állítás. *Legyen $F\in\mathbb{Z}_p[[x_1,\dots,x_r]]$ és $\mathbf{G}=(G_1,\dots,G_r)$, $G_i\in\mathbb{Z}_p[[y_1,\dots,y_s]]$. Ha az összes G_i konstans tagja nulla, akkor $F\circ\mathbf{G}\in\mathbb{Z}_p[[\mathbf{y}]]$, és minden $\mathbf{y}\in p\mathbb{Z}_p^s$-re $(F\circ\mathbf{G})(\mathbf{y}) = F(\mathbf{G}(\mathbf{y}))$.*

Bizonyítás. A definícióból triviális, hogy $F\circ\mathbf{G}\in\mathbb{Z}_p[[\mathbf{y}]]$. Az $(F\circ\mathbf{G})(\mathbf{y}) = F(\mathbf{G}(\mathbf{y}))$ ugyanúgy bizonyítható, mint az előző állítás. A konvergencia most nyilvánvaló, mert az összes együttható $\mathbb{Z}_p$-beli, és ha $\mathbf{y}\in p\mathbb{Z}_p^s$, akkor $|\mathbf{y}^\alpha|_p \le p^{-\langle\alpha\rangle}$. □

1.4.10. Definíció. Legyen $D \subseteq \mathbb{Q}_p^r$ nyílt halmaz. Egy $f : D \to \mathbb{Q}_p$ függvény *analitikus* $\mathbf{x} \in D$-ben, ha van olyan $U \ni \mathbf{x}$ környezet és F formális hatványsor, hogy F konvergens $U - \mathbf{x}$-en, és $f(\mathbf{y}) = F(\mathbf{y} - \mathbf{x})$ minden $\mathbf{y} \in U$-ra. f analitikus a D-n, ha a D minden pontjában analitikus. Egy $\mathbf{f} : D \to \mathbb{Q}_p^s$ függvény analitikus, ha komponensenként analitikus.

1.4.11. Lemma. *Legyen $F(\mathbf{x})$ olyan hatványsor, ami minden $\mathbf{x} \in \mathbb{Z}_p^r$-ben konvergens. Ekkor az F által meghatározott függvény analitikus $\mathbb{Z}_p^r$-en.*

Bizonyítás. Legyen $F(\mathbf{x}) = \sum_{\alpha \in \mathbb{N}^r} a_\alpha \mathbf{x}^\alpha$. F konvergens az $\mathbf{x} = (1, \dots, 1)$-ben, ezért az 1.2.1. állítás miatt $\lim_{\alpha \in \mathbb{N}^r} a_\alpha = 0$. Rögzítsük $\mathbf{y} \in \mathbb{Z}_p^r$-et. A binomiális tétel és az 1.2.4. állítás miatt

$$F(\mathbf{y}+\mathbf{x}) = \sum_{\alpha \in \mathbb{N}^r} a_\alpha (\mathbf{y}+\mathbf{x})^\alpha = \sum_{\alpha \in \mathbb{N}^r} \sum_{\beta+\gamma=\alpha} a_\alpha \binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_r}{\beta_r} \mathbf{y}^\beta \mathbf{x}^\gamma =$$

$$= \sum_{\gamma \in \mathbb{N}^r} \sum_{\beta+\gamma=\alpha} a_\alpha \binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_r}{\beta_r} \mathbf{y}^\beta \mathbf{x}^\gamma = \sum_{\gamma \in \mathbb{N}^r} \left(\sum_{\beta+\gamma=\alpha} a_\alpha \binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_r}{\beta_r} \mathbf{y}^\beta \right) \mathbf{x}^\gamma$$

A konvergenciához azt kell ellenőrizzük, hogy

$$\lim_{\beta+\gamma=\alpha} a_\alpha \binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_r}{\beta_r} \mathbf{y}^\beta \mathbf{x}^\gamma = 0,$$

illetve rögzített γ-ra

$$\lim_{\beta+\gamma=\alpha} a_\alpha \binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_r}{\beta_r} \mathbf{y}^\beta = 0.$$

Mindkettő nyilvánvaló, hiszen rögzített α-hoz véges sok γ és β tartozik, és az a_α kivételével minden tényező $\mathbb{Z}_p$-beli, így a normájuk legfeljebb 1. Ezzel megmutattuk, hogy az $\mathbf{x} \mapsto F(\mathbf{y}+\mathbf{x})$ előáll hatványsorként, tehát F analitikus $\mathbf{y}$-ban. □

Megjegyzés. Egy $\mathbf{x} \in \mathbb{Q}_p^r$ minden környezete tartalmaz $\mathbf{x} + p^k \mathbb{Z}_p^r$ alakú környezetet. Emiatt egy f függvény pontosan akkor analitikus $\mathbf{x}$-ben, ha valamilyen k-ra van olyan F formális hatványsor, hogy $f(\mathbf{x}+p^k\mathbf{y}) = F(\mathbf{y})$ minden $\mathbf{y} \in \mathbb{Z}_p^r$-re. Az 1.4.11. lemma következtében f az $\mathbf{x}+p^k\mathbf{y}$ alakú pontokban is analitikus, tehát nincs különbség aközött, hogy f az $\mathbf{x}$-ben, vagy az $\mathbf{x}$-nek egy környezetében analitikus.

1.4.12. Állítás. *Ha $\mathbf{f} : D \to \mathbb{Q}_p^s$ analitikus, akkor folytonos.*

Bizonyítás. Elég $s = 1$-re bizonyítani. Legyen $f : D \to \mathbb{Q}_p$ analitikus, és legyen $\mathbf{x} \in D$ és $0 < \varepsilon < 1$ tetszőleges. Van olyan $U \ni \mathbf{x}$ környezet, hogy minden $\mathbf{y} \in U - \mathbf{x}$-re

$$f(\mathbf{x}+\mathbf{y}) = \sum_{\alpha \in \mathbb{N}^r} a_\alpha \mathbf{y}^\alpha$$

alakú. Az 1.4.2. lemma miatt van olyan $K > 1$, amelyre $|a_\alpha|_p \le K^{\langle \alpha \rangle + 1}$ minden α-ra. Ha $\|\mathbf{y}\| \le \varepsilon K^{-2}$, akkor az 1.2.3. állítás miatt

$$|f(\mathbf{x}+\mathbf{y}) - f(\mathbf{x})|_p = \left| \sum_{\alpha \neq \mathbf{0}} a_\alpha \mathbf{y}^\alpha \right|_p \le \sup_{\alpha \neq \mathbf{0}} |a_\alpha \mathbf{y}^\alpha|_p \le \sup_{\alpha \neq \mathbf{0}} K^{1-\langle \alpha \rangle} \varepsilon^{\langle \alpha \rangle} \le \varepsilon,$$

ezzel megmutattuk az $\mathbf{x}$-beli folytonosságot. □

1.4.13. Állítás. *Legyenek $U \subseteq \mathbb{Q}_p^r$, $V \subseteq \mathbb{Q}_p^s$ és $W \subseteq \mathbb{Q}_p^t$ nyílt halmazok. Tegyük fel, hogy a $\mathbf{g} : U \to V$ és $\mathbf{f} : V \to W$ analitikusak. Ekkor $\mathbf{f} \circ \mathbf{g}$ is analitikus.*

Bizonyítás. Elég a $t = 1$ esetet vizsgálni. Legyen $\mathbf{x} \in U$ tetszőleges. Ekkor elég kicsi $\mathbf{y}$-ra $\mathbf{g}(\mathbf{x}+\mathbf{y}) = \mathbf{g}(\mathbf{x}) + \mathbf{G}(\mathbf{y})$ alakú, ahol $\mathbf{G}$ minden komponense olyan formális hatványsor, amelynek a konstans tagja nulla. Ha F az f-nek a $\mathbf{g}(\mathbf{x})$ körüli hatványsora, akkor a $\mathbf{g}$ folytonossága és az 1.4.8. állítás miatt elég kicsi $\mathbf{y}$-ra

$$f(\mathbf{g}(\mathbf{x}+\mathbf{y})) = f(\mathbf{g}(\mathbf{x}) + \mathbf{G}(\mathbf{y})) = F(\mathbf{G}(\mathbf{y})) = (F \circ \mathbf{G})(\mathbf{y}),$$

tehát $f \circ \mathbf{g}$ analitikus $\mathbf{y}$-ban. □

2. Pro-p- és hatványteljes csoportok

2.1. Provéges csoportok

2.1.1. Definíció. A G csoportot *topologikus csoportnak* nevezzük, ha adott rajta egy topológia, amelyre nézve a szorzás és az inverzképzés folytonosak.

A továbbiakban $H \leq_o G$-vel és $H \leq_c G$-vel jelöljük a nyílt, illetve zárt részcsoportot. A normálosztókat hasonlóan $N \lhd_o G$-vel és $N \lhd_c G$-vel jelöljük.

2.1.2. Definíció. Egy topologikus csoport *provéges*, ha kompakt és Hausdorff, továbbá a nyílt részcsoportjai az egységelem környezetbázisát alkotják.

A provéges csoportokra a legegyszerűbb példák a véges csoportok a diszkrét topológiával (a Hausdorff-tulajdonság miatt egy véges provéges csoport topológiája csak diszkrét lehet).

Legyen G egy provéges csoport. Mivel a $g \in G$-vel való jobbról, illetve balról szorzás homeomorfizmus, egy nyílt részcsoport mellékosztályai is nyíltak. A kompaktság következtében minden nyílt részcsoport véges indexű, emiatt zárt is. Látható, hogy egy zárt részcsoport pontosan akkor nyílt, ha véges indexű.

2.1.3. Állítás. *Egy provéges csoportban a nyílt normálosztók mellékosztályai a topológiának egy bázisát alkotják.*

Bizonyítás. Először megmutatjuk, hogy minden $H \leq_o G$ tartalmaz nyílt normálosztót. Vegyünk egy hx elemet, ahol $h \in H$. Ekkor $H^{hx} = (H^h)^x = H^x$. Emiatt a H^x csak attól függ, hogy x a H-nak melyik bal mellékosztályában van, tehát H-nak véges sok konjugáltja van. Ezek nyíltak, mert a konjugálás homeomorfizmus, így a $\bigcap_{x \in G} H^x$ nyílt normálosztó G-ben.

Ezzel beláttuk, hogy a nyílt normálosztók az egységelemnek egy környezetbázisát alkotják. Ha $g \in G$ tetszőleges, akkor a gN ($N \lhd_o G$) alakú mellékosztályok a g-nek egy környezetbázisát adják, emiatt az összes gN egy bázist alkot. □

2.1.4. Állítás. *Legyen $X \subseteq G$ részhalmaz. Ekkor*

$$\overline{X} = \bigcap_{N \lhd_o G} XN.$$

Bizonyítás. A metszetben szereplő részcsoportok nyíltak, ezért zártak is, tehát a metszet zárt, és tartalmazza X-et. Emiatt $\overline{X} \subseteq \bigcap_{N \lhd_o G} XN$.

Legyen $g \notin \overline{X}$. A 2.1.3. állítás miatt van olyan $N \lhd_o G$, amelyre $gN \cap \overline{X} = \emptyset$. Világos, hogy ekkor $g \notin XN$. Ezzel megmutattuk, hogy $\overline{X} \supseteq \bigcap_{N \lhd_o G} XN$. □

2.1.5. Állítás. *Legyen $N \lhd_c G$. Ekkor a G/N faktorcsoport a faktortopológiával provéges.*

Bizonyítás. A faktortopológia definíciójából adódik, hogy a G/N topologikus csoport, illetve a faktorleképezés folytonosságából a kompaktság triviális.

Ha $xN \neq yN$, akkor az yN zártsága és a 2.1.3. állítás miatt van olyan $M \lhd_o G$, amelyre $xM \cap yN = \emptyset$. Ekkor $xMN \cap yMN = \emptyset$, vagyis az xMN/N és yMN/N diszjunkt környezetek a G/N-ben.

Ha U/N nyílt környezete az egységelemnek, akkor U nyílt G-ben, és N mellékosztályainak uniója. A 2.1.3. állítás miatt van olyan $M \lhd_o G$, amelyre $M \subseteq U$, ebből következik, hogy az $MN/N \subseteq U/N$ nyílt részcsoportja G/N-nek. □

2.1.6. Állítás (Cauchy-kritérium)**.** *Tegyük fel, hogy a $(g_n) \in G$ sorozatra teljesül, hogy minden $N \lhd_o G$-re van olyan n_0, hogy minden $n, m \geq n_0$-ra $g_n g_m^{-1} \in N$. Ekkor a (g_n) sorozat konvergens.*

Bizonyítás. A feltételből következik, hogy minden $N \lhd_o G$-re a sorozat valahonnan kezdve valamelyik $x_N N$ mellékosztályban van. Véges sok ilyen mellékosztályra teljesül, hogy a soroazt valahonnan kezdve mindegyikben benne van. Emiatt az $x_N N$ alakú mellékosztályok zárt halmazok centrált rendszerét alkotják, így a kompaktság miatt a metszetük tartalmaz valamilyen g elemet. A 2.1.3. állításból adódik, hogy $g_n \to g$. □

Megjegyzés. A Cauchy-kritérium abban az esetben is alkalmazható, ha csak olyan N-eket veszünk, amelyek az egységelemnek egy környezetbázisát alkotják.

2.1.7. Definíció. Az $X \subseteq G$ halmaz *topologikusan generálja* G-t, ha $\langle X \rangle$ sűrű, azaz $\overline{\langle X \rangle} = G$. A G *végesen generált*, ha egy véges halmaz topologikusan generálja.

2.1.8. Állítás. *Tegyük fel, hogy G végesen generált, és $H \leq_o G$. Ekkor a H is végesen generált.*

Bizonyítás. Legyen X véges halmaz, amelyre $\overline{\langle X \rangle} = G$. Feltehető, hogy X minden elemének az inverzét is tartalmazza, Válasszunk egy T transzverzálist a H-hoz, azaz egy olyan halmazt, ami a H minden jobb mellékosztályából pontosan egy elemet tartalmaz. Feltehető, hogy $1 \in T$. Legyen

$$Y = \{t_1 x t_2^{-1} \in H \mid x \in X, t_i \in T\}.$$

Az X és a T végesek, ezért az Y is véges.

Vegyünk egy $x_1 \cdots x_n \in H$ elemet, ahol $x_i \in X$. Az $x_1 \cdots x_i$ minden $0 \leq i \leq n$-re benne van valamelyik Ht_i-ben, ahol $t_i \in T$. Ekkor

$$x_1 \cdots x_{i-1} t_{i-1}^{-1} \in H$$

és

$$x_1 \cdots x_i t_i^{-1} \in H,$$

ezért $t_{i-1} x_i t_i^{-1} \in H$. Látható, hogy $t_0 = t_n = 1$, ezért

$$x_1 x_2 \cdots x_n = (t_0 x_1 t_1^{-1})(t_1 x_2 t_2^{-1}) \cdots (t_{n-1} x_n t_n^{-1}).$$

Tehát $\langle Y \rangle \supseteq \langle X \rangle \cap H$. Emiatt

$$\overline{\langle Y \rangle} \supseteq \overline{\langle X \rangle \cap H} \supseteq \overline{\langle X \rangle} \cap H = H,$$

felhasználva, hogy H nyílt. □

2.1.9. Definíció. A G *Frattini-részcsoportja* a G maximális nyílt valódi részcsoportjainak metszete. A Frattini-részcsoportot $\Phi(G)$-vel jelöljük.

G-ben a nyílt részcsoportok egyben zártak is, ebből azonnal adódik, hogy $\Phi(G)$ zárt.

2.1.10. Állítás. *Egy $X \subseteq G$ halmaz pontosan akkor generálja topologikusan G-t, ha az $X\Phi(G)/\Phi(G)$ topologikusan generálja $G/\Phi(G)$-t.*

Bizonyítás. Ha $\overline{\langle X \rangle} = G$, akkor a faktorleképezés folytonossága miatt

$$\overline{\langle X\Phi(G)/\Phi(G) \rangle} = \overline{\langle X \rangle \Phi(G)/\Phi(G)} \geq \overline{\langle X \rangle} \Phi(G)/\Phi(G) = G/\Phi(G)$$

Most tegyük fel, hogy $\overline{\langle X \rangle} < G$. A 2.1.4. állítás miatt van olyan $N \lhd_o G$, amelyre $\langle X \rangle N < G$. Az $\langle X \rangle N$ nyílt, ezért véges indexű, így kiegészíthető egy maximális $M < G$-vé. Az M szintén nyílt, ezért $\Phi(G) \leq M$. Emiatt

$$\overline{\langle X\Phi(G)/\Phi(G) \rangle} = \overline{\langle X \rangle \Phi(G)/\Phi(G)} \leq M/\Phi(G) < G/\Phi(G).$$

□

2.2. Pro-p-csoportok

2.2.1. Definíció. Legyen p prím. A G provéges csoport *pro-p-csoport*, ha minden nyílt részcsoportja p-hatvány indexű.

2.2.2. Állítás. *A $(\mathbb{Z}_p, +)$ pro-p-csoport.*

Bizonyítás. A kompaktságot korábban láttuk, a Hausdorff-tulajdonság nyilvánvaló.

Legyen $U \subseteq \mathbb{Z}_p$ nyílt környezete a 0-nak. Ekkor U tartalmazza a $p^n\mathbb{Z}_p$-t valamilyen n-re. Ez az $x \bmod p^n$ leképezés magja, ezért p-hatvány indexű nyílt részcsoport. Ezzel beláttuk, hogy a nyílt részcsoportok az egységelemnek egy környezetbázisát alkotják. Mivel $\mathbb{Z}_p$ minden nyílt részcsoportja tartalmaz p-hatvány indexű nyílt részcsoportot, következik, hogy minden nyílt részcsoport indexe p-hatvány. □

A továbbiakban legyen G egy pro-p-csoport.

2.2.3. Állítás. *Legyen $g \in G$ tetszőleges, és legyen (x_n) egy $\mathbb{Z}$-beli sorozat, ami a $|\cdot|_p$ szerint Cauchy-sorozat. Ekkor a (g^{x_n}) sorozat konvergens.*

Bizonyítás. A 2.1.6. állítás miatt elég, ha a (g^{x_n}) Cauchy-sorozat. Legyen $N \lhd_o G$. Ekkor $|G{:}N| = p^k$ valamilyen k-ra. Ha n és m elég nagy, akkor $|x_n - x_m|_p \leq p^{-k}$, azaz $p^k \mid x_n - x_m$. Emiatt $g^{x_n} g^{-x_m} = g^{x_n - x_m} \in N$, hiszen a G/N-ben minden elem p^k-adik hatványa az egységelem. □

2.2.4. Definíció. Legyen $g \in G$ és $\lambda \in \mathbb{Z}_p$. Ekkor $\lambda = \lim_{n\to\infty} x_n$, ahol $x_n \in \mathbb{Z}$. Legyen

$$g^\lambda = \lim_{n\to\infty} g^{x_n}.$$

A Hausdorff-tulajdonságból adódik a határérték egyértelműsége. Ha $x_n \to \lambda$ és $y_n \to \lambda$, akkor a (g^{x_n}) és (g^{y_n}) sorozatok összefésülésével konvergens sorozatot kapunk, emiatt a definíció nem függ a sorozat megválasztásától.

2.2.5. Állítás. *A $(g, \lambda) \mapsto g^\lambda$ folytonos leképezés.*

Bizonyítás. A 2.1.3. állítás miatt elég, ha minden $N \lhd_o G$ őse nyílt. Tegyük fel, hogy $x_n \in \mathbb{Z}$, $x_n \to \lambda$ és $g^\lambda \in N$. N nyílt, ezért elég nagy n-re $g^{x_n} \in N$. A sorozat elejét elhagyva feltehető, hogy ez minden n-re igaz. Ha $h \in gN$, akkor nyilván $h^{x_n} \in N$ is teljesül. Legyen $|G : N| = p^k$. Ha $y \in \mathbb{Z}$, $y \equiv x_n \pmod{p^k}$, akkor $h^y \in N$. Az N zártságából következik, hogy ha $\mu \in \mathbb{Z}_p$ és $\mu \equiv \lambda \pmod{p^n}$, akkor $h^\mu \in N$. Tehát N ősképe tartalmazza a $gN \times (\lambda + p^k\mathbb{Z}_p)$ halmazt, ami a (g, λ)-nak nyílt környezete. □

2.2.6. Állítás. *Tetszőleges $g, h \in G$-re és $\lambda, \mu \in \mathbb{Z}_p$-re $g^{\lambda+\mu} = g^\lambda g^\mu$, $g^{\lambda\mu} = (g^\lambda)^\mu$ és $(g^h)^\lambda = (g^\lambda)^h$.*

Bizonyítás. Az állítás triviális, ha $\lambda, \mu \in \mathbb{Z}$. A folytonosságból látható, hogy akkor is igaz, ha $\lambda, \mu \in \mathbb{Z}_p$. □

2.2.7. Lemma. *Ha P véges p-csoport, akkor minden $M < P$ maximális valódi részcsoport normálosztó, és $P/M \cong Z_p$, ahol Z_p a p rendű ciklikus csoport.*

Bizonyítás. $|P|$ szerinti indukcióval bizonyítjuk. $|P| = 1$ esetén az állítás triviális.

Ha $|P| \geq p$, akkor $Z(P)$ nem triviális. Ha $Z(P) \leq M$, akkor az $M/Z(P)$ maximális $P/Z(P)$-ben, ezért az indukciós feltevés miatt

$$M/Z(P) \lhd P/Z(P).$$

Emiatt $M \lhd P$.

Ha $Z(P) \not\leq M$, akkor $N_P(M) \geq MZ(P) > M$, ezért a maximalitás miatt $N_P(M) = P$, vagyis M normálosztó.

A maximalitás miatt az N/M-nek csak triviális részcsoportjai vannak, ezért csak p rendű ciklikus lehet. □

2.2.8. Állítás.

$$\Phi(G) = \overline{G^p G'},$$

ahol $G^p = \langle g^p \mid g \in G \rangle$.

Bizonyítás. $\leq$: A 2.1.4. állítás miatt elég azt megmutatni, hogy

$$\Phi(G) \leq G^p G' N$$

minden $N \lhd_o G$-re. Ekkor a

$$V = G/G^p G' N$$

egy véges $\mathbb{F}_p$ feletti vektortér additív csoportja (mert kommutatív, és minden $x \in V$-re $x^p = 1$). Emiatt a maximális részcsoportjai pontosan az 1 kodimenziójú alterek, ezeknek a metszete triviális. Ebből már következik az állítás, mert a V-beli maximális részcsoportok G-beli ősképei is maximálisak.

$\geq$: Legyen $M \leq_o G$ maximális. A 2.1.3. állítás miatt választható $N \lhd_o G$, amelyre $N \leq M$. Ekkor M/N maximális a G/N véges p-csoportban, így a 2.2.7. lemma következtében $M/N \lhd G/N$, azaz $M \lhd_o G$, továbbá $G/M \cong (G/N)/(M/N) \cong Z_p$. Emiatt $M \leq G'$ és $M \leq G^p$, innen az M zártságából következik az állítás. □

2.2.9. Következmény. *A $G/\Phi(G)$ elemi Abel-csoport, azaz egy $\mathbb{F}_p$ feletti vektortér additív csoportja.*

2.2.10. Tétel (Burnside-féle bázistétel)**.** *Egy $X \subseteq G$ pontosan akkor minimális topologikus generátorrendszer, ha az $X\Phi(G)/\Phi(G)$ a $G/\Phi(G)$ vektortér bázisa.*

Bizonyítás. Az $\mathbb{F}_p$ additív csoportját generálja az 1. Emiatt egy $\mathbb{F}_p$ feletti vektortér additív csoportjának részcsoportjai pontosan a lineáris alterek. Így az additív csoport minimális generátorrendszerei pontosan a bázisok. Innen a 2.1.10. állítást felhasználva készen vagyunk. □

2.2.11. Definíció. Legyen G egy pro-p-csoport. A $P_i(G)$ részcsoportot rekurzívan definiáljuk:

$$P_1(G) = G$$
$$P_{i+1}(G) = \overline{P_i(G)^p [P_i(G), G]}$$

Világos, hogy $P_2(G) = \Phi(G)$, és $P_{i+1}(G) \geq \Phi(P_i(G))$ minden i-re.

2.2.12. Állítás. *Legyen $K \lhd_c G$. Ekkor $P_i(G/K) = P_i(G)K/K$.*

Bizonyítás. $i = 1$-re az állítás triviális. Tegyük fel, hogy i-re már tudjuk, hogy igaz. Ekkor

$$P_{i+1}(G/K) = \overline{P_i(G/K)[P_i(G/K), G/K]} = \overline{P_i(G)[P_i(G), G]K/K} = \overline{P_i(G)[P_i(G), G]}K/K = P_i(G)K/K,$$

felhasználva, hogy $\overline{XK/K} = \overline{X}K/K$, ami onnan látható, hogy a faktorleképezés folytonos, és a kompaktság miatt zárt leképezés (zárt képe zárt). □

2.3. Végesen generált pro-p-csoportok

Ebben a szakaszban G egy végesen generált pro-p-csoport.

2.3.1. Állítás. *$\Phi(G)$ nyílt.*

Bizonyítás. Legyen X egy véges generátorrendszer. Ekkor a 2.1.10. állítás szerint az $Y = X\Phi(G)/\Phi(G)$ topologikusan generálja a $V = G/\Phi(G)$-t. Az Y is véges, ezért az $\langle Y \rangle \leq V$ véges dimenziós altér. Így $\langle Y \rangle$ véges, ezért zárt, tehát

$$V = \overline{\langle Y \rangle} = \langle Y \rangle,$$

emiatt V is véges. Ebből következik, hogy a $\Phi(G)$ véges indexű zárt részcsoport. □

2.3.2. Következmény. *A $P_i(G)$ nyílt minden i-re.*

Bizonyítás. Ha a $P_i(G)$ nyílt, akkor a 2.1.8. állítás következtében végesen generált. Emiatt a $\Phi(P_i(G))$ nyílt, tehát a $P_{i+1}(G) \geq \Phi(P_i(G))$ is nyílt. □

2.3.3. Lemma. *Legyen P véges p-csoport, és legyen $1 < N \lhd P$. Ekkor van olyan $J \lhd P$, amelyre $J < N$, $N/J \cong Z_p$, és $N/J \leq Z(P/J)$.*

Bizonyítás. $|P|$ szerinti indukcióval bizonyítjuk. Ha $Z(P) \geq N$, akkor az N tetszőleges maximális részcsoportját választhatjuk J-nek a 2.2.7. állítás miatt.

Az N normálosztó, ezért a P néhány konjugáltosztályának az uniója. Minden konjugáltosztály mérete p-vel osztható, kivéve a $Z(P)$ elemeit, amik egyelemű konjugáltosztályokat alkotnak. Emiatt $p \mid |N \cap Z(P)|$, tehát $1 < N \cap Z(P)$. Ha $Z(P) \not\geq N$, akkor az indukciós feltevés szerint a $G/(N \cap Z(P))$-ben van olyan $J/(N \cap \cap Z(P)) \lhd_o P$, ami teljesíti a feltételeket. Könnyen látható, hogy ekkor a J jó lesz. □

2.3.4. Állítás. *A $P_i(G)$-k az egységelemnek egy környezetbázisát alkotják.*

Bizonyítás. Elég azt megmutatni, hogy minden $N \lhd_o G$ tartalmazza valamelyik $P_i(G)$-t. A 2.2.12. állítás miatt ehhez elég, ha a $P = G/N$-hez van olyan i, hogy $P_i(P) = 1$.

Ha $P_i(P) > 1$, akkor válasszuk J-t a 2.3.3. lemma szerint ($N = P_i(P)$-vel). Ekkor

$$P_{i+1}(P) = P_i(P)^p[P_i(P), P] \leq J < P_i(P).$$

A P végessége miatt a $P_i(P)$ nem csökkenhet akármeddig, ezért valamikor eléri a $P_i(P) = 1$-et. □

2.3.5. Lemma. *Legyen $P = \langle a_1, \ldots, a_d \rangle$ véges p-csoport. Ekkor*

$$P' = \big\{ [x_1, a_1] \cdots [x_d, a_d] \,\big|\, x_1, \ldots, x_d \in P \big\},$$

ahol $[a, b] = a^{-1}b^{-1}ab$ a kommutátor.

Bizonyítás. $|P|$ szerinti indukcióval bizonyítjuk. Az állítás triviális abban az esetben, ha P kommutatív.

Legyen $Z_1 = Z(P)$ és $Z_2/Z_1 = Z(P/Z_1)$. Ha P nem kommutatív, akkor P/Z_1 nemtriviális p-csoport, ezért $Z_2 > Z_1$. Emiatt $1 < [Z_2, P] \leq Z_1$. Az indukciós feltevést a $P/[Z_2, P]$-re alkalmazva adódik, hogy minden $x \in P'$ előáll

$$x = [x_1, a_1] \cdots [x_d, a_d]w$$

alakban, ahol $w \in [Z_2, P]$.

Ha $z \in Z_2$ és $y, g \in P$ akkor ellenőrizhető, hogy

$$[zy, g] = [z, g]^y[y, g] = [z, g][y, g],$$

mivel $[z, g] \in [Z_2, P] \leq Z_1$. Az előző összefüggés ismételt alkalmazásával látható, hogy elég, ha a w-t generálják a $[z, a_i]$ alakú elemek, mert ezeket összevonhatjuk az $[x_i, a_i]$-kkel. Hasonlóan látható, hogy

$$[z, gh] = [z, h][z, g]^h = [z, g][z, h].$$

A $[Z_2, P]$ kommutativitása miatt a

$$Z_2 \times P \to [Z_2, P], \quad (z, g) \mapsto [z, g]$$

leképezés epimorfizmus. A $Z_2 \times P$-t generálják a (z, a_i) alakú elemek, ezért a $[Z_2, P]$-t generálják a $[z, a_i]$ alakú elemek, tehát a w-t is. □

2.3.6. Állítás. *G' zárt.*

Bizonyítás. Legyen $a_1, \ldots, a_d$ topologikus generátorrendszer. Ekkor

$$\langle a_1 N/N, \ldots, a_d N/N \rangle = G/N$$

minden $N \lhd_o G$-re. A 2.3.5. lemmát G/N-re alkalmazva kapjuk, hogy

$$G'N = \bigcup_{x_1, \ldots, x_d \in G} [x_1, a_1] \cdots [x_d, a_d]N = f(X)N,$$

ahol $f(x_1, \ldots x_d) = [x_1, a_1] \cdots [x_d, a_d]$, és X a $G \times \ldots \times G$ szorzattér. Az f folytonossága miatt az $f(X)$ kompakt, így a 2.1.4. állítást felhasználva

$$\overline{G'} = \bigcap_{N \lhd_o G} G'N = \bigcap_{N \lhd_o G} f(X)N = f(X) \leq G'$$

□

2.3.7. Állítás. $\Phi(G) = G^pG'$.

Bizonyítás. A 2.2.8. állítás miatt elég azt megmutatni, hogy a G^pG' zárt. A G/G' Abel-csoport, ezért a $g \mapsto g^p$ egy $G/G' \twoheadrightarrow G^p/G'$ epimorfizmus. Emiatt a

$$G^pG'/G' = (G/G')^p = \{g^p : g \in G/G'\}$$

kompakt. A G^pG' zártsága a faktorleképezés folytonosságából adódik. □

2.3.8. Tétel. *Egy végesen generált pro-p-csoportban minden véges indexű részcsoport nyílt.*

Bizonyítás. Legyen $H \leq G$ véges indexű. A 2.1.3. állítás bizonyításához hasonlóan látható, hogy H tartalmaz valamilyen véges indexű $K \lhd G$-t, elég erről megmutatni, hogy nyílt.

Először megmutatjuk, hogy K indexe csak p-hatvány lehet. Ha nem p-hatvány, akkor a Cauchy-tétel miatt a G/K-nak van q rendű eleme, ahol $q \neq p$ prím. Emiatt a G/K-ban a $g \mapsto g^q$ nem bijektív, ezért a G-ben nem minden elem áll elő q-adik hatványként. Ez viszont ellentmondás, mert ha $r = q^{-1} \in \mathbb{Z}_p$, akkor tetszőleges $g \in G$-re

$$g = g^{rq} = (g^r)^q.$$

Most K indexe szerinti indukciót alkalmazunk. A $K = G$ esetben az állítás triviális. Ha a G/K nem triviális, akkor $\Phi(G/K) < G/K$. A G/K véges p-csoport, ezért a a 2.2.8 állítás szerint

$$(G/K)^p(G/K)' = \Phi(G/K) < G/K,$$

így $G^pG'K < G$. Emiatt $|G^pG'K : K| < |G : K|$. A G^pG' a 2.3.1. és 2.3.7. állítás miatt nyílt, így a $G^pG'K$ is nyílt. A 2.1.8. állítás miatt a $G^pG'K$ végesen generált, ezért alkalmazható az indukciós feltevés. Így K nyílt a $G^pG'K$-ban, tehát a G-ben is. □

2.3.9. Következmény. *Ha H provéges csoport, akkor minden $\varphi : G \to H$ homomorfizmus folytonos.*

Bizonyítás. Ha $N \lhd_o H$, akkor $|G : \varphi^{-1}(N)|$ véges, tehát a 2.3.8. tétel szerint $\varphi^{-1}(N)$ nyílt. A 2.1.3. állítás miatt ebből már következik φ folytonossága. □

2.3.10. Következmény. *Egy végesen generált pro-p-csoport topológiáját meghatározza a csoportstruktúra.*

Bizonyítás. Legyen τ_1 és τ_2 két topológia G-n, amellyel végesen generált pro-p-csoport. Ha $f : (G, \tau_1) \to (G, \tau_2)$ az identitás, akkor az előző állítás miatt f folytonos, és hasonlóan f^{-1} is folytonos. □

2.4. Hatványteljes csoportok

2.4.1. Definíció. Legyen G pro-p-csoport, és $N \leq_o G$. Ekkor N *hatványteljesen van beágyazva* G-be, ha $p > 2$ esetén $[N, G] \leq \overline{N^p}$, $p = 2$ esetén pedig $[N, G] \leq \overline{N^4}$. Ezt N *p.e.* G-vel jelöljük (ez az angol „powerfully embedded" rövidítése). A G *hatványteljes*, ha G *p.e.* G.

2.4.2. Állítás. *Ha N p.e. G, akkor N hatványteljes és normálosztó.*

Bizonyítás. A hatványteljesség a definícióból triviális.

Ha $n \in N$ és $g \in G$ tetszőleges, akkor

$$n^g = n[n, g] \in n[N, G] \subseteq n\overline{N^p} \subseteq N,$$

emiatt normálosztó. □

2.4.3. Állítás. *Ha G hatványteljes, akkor $\Phi(G) = \overline{G^p}$.*

Bizonyítás. A 2.2.8. állítás szerint $\Phi(G) = \overline{G^pG'}$.

$$G^pG' \leq G^p\overline{G^p} = \overline{G^p} \leq \overline{G^pG'},$$

ezért $\overline{G^pG'} = \overline{G^p}$. □

2.4.4. Állítás. *Legyen $N \leq_o G$, ahol G pro-p-csoport. Ekkor N p.e. G pontosan akkor, ha minden $K \lhd_o G$-re NK/K p.e. G/K.*

Bizonyítás. Ha $p > 2$, akkor a 2.1.4. állítás miatt $[N, G] \leq \overline{N^p}$ pontosan akkor, ha $[N, G]K \leq N^p K$ minden $K \lhd_o G$-re, ami ekvivalens azzal, hogy

$$[NK/K, G/K] \leq (NK/K)^p,$$

azaz NK/K p.e. G/K.

A $p = 2$ eset hasonló. □

2.4.5. Lemma. *Legyen $x, y \in G$, és tegyük fel, hogy $[y, x] \in Z(G)$. Ekkor*

$$(xy)^n = x^n y^n [y, x]^{n(n-1)/2}$$

Bizonyítás. n szerinti indukcióval bizonyítjuk, $n = 0$ esetén triviális. Először vegyük észre, hogy

$$y^n x = x(y^n)^x = x(y^x)^n = x(y^x)^n = x(y[y, x])^n = xy^n[y, x]^n.$$

Ezt felhasználva

$$(xy)^{n+1} = (xy)^n xy = x^n y^n xy[x, y]^{n(n-1)/2} = x^n xy^n [y, x]^n y[x, y]^{n(n-1)/2} = x^{n+1} y^{n+1} [y, x]^{(n+1)n/2},$$

ezzel beláttuk az indukciós lépést. □

2.4.6. Állítás. *Legyen G véges p-csoport, és N p.e. G. Ekkor N^p p.e. G.*

Bizonyítás. Legyen $M = (N^p)^p$, ha $p > 2$, és legyen $M = (N^2)^4$, ha $p = 2$. Tegyük fel, hogy $[N^p, G] \not\leq M$. Ez azt jelenti, hogy

$$1 < [N^p, G]M/M \leq G/M.$$

A 2.3.3. lemmát G/M-ben alkalmazva találhatunk olyan $M \leq J \lhd G$-t, amelyre $J < [N^p, G]M$, $[N^p, G]M/J \cong Z_p$ és $[N^p, G]M/J \leq Z(G/J)$. Cseréljük le a csoportokat a $G \to G/J$ faktorleképezés szerinti képeikre. Így feltehető, hogy $M = 1$, $[N^p, G] \cong Z_p$ és $[N^p, G] \leq Z(G)$. Elég azt megmutatni, hogy $[N^p, G] = 1$, ami ellentmond az előző feltételeknek.

Vezessük be az $[a, b, c] = [[a, b], c]$ jelölést. Legyen $x \in N$ és $g \in G$. Ekkor $[x, g] \in N^p$, ezért $[x, g, x] \in Z(G)$. A 2.4.5. lemma miatt

$$\begin{aligned} [x^p, g] = x^{-p}(x^p)^g = x^{-p}(x^g)^p = x^{-p}(x[x, g])^p = \\ = x^{-p}x^p[x, g]^p[x, g, x]^{p(p-1)/2} = [x, g]^p[x, g, x]^{p(p-1)/2}. \end{aligned} \qquad (*)$$

$p > 2$ esetén $[x, g], [x, g, x] \in N^p$ és $p \mid \frac{p(p-1)}{2}$, emiatt $[x^p, g] = 1$.

Ha $p = 2$, akkor legyen $y \in N$ tetszőleges. A $(*)$ egyenletbe $x = y^2$-et helyettesítve

$$[y^4, g] = [y^2, g]^2[y^2, g, y^2].$$

Mivel $[y^2, g] \in [N^2, G] \cong Z_2$, következik, hogy $[y^2, g]^2 = [y^2, g, y^2] = 1$, tehát $[y^4, g] = 1$. Ez minden g-re igaz, ezért $N^4 \leq Z(G)$.

A $(*)$ egyenlet szerint

$$[x^2, g] = [x, g]^2[x, g, x] = [x, g]^2,$$

felhasználva, hogy $[x, g] \in N^4 \leq Z(G)$. Emiatt elég azt igazolnunk, hogy $(N^4)^2 = 1$. Ehhez vegyük észre, hogy az $x \mapsto x^2$ egy $N^4 \twoheadrightarrow (N^4)^2$ epimorfizmus az N^4 kommutativitása miatt. Az N^4-t generálják az x^4 alakú elemek ($x \in N$), ezért az $(N^4)^2$-et generálják az $(x^4)^2 = x^8$ alakúak. Tehát

$$(N^4)^2 = N^8 \leq (N^2)^4 = 1.$$

□

2.4.7. Következmény. *Ha G végesen generált pro-p-csoport, és N p.e. G, akkor $\overline{N^p}$ p.e. G.*

Bizonyítás. A 2.1.8. állítás miatt N végesen generált, ezért a 2.3.1. és 2.4.3. állítás következtében az $\overline{N^p}$ nyílt. A 2.4.4. és 2.4.6. állítás miatt készen vagyunk, mert $\overline{N^p}K/K = (NK/K)^p$, ha $K \lhd_o G$. □

A szakasz hátralévő részében a $G_i = P_i(G)$ jelölést alkalmazzuk, ha G végesen generált hatványteljes pro-p-csoport.

2.4.8. Tétel. *Ha G végesen generált hatványteljes pro-p-csoport, akkor G_i p.e. G minden $i \geq 1$-re.*

Bizonyítás. i szerinti indukcióval bizonyítjuk. $G_1 = G$, ezért $i = 1$-re az állítás triviális. Ha G_i *p.e.* G, akkor

$$G_i^p[G_i, G] \leq \overline{G_i^p} = \overline{G_i^p[G_i, G]},$$

ezért $G_{i+1} = \overline{G_i^p}$, ami a 2.4.7. állítás miatt hatványteljesen van beágyazva. □

2.4.9. Következmény. $G_{i+1} = \Phi(G_i)$.

2.4.10. Következmény. $P_{k+1}(G_i) = G_{i+k}$.

Legyen N normálosztó. Vezessük be az $x \equiv y \pmod N$ jelölést arra, hogy $xN = yN$.

2.4.11. Lemma. *Ha $x \in G$ és $y \in G_i$, akkor*

$$(xy)^p \equiv x^p y^p \pmod{G_{i+2}}$$

Bizonyítás. A 2.2.12. állítás miatt G_{i+2}-vel faktorizálhatunk, így feltehető, hogy G_{i+2}=1. Ekkor $[G_{i+1}, G]$=1, tehát $G_{i+1} \leq Z(G)$. $[y, x] \in [G_i, G] \leq G_{i+1}$, ezért a 2.4.5. lemma szerint

$$(xy)^p = x^p y^p [y, x]^{p(p-1)/2},$$

így elég azt megmutatni, hogy $[y, x]^{p(p-1)/2} \in G_{i+2}$. A $p > 2$ esetben ez következik abból, hogy $p \mid \frac{p(p-1)}{2}$ és $[y, x] \in G_{i+1}$. Ha $p = 2$, akkor

$$[y, x] \in G_i^4 \leq (G_i^2)^2 \leq G_{i+2}.$$

□

2.4.12. Állítás. *Az $x \mapsto x^p$ leképezés egy $G_i/G_{i+1} \twoheadrightarrow G_{i+1}/G_{i+2}$ epimorfizmust indukál.*

Bizonyítás. A 2.4.11. lemmából egy $G_i \to G_{i+1}/G_{i+2}$ homomorfizmus adódik, ami szürjektív, mert $G_{i+1} = \overline{G_i^p} \leq G_i^p G_{i+2}$. A G_{i+1} képe triviális, mert $G_{i+1}^p \leq G_{i+2}$, így a G_i/G_{i+1}-en is jóldefiniált a homomorfizmus. □

2.4.13. Következmény. *Az $x \mapsto x^{p^k}$ egy $G_i/G_{i+1} \twoheadrightarrow G_{i+k}/G_{i+k+1}$ epimorfizmust indukál minden $k \geq 0$-ra és $i \geq 1$-re.*

2.4.14. Állítás. *A G^p minden g eleme előáll x^p alakban.*

Bizonyítás. Rekurzívan definiálunk egy $(x_i)_{i \geq 0}$ sorozatot, amelyre

$$x_i^p \equiv g \pmod{G_{i+1}}.$$

Az x_0-t tetszőlegesen megválaszthatjuk. Legyen $x_{i+1} = x_i y_i$ alakú, ahol $y_i \in G_i$. Ekkor a 2.4.11. lemma miatt

$$x_{i+1}^p \equiv x_i^p y_i^p \pmod{G_{i+2}}.$$

A 2.4.12. állítás miatt y_i megválasztható úgy, hogy

$$y_i^p \equiv x_i^{-p} g \pmod{G_{i+2}},$$

mivel $x_i^{-p} g \in G_{i+1}$. Ekkor teljesül a feltétel.

Ha $i \leq n < m$, akkor

$$x_n^{-1} x_m = y_n \cdots y_{m-1} \in G_i.$$

A 2.3.4. állítás miatt az (x_i)-re alkalmazhatjuk a Cauchy-kritériumot, így $x_i \to x$ valamilyen x-re. Ekkor a G/G_i-be menő faktorleképezés folytonossága miatt

$$x^p = \lim_{n \to \infty} x_n^p \equiv g \pmod{G_i}$$

minden i-re, így a 2.3.4. állítást ismét alkalmazva $x^p = g$. □

2.4.15. Következmény.

$$G_{i+k} = \left\{ x^{p^k} \;\middle|\; x \in G_i \right\} = G_i^{p^k}.$$

Bizonyítás. A kompaktság miatt a $G_i^p = \{x^p \mid x \in G_i\}$ zárt, ezért $G_{i+1} = \overline{G_i^p} = G_i^p$. A bizonyítandó állítás k szerinti indukcióval könnyen látható. □

2.4.16. Állítás. *Legyen $a_1, \dots, a_d$ a G-nek egy topologikus generátorrendszere. Ekkor minden $g \in G$ előáll*

$$g = a_1^{\lambda_1} \cdots a_d^{\lambda_d}$$

alakban, ahol $\lambda_1, \dots, \lambda_d \in \mathbb{Z}_p$.

Bizonyítás. Rekurzívan definiáljuk az $(n_{j,i})_{i \geq 0}$ sorozatokat úgy, hogy a

$$g_i = a_1^{n_{1,i}} \cdots a_d^{n_{d,i}} \equiv g \pmod{G_{i+1}}$$

feltétel minden i-re teljesüljön. Az $a_{j,0}$-t tetszőlegesen megválaszthatjuk.

Most legyen $i \geq 0$. Legyen $n_{j,i+1} = n_{j,i} + p^i k_{j,i}$ alakú. $a_j^{p^i} \in G_{i+1}$, ezért az $a_j^{p^i}$ képe centrális a G/G_{i+2}-ben. Emiatt

$$g_{i+1} = a_1^{n_{1,i+1}} \cdots a_d^{n_{d,i+1}} = a_1^{n_{1,i}} a_1^{p^i k_{j,i}} \cdots a_d^{n_{d,i}} a_d^{p^i k_{j,i}} \equiv g_i a_1^{p^i k_{1,i+1}} \cdots a_d^{p^i k_{d,i+1}} \pmod{G_{i+2}}.$$

A 2.4.13. állítás miatt az $a_j^{p^i} G_{i+2}/G_{i+2}$ alakú elemek generálják a G_{i+1}/G_{i+2}-t. A G_{i+1}/G_{i+2} kommutatív, ezért található olyan $k_{1,i+1}, \dots, k_{d,i+1}$, amelyre

$$a_1^{p^i k_{1,i+1}} \cdots a_d^{p^i k_{d,i+1}} \equiv g_i^{-1} g \pmod{G_{i+2}}.$$

Ebből már következik, hogy

$$g_{i+1} \equiv g \pmod{G_{i+2}}.$$

Látható, hogy ha $n, m \geq i$, akkor $p^i \mid n_{j,n} - n_{j,m}$. Emiatt

$$\lim_{n \to \infty} n_{j,n} = \lambda_j \in \mathbb{Z}_p.$$

A g_n definíciójából világos, hogy

$$g = \lim_{n \to \infty} g_n \equiv \lim_{n \to \infty} a_1^{n_{1,n}} \cdots a_d^{n_{d,n}} = a_1^{\lambda_1} \cdots a_d^{\lambda_d} \pmod{G_{i+1}}$$

minden i-re, tehát $g = a_1^{\lambda_1} \cdots a_d^{\lambda_d}$. □

2.5. Egyenletes csoportok

2.5.1. Definíció. Legyen G végesen generált hatványteljes pro-p-csoport, és legyen $G_i = P_i(G)$. A G *egyenletes*, ha a $|G_i : G_{i+1}|$ minden i-re azonos.

2.5.2. Állítás. *A G végesen generált hatványteljes pro-p-csoport pontosan akkor egyenletes, ha az $x \mapsto x^p$ egy $G_i/G_{i+1} \xrightarrow{\sim} G_{i+1}/G_{i+2}$ izomorfizmust indukál minden i-re.*

Bizonyítás. A 2.4.12. állításból nyilvánvaló. □

2.5.3. Következmény. *Legyen G egyenletes, és legyen $a_1, \dots, a_d$ minimális topologikus generátorrendszer. Ekkor tetszőleges i-re az $a_1^{p^{i-1}}, \dots, a_d^{p^{i-1}}$ minimális topologikus generátorrendszere G_i-nak.*

Bizonyítás. Az előző állítás miatt az $x \mapsto x^{p^{i-1}}$ egy $G/G_2 \xrightarrow{\sim} G_i/G_{i+1}$ izomorfizmust indukál. A 2.2.10 állítás szerint $a_1, \dots, a_d$ bázisa a G/G_2-nak, ezért az $a_1^{p^{i-1}}, \dots, a_d^{p^{i-1}}$ bázisa a G_i/G_{i+1}-nek, tehát minimális topologikus generátorrendszer. □

2.5.4. Állítás. *Ha G végesen generált hatványteljes pro-p-csoport, akkor elég nagy i-re a G_i egyenletes.*

Bizonyítás. A 2.4.12. állítás miatt $|G_i:G_{i+1}| \geq |G_{i+1}:G_{i+2}|$. Ez egy pozitív egészekből álló monoton csökkenő sorozat, ezért elég nagy i-re $|G_i : G_{i+1}|$ állandó. A 2.4.10. állítás következtében a G_i egyenletes, ha i elég nagy. □

2.5.5. Tétel. *Egy végesen generált hatványteljes pro-p-csoport akkor és csak akkor egyenletes, ha torziómentes.*

Bizonyítás. Legyen G egyenletes, és tegyük fel, hogy x rendje $n > 1$. Ha $p \nmid n$, akkor az xG_i/G_i rendje n osztója, ezért $x \in G_i$ minden i-re. Ebből következik, hogy $x = 1$, ami ellentmondás. Emiatt $p \mid n$, ezért az $x^{n/p}$-re áttérve feltehető, hogy x rendje p.

$x \neq 1$, ezért a 2.3.4. állítás miatt x nem lehet minden G_i-ben. Így van olyan i, amelyre $x \in G_i \setminus G_{i+1}$. A 2.5.2. állítás miatt $x^p \in G_{i+1} \setminus G_{i+2}$, ami ellentmondás, mert $x^p = 1$. Ezzel beláttuk, hogy G torziómentes.

Most vegyünk egy olyan G-t, ami nem egyenletes. Ekkor valamilyen i-re az $x \mapsto x^p$, $G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ leképezés nem injektív. A 2.4.10. állítás miatt a G-t lecserélhetjük G_i-re, így feltehető, hogy $i = 1$. Ekkor van olyan x_2, amelyre $x_1^p \in G_3$, de $x_i \notin G_2$.

Az (x_n) sorozatot folytassuk úgy, mint a 2.4.14. állítás bizonyításában $g = 1$ esetén. Ekkor $x_n \to x$, $x^p = 1$, és $x_n \equiv x_2 \pmod{G_2}$ minden $n \geq 2$-re. Így $x \equiv x_2 \pmod{G_2}$, ezért $x \notin G_2$. Emiatt $x \neq 1$, tehát G nem torziómentes. □

2.5.6. Tétel. *Legyen G egyenletes, és legyen $a_1, \ldots, a_d$ egy minimális topologikus generátorrendszere. Ekkor minden $g \in G$ egyértelműen áll elő*

$$g = a_1^{\lambda_1} \cdots a_d^{\lambda_d}$$

alakban, ahol $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}_p$.

Bizonyítás. A 2.4.16. állítás szerint minden elem előáll, elég az egyértelműséget igazolni. A 2.2.10. tétel miatt $|G : G_2| = p^d$, ezért $|G_i : G_{i+1}| = p^d$ minden i-re.

Legyen $k \geq 1$ tetszőleges. A $b_j = a_j G_{k+1}/G_{k+1}$ elemekre teljesül, hogy a G/G_{k+1} minden eleme előáll $h = b_1^{\lambda_1} \cdots b_d^{\lambda_d}$ alakban. A $G/G_{k+1} = G/G^{p^k}$ csoportban minden elem p^k-adik hatványa az egységelem, emiatt csak a $\lambda_j \bmod p^k$-tól függ a h értéke. Ezek együtt p^{kd}-félék lehetnek. Vegyük észre, hogy $|G : G_{k+1}| = p^{kd}$, amiből következik a $\lambda_j \bmod p^k$ egyértelműsége. Ez minden k-ra igaz, ezért a λ_j-k is egyértelműek. □

2.5.7. Következmény. *Legyen $a_1, \ldots, a_d$ a G egyenletes csoport minimális topologikus generátorrendszere. Ekkor a*

$$(\lambda_1, \ldots \lambda_d) \mapsto a_1^{\lambda_1} \cdots a_d^{\lambda_d}$$

egy $\mathbb{Z}_p^d \to G$ homeomorfizmus.

Bizonyítás. A bijektivitást az előbb láttuk. A folytonosság a 2.2.5. állításból könnyen látható. Mivel a $\mathbb{Z}_p^d$ kompakt, és a G Hausdorff-tér, ebből már következik, hogy a leképezés homeomorfizmus. □

3. p-adikus Lie-csoportok

3.1. Analitikus sokaságok

3.1.1. Definíció. Legyen M topologikus tér, és $d \geq 0$ rögzített. Egy $\varphi : U \to V$ leképezést *térképnek* nevezünk, ha homeomorfizmus az $U \subseteq M$ és $V \subseteq \mathbb{Z}_p^d$ nyílt részhalmazok között.

A $\varphi_1 : U_1 \to V_1$ és $\varphi_2 : U_2 \to V_2$ térképek *kompatibilisek*, ha a

$$\varphi_2 \circ \varphi_1^{-1} : \varphi_1(U_1 \cap U_2) \to \varphi_1(U_1 \cap U_2),$$

illetve a

$$\varphi_1 \circ \varphi_2^{-1} : \varphi_2(U_1 \cap U_2) \to \varphi_2(U_1 \cap U_2)$$

áttérési leképezések analitikusak.

Atlasznak nevezzük térképeknek egy $\mathcal{A} = \{(U_i, \varphi_i) \mid i \in I\}$ halmazát, ha $\bigcup U_i = M$, és bármely két φ_i kompatibilis. Két atlasz *ekvivalens*, ha az uniójuk is atlasz.

Az $(M, \mathcal{A})$ *p-adikus analitikus sokaság*, ha $\mathcal{A}$ atlasz M-en.

A továbbiakban sokaság alatt p-adikus analitikus sokaságot értünk.

3.1.2. Definíció. Legyen $(M, \mathcal{A})$ és $(N, \mathcal{B})$ két sokaság. Egy $f : M \to N$ leképezés *analitikus*, ha minden $(U, \varphi) \in \mathcal{A}$ és $(V, \psi) \in \mathcal{B}$ esetén $f^{-1}(V)$ nyílt, továbbá a $\psi \circ f \circ \varphi^{-1}$ leképezés analitikus $\varphi(U \cap f^{-1}(V))$-n.

3.1.3. Állítás. *Tegyük fel, hogy $f : M \to N$ és $g : N \to K$ analitikusak, ahol $(M, \mathcal{A})$, $(N, \mathcal{B})$ és $(K, \mathcal{C})$ sokaságok. Ekkor a $g \circ f : M \to K$ is analitikus.*

Bizonyítás. Legyen $(U, \varphi) \in \mathcal{A}$ és $(W, \theta) \in \mathcal{C}$ tetszőleges. Ekkor minden $x \in U \cap (g \circ f)^{-1}(W)$-hez van olyan $(V, \psi) \in \mathcal{B}$, amelyre $f(\varphi(x)) \in V$. Ellenőrizhető, hogy

$$\theta \circ (g \circ f) \circ \varphi_1^{-1} = (\theta \circ g \circ \psi^{-1}) \circ (\psi \circ f \circ \varphi^{-1})$$

ott, ahol minden értelmezve van, azaz a $D = \varphi(U \cap f^{-1}(V \cap g^{-1}(W)))$-n. Az f és g analitikussága miatt D nyílt. Így az x-nek egy $\varphi^{-1}(D) \subseteq U \cap (g \circ f)^{-1}(W)$ környezetét kaptuk. A lehetséges U-k lefedik M-et, ezért a $(g \circ f^{-1})(W)$ nyílt.

Az 1.4.13. állításból következik, hogy a $\theta \circ (g \circ f) \circ \varphi^{-1}$ analitikus a D-n, speciálisan a $\varphi(x)$-ben is analitikus. Ez minden x-re igaz, emiatt az egész $\varphi(U \cap (g \circ f)^{-1}(W))$-n analitikus. □

3.1.4. Állítás. *Az M-en az $\mathcal{A}_1$ és $\mathcal{A}_2$ atlaszok akkor és csak akkor ekvivalensek, ha az $f : (M, \mathcal{A}_1) \to (M, \mathcal{A}_2)$ identikus leképezés analitikus, és f^{-1} is analitikus.*

Bizonyítás. Ha $(U_1, \varphi_1) \in \mathcal{A}_1$ és $(U_2, \varphi_2) \in \mathcal{A}_2$, akkor a φ_1 és φ_2 pontosan akkor kompatibilisek, ha a

$$\varphi_2 \circ \varphi_1^{-1} = \varphi_2 \circ f \circ \varphi_1^{-1},$$

illetve a

$$\varphi_1 \circ \varphi_2^{-1} = \varphi_1 \circ f^{-1} \circ \varphi_2^{-1}$$

analitikusak az értelmezési tartományukon. Az f homeomorfizmus, ezért ezek ekvivalensek f, illetve f^{-1} analitikusságával. □

3.1.5. Következmény. *Az atlaszok ekvivalenciája ekvivalenciareláció.*

Bizonyítás. A reflexivitás és a szimmetria nyilvánvaló. A tranzitivitáshoz elég, ha a 3.1.4. állításban szereplő leképezések kompozíciója analitikus, ami a 3.1.3. állításból következik. □

Látható, hogy ha $f : M \to N$ analitikus valamilyen atlaszokkal, akkor ekvivalens atlaszokra való áttéréskor az f-et analitikus leképezésekkel komponáljuk, így továbbra is analitikus marad. Emiatt az ekvivalens atlaszokhoz tartozó sokaságstruktúrákat azonosnak tekintjük. Egy leképezést akkor tekintünk térképnek, ha M bármelyik atlasza tartalmazza. Az összes ilyen térkép egy atlaszt alkot, ezt M *maximális atlaszának* nevezzük.

A sokaságokra az egyik legegyszerűbb példa a $\mathbb{Q}_p^r$. Ezen a $\varphi_{\mathbf{x}} : \mathbf{x} + \mathbb{Z}_p^r \to \mathbb{Z}_p^r$, $\varphi_{\mathbf{x}}(\mathbf{x}+\mathbf{y}) = \mathbf{y}$ leképezések a térképek. Nyilvánvaló, hogy ezek a térképek kompatibilisek, hiszen az áttérési leképezések eltolások.

Ha az M sokaságnak N nyílt részhalmaza, akkor N-en is megadható egy sokaságstruktúra. Ha (U, φ) térkép M-en, akkor az $(U \cap N, \varphi|_{U\cap N})$ térkép N-en, ezek egy atlaszt alkotnak.

3.1.6. Definíció. Legyen M és N két sokaság $\mathcal{A}$, illetve $\mathcal{B}$ atlasszal. Az M és N *szorzata* az $M \times N$ szorzattér az $\{(U \times V, \varphi \times \psi) \mid (U, \varphi) \in \mathcal{A}, (V, \psi) \in \mathcal{B}\}$ atlasszal, ahol $(\varphi \times \psi)(x, y) = (\varphi(x), \psi(y))$.

3.1.7. Definíció. Legyen G olyan topologikus csoport, amin adott egy sokaságstruktúra. A G *p-adikus Lie-csoport* (más néven *p-adikus analitikus csoport*), ha az $(x, y) \mapsto xy$ és $x \mapsto x^{-1}$ leképezések analitikusak.

3.1.8. Lemma. *Tegyük fel, hogy G topologikus csoport és sokaság. Ekkor G pontosan akkor Lie-csoport, ha az $(x, y) \mapsto xy^{-1}$ leképezés analitikus.*

Bizonyítás. Ha G Lie-csoport, akkor az $y \mapsto y^{-1}$ analitikus. ezért az $(x, y) \mapsto (x, y^{-1})$ is analitikus. Ebből következik, hogy $(x, y) \mapsto xy$-nal való kompozíciója, az $(x, y) \mapsto xy^{-1}$ is analitikus.

Most tegyük fel, hogy az $(x, y) \mapsto xy^{-1}$ analitikus. Az $y \mapsto (1, y)$ analitikus, ezért az $y \mapsto y^{-1}$ is analitikus. Emiatt az $xy = x(y^{-1})^{-1}$ is analitikus. □

3.1.9. Lemma. *Legyen G topologikus csoport, és $H \leq_o G$ Lie-csoport. Tegyük fel, hogy minden $g \in G$-re van olyan $V_g \leq_o H$, amelyre $V_g^g \leq H$, és a*

$$V_g \to H, \quad h \mapsto h^g$$

leképezés analitikus. Ekkor a H sokaságstruktúrája kiterjeszthető G-re úgy, hogy G is Lie-csoport legyen.

Bizonyítás. Legyen $\varphi : U \to V$ egy térkép H-n, és legyen $g \in G$ tetszőleges. Ekkor a $\varphi_g : gU \to V$, $\varphi_g(x) = \varphi(g^{-1}x)$ térkép. Legyenek φ_g és ψ_h ilyen térképek, ekkor

$$\varphi_g(\psi_h^{-1}(y)) = \varphi(g^{-1}h\psi^{-1}(y))$$

ott, ahol ez értelmezve van. Ha van ilyen y, akkor $g^{-1}h \in H$, ezért az $x \mapsto g^{-1}hx$ analitikus H-n. Ebből következik, hogy a $\varphi_g \circ \psi_h^{-1}$ analitikus, tehát φ_g és ψ_h kompatibilisek. A φ_g alakú térképek értelmezési tartományai lefedik G-t, ezért G-nek egy atlaszát alkotják. Tetszőleges φ-re $\varphi_1 = \varphi$, ezért a H sokaságstruktúrájának egy kiterjesztését kaptuk.

A 3.1.8. lemma felhasználásával igazoljuk, hogy G Lie-csoport. Azt kell megmutatnunk, hogy az $(x, y) \mapsto xy^{-1}$ analitikus minden (g, h)-nak valamilyen környezetében. Legyen $x \in gV_{h^{-1}}$ és $y \in hV_{h^{-1}}$. Ekkor

$$xy^{-1} = g(g^{-1}x)(h^{-1}y)^{-1}h^{-1} = gh^{-1}\big((g^{-1}x)(h^{-1}y)^{-1}\big)^{h^{-1}}.$$

Ellenőrizhető, hogy $(g^{-1}x)(h^{-1}y)^{-1} \in V_{h^{-1}}$. A φ_g definíciójából világos, hogy az $x \mapsto gx$ analitikus H-n, illetve az $x \mapsto g^{-1}x$ analitikus gH-n. Ennek következtében az $(x, y) \mapsto xy^{-1}$ analitikus a $gV_{h^{-1}} \times hV_{h^{-1}}$ nyílt halmazon. □

Megjegyzés. Nem nehéz belátni, hogy a φ_g-k mindenképp térképei G-nek, ebből következik a kiterjesztés egyértelműsége.

3.1.10. Tétel. *Egy topologikus csoporton akkor és csak akkor adható meg olyan sokaságstruktúra, amellyel p-adikus Lie-csoport, ha nyílt részcsoportként tartalmaz egyenletes pro-p-csoportot.*

A dolgozat hátralévő részében a 3.1.10. tételt bizonyítjuk. A 3.2. szakaszban először megmutatjuk, hogy minden p-adikus Lie-csoport tartalmaz úgynevezett *standard csoportot*, majd belátjuk, hogy minden standard csoport egyenletes. A 3.3. szakaszban azt fogjuk igazolni, hogy a 2.5.7. állításban szereplő homeomorfizmussal olyan globális térképet kaphatunk egy G egyenletes csoporton, amellyel a csoportműveletek analitikusak. Ehhez a $\mathbb{Q}_pG$ csoportalgebrán definiálunk egy normát, majd a csoportalgebrában számolva megmutatjuk, hogy a csoportműveletek felírhatóak hatványsor alakban.

Megjegyzés. Az előző tételnél egy erősebb állítás is igaz: egy egyenletes pro-p-csoporton pontosan egy sokaságstruktúra van, amellyel Lie-csoport. A sokaságstruktúra egyértelműen terjeszthető ki, ennek következtében egy topologikus csoporton legfeljebb egyféle sokaságstruktúra adható meg.

3.2. Standard csoportok

Legyen $\varepsilon = 1$, ha $p > 2$, és legyen $\varepsilon = 2$, ha $p = 2$.

3.2.1. Definíció. Legyen G egy p-adikus Lie-csoport. A G *standard csoport*, ha van olyan $\psi : G \to p^{\varepsilon}\mathbb{Z}_p^d$ homeomorfizmus, hogy a $\{(G, \psi)\}$ a G-nek egy atlasza, illetve van olyan $\mathbf{P} = (P_1, \dots, P_d)$, $P_i \in \mathbb{Z}_p[[\mathbf{x}, \mathbf{y}]]$, hogy minden $g, h \in G$-re

$$\psi(gh^{-1}) = \mathbf{P}(\psi(g), \psi(h)).$$

3.2.2. Lemma. *Legyen $\mathbf{P} = (P_1, \dots, P_d)$, $P_i \in \mathbb{Q}_p[[\mathbf{x}, \mathbf{y}]]$, és tegyük fel, hogy elég kicsi $\mathbf{x}$-re $\mathbf{P}(\mathbf{x}, \mathbf{0}) = \mathbf{x}$ és $\mathbf{P}(\mathbf{x}, \mathbf{x}) = \mathbf{0}$. Ekkor*

$$P_i(\mathbf{x}, \mathbf{y}) = x_i - y_i + \sum_{\langle\alpha\rangle+\langle\beta\rangle\geq 2} a_{i,\alpha,\beta}\mathbf{x}^{\alpha}\mathbf{y}^{\beta}$$

alakú.

Bizonyítás. Legyen $P_i(\mathbf{x}, \mathbf{y}) = \sum_{\alpha,\beta} a_{i,\alpha,\beta}\mathbf{x}^{\alpha}\mathbf{y}^{\beta}$. Jelöljük ε_i-vel azt a d hosszú vektort, amelynek a j. komponense a $\delta_{i,j}$ Kronecker-delta. Ha $\mathbf{y}$ helyére $\mathbf{0}$-t helyettesítünk, akkor az 1.4.3. állításból következik, hogy $a_{i,\mathbf{0},\mathbf{0}} = 0$, és $a_{i,\varepsilon_j,\mathbf{0}} = \delta_{i,j}$.

Az 1.4.8. állítást felhasználva látható, hogy ha $t \in \mathbb{Z}_p$ elég kicsi, akkor tetszőleges i, j-re

$$0 = P_i(t\varepsilon_j, t\varepsilon_j) = \sum_{n=0}^{\infty}\left(\sum_{k+m=n} a_{i,k\varepsilon_j,m\varepsilon_j}\right)t^n,$$

így az 1.4.3. állítás miatt $a_{i,\varepsilon_j,\mathbf{0}} + a_{i,\mathbf{0},\varepsilon_j} = 0$, vagyis $a_{i,\mathbf{0},\varepsilon_j} = -\delta_{i,j}$. Ezzel a bizonyítandó állítást kaptuk. □

3.2.3. Tétel. *Minden p-adikus Lie-csoport tartalmaz nyílt standard részcsoportot.*

Bizonyítás. Legyen (U, φ) egy térkép az egységelem körül. Eltolással elérhető, hogy $\varphi(1)=\mathbf{0}$ legyen. A $(g, h)\mapsto gh^{-1}$ analitikus a $(\mathbf{0}, \mathbf{0})$-ban, ezért van olyan $\mathbf{P}$ hatványsorokból álló vektor, és a $(\mathbf{0}, \mathbf{0})$-nak egy V környezete, hogy

$$\varphi(\varphi^{-1}(\mathbf{x})\varphi^{-1}(\mathbf{y})^{-1}) = \mathbf{P}(\mathbf{x}, \mathbf{y}),$$

ha $(\mathbf{x}, \mathbf{y}) \in V$. $\mathbf{P}$-re teljesülnek a 3.2.2. lemma feltételei, ezért

$$P_i(\mathbf{x}, \mathbf{y}) = x_i - y_i + \sum_{\langle\alpha\rangle+\langle\beta\rangle\geq 2} a_{i,\alpha,\beta}\mathbf{x}^{\alpha}\mathbf{y}^{\beta}.$$

Az 1.4.2. lemma miatt van olyan $K > 1$, hogy minden i, α, β esetén $|a_{i,\alpha,\beta}|_p \leq K^{\langle\alpha\rangle+\langle\beta\rangle+1}$. Legyen k olyan nagy, hogy $p^{k-\varepsilon} \geq K^3$ és $p^k\mathbb{Z}_p^{2d} \subseteq V$. Ekkor $\langle\alpha\rangle + \langle\beta\rangle \geq 2$ esetén

$$|a_{i,\alpha,\beta}|_p \leq K^{\langle\alpha\rangle+\langle\beta\rangle+1} \leq K^{3(\langle\alpha\rangle+\langle\beta\rangle-1)} \leq p^{(k-\varepsilon)(\langle\alpha\rangle+\langle\beta\rangle-1)}. \qquad (*)$$

Ha $\mathbf{x}, \mathbf{y} \in p^k\mathbb{Z}_p^d$, akkor

$$\left|a_{i,\alpha,\beta}\mathbf{x}^{\alpha}\mathbf{y}^{\beta}\right|_p \leq p^{(k-\varepsilon)(\langle\alpha\rangle+\langle\beta\rangle-1)}p^{-k(\langle\alpha\rangle+\langle\beta\rangle)} \leq p^{k(\langle\alpha\rangle+\langle\beta\rangle-1)}p^{-k(\langle\alpha\rangle+\langle\beta\rangle-1)}p^{-k} = p^{-k},$$

így az 1.2.3. állítás miatt $\mathbf{P}(\mathbf{x},\mathbf{y}) \in p^k\mathbb{Z}_p^d$. Ez azt jelenti, hogy a $p^k\mathbb{Z}_p^d$ zárt a $\mathbf{P}$-re, tehát a $H = \varphi^{-1}(p^k\mathbb{Z}_p^d)$ nyílt részcsoport.

Legyen $\psi : H \to p^\varepsilon\mathbb{Z}_p^d$, $\psi(g) = p^{-k+\varepsilon}\varphi(g)$. Világos, hogy ψ homeomorfizmus. Az is könnyen ellenőrizhető, hogy ψ a sokaságstruktúrával kompatibilis térkép. Tetszőleges $\mathbf{x},\mathbf{y} \in p^\varepsilon\mathbb{Z}_p^d$ esetén

$$\psi(\psi^{-1}(\mathbf{x})\psi^{-1}(\mathbf{y})^{-1}) = p^{-k+\varepsilon}\varphi(\varphi^{-1}(p^{k-\varepsilon}\mathbf{x})\varphi^{-1}(p^{k-\varepsilon}\mathbf{y})^{-1}) = p^{-k+\varepsilon}\mathbf{P}(p^{k-\varepsilon}\mathbf{x}, p^{k-\varepsilon}\mathbf{y}).$$

Legyen $\tilde{\mathbf{P}}(\mathbf{x},\mathbf{y}) = p^{-k+\varepsilon}\mathbf{P}(p^{k-\varepsilon}\mathbf{x}, p^{k-\varepsilon}\mathbf{y})$, ekkor minden $g,h \in H$-ra $\psi(gh^{-1}) = \tilde{\mathbf{P}}(\psi(g),\psi(h))$. Bármely i-re

$$\tilde{P}_i(\mathbf{x},\mathbf{y}) = x_i - y_i + \sum_{\langle\alpha\rangle+\langle\beta\rangle\geq 2} p^{(k-\varepsilon)(\langle\alpha\rangle+\langle\beta\rangle-1)} a_{i,\alpha,\beta}\mathbf{x}^\alpha\mathbf{y}^\beta.$$

A $(*)$ egyenlőtlenségből következik, hogy $\tilde{\mathbf{P}}_i \in \mathbb{Z}_p[[\mathbf{x},\mathbf{y}]]$. □

A továbbiakban legyen G standard csoport ψ térképpel, és legyen $\mathbf{P}$ olyan, hogy $\psi(gh^{-1}) = \mathbf{P}(\psi(g),\psi(h))$.

3.2.4. Lemma. *Legyen $g \in G$, és tegyük fel, hogy valamilyen $k \geq 1$-re $\psi(g) \in p^k\mathbb{Z}_p^d$. Ekkor*

$$\psi(g^p) \equiv p\,\psi(g) \pmod{p^{k+2}}.$$

Bizonyítás. Az 1.4.9. állítás miatt a $\mathbf{Q}(\mathbf{x},\mathbf{y}) = \mathbf{P}(\mathbf{x},\mathbf{P}(\mathbf{0},\mathbf{y}))$ minden komponense $\mathbb{Z}_p[[\mathbf{x},\mathbf{y}]]$-beli, és $\mathbf{Q}$ konvergens a $p\mathbb{Z}_p^{2d}$-n. Így minden $g,h \in G$-re $\psi(gh) = \mathbf{Q}(\psi(g),\psi(h))$. Ha $\langle\alpha\rangle + \langle\beta\rangle \geq 3$ és $\mathbf{x},\mathbf{y} \in p^k\mathbb{Z}_p^d$, akkor $\mathbf{x}^\alpha\mathbf{y}^\beta \in$ $\in p^{3k}\mathbb{Z}_p \subseteq p^{k+2}\mathbb{Z}_p$. Emiatt elég $\mathbf{Q}$-nak a legfeljebb másodfokú tagjait vizsgálni. Mivel $\mathbf{Q}(\mathbf{x},\mathbf{0}) = \mathbf{Q}(\mathbf{0},\mathbf{x}) = \mathbf{x}$, a 3.2.2. lemma miatt

$$Q_i(\mathbf{x},\mathbf{y}) \equiv x_i + y_i + \sum_{j,l} a_{i,j,l}x_jy_l \pmod{p^{k+2}}$$

minden $\mathbf{x},\mathbf{y} \in p^k\mathbb{Z}_p^d$-re, ahol $a_{i,j,l} \in \mathbb{Z}_p$ konstans.

Megmutatjuk, hogy ha $\psi(g) = \mathbf{x}$, akkor minden $n \geq 1$-re

$$\psi_i(g^n) \equiv nx_i + \sum_{j,l} \frac{n(n-1)}{2} a_{i,j,l}x_jx_l \pmod{p^{k+2}}. \qquad (*)$$

Az $n = 1$ eset triviális. Ha n-re igaz a $(*)$ egyenlet, akkor

$$\psi_i(g^{n+1}) = Q_i(\mathbf{x},\psi(g^n)) \equiv x_i + \psi_i(g^n) + \sum_{j,l} a_{i,j,l}x_j\psi_l(g^n) \equiv$$

$$\equiv (n+1)x_i + \sum_{j,l} \frac{n(n-1)}{2} a_{i,j,l}x_jx_l + \sum_{j,l} na_{i,j,l}x_jx_l = (n+1)x_i + \sum_{j,l} \frac{(n+1)n}{2} a_{i,j,l}x_jx_l \pmod{p^{k+2}}$$

Itt felhasználtuk, hogy $x_j\psi_l(g^n) \equiv nx_jx_l$, ez azért teljesül, mert a harmadfokú tagok figyelmen kívül hagyhatóak.

Helyettesítsünk a $(*)$ egyenletbe $n = p$-t. Ha $p > 2$, akkor $p \mid \frac{p(p-1)}{2}$, ezért $\frac{p(p-1)}{2}x_jx_l \in p^{2k+1}\mathbb{Z}_p^d \subseteq p^{k+2}\mathbb{Z}_p^d$. A $p = 2$ esetben $x_j \in p^2\mathbb{Z}_p^d$, ezért $x_jx_l \in p^{k+2}\mathbb{Z}_p^d$. □

3.2.5. Tétel. *Minden standard csoport egyenletes.*

Bizonyítás. Mivel $\mathbf{P}$ konstans tagja $\mathbf{0}$, az 1.2.3. állításból adódik, hogy ha $\mathbf{x},\mathbf{y} \in p^k\mathbb{Z}_p^d$, akkor $\mathbf{P}(\mathbf{x},\mathbf{y}) \in p^k\mathbb{Z}_p^d$. Tehát a $G_k = \varphi^{-1}(p^{k-1+\varepsilon}\mathbb{Z}_p^d)$ minden $k \geq 1$-re részcsoport. A G_k-k az egységelemnek egy környezetbázisát alkotják, emellett G kompakt és Hausdorff, ezért provéges. Ha $H \leq_o G$, akkor H tartalmazza valamelyik G_k-t. A G_k indexe p-hatvány, így a H indexe is, tehát G pro-p-csoport.

Azt fogjuk igazolni, hogy $\overline{G_k^p} = G_{k+1}$ minden k-ra (ebből az is következik, hogy G_k normálosztó). Ha $g \in G_k$, akkor a 3.2.4. lemma miatt $g^p \in G_{k+1}$. A G_{k+1} zárt, ezért $\overline{G_k^p} \leq G_{k+1}$.

Legyen $g \in G_{k+1}$ tetszőleges. Legyen $h_0 = \psi^{-1}(p^{-1}\psi(g))$, ekkor $h_0 \in G_k$. A 3.2.4. lemma szerint

$$\psi(h_0^p) \equiv \psi(g) \pmod{p^{k+1+\varepsilon}},$$

A 3.2.2. lemma miatt

$$\psi(gh_0^{-p}) \equiv \psi(g) - \psi(h_0^p) \equiv 0 \pmod{p^{k+1+\varepsilon}},$$

vagyis $gh_0^{-p} \in G_{k+2}$. Ezt folytatva kapunk egy $h_0, h_1, \dots$ sorozatot, amelyre teljesül, hogy $h_n \in G_{k+n}$, és $gh_0^{-p} \cdots h_n^{-p} \in G_{k+n+2}$. Ebből következik, hogy

$$\psi(g) \equiv \psi(h_n^p \cdots h_0^p) \pmod{p^{k+n+1+\varepsilon}}.$$

Ez tetszőlegesen nagy n-re igaz, ezért $g \in \overline{G_k^p}$.

Most megmutatjuk, hogy G hatványteljes. Legyen $g, h \in G$ tetszőleges. A 3.2.2. lemmát és az 1.4.9. állítást felhasználva ellenőrizhető, hogy

$$\psi_i([g,h]) = -\psi_i(g) - \psi_i(h) + \psi_i(g) + \psi_i(h) + \sum_{\langle\alpha\rangle+\langle\beta\rangle\geq 2} a_{i,\alpha}\psi(g)^\alpha\psi(h)^\beta = \sum_{\langle\alpha\rangle+\langle\beta\rangle\geq 2} a_{i,\alpha}\psi(g)^\alpha\psi(h)^\beta$$

alakú, ahol $a_{i,\alpha} \in \mathbb{Z}_p$. $\psi(g), \psi(h) \in p\mathbb{Z}_p^d$, ezért ha $\langle\alpha\rangle + \langle\beta\rangle \geq 2$, akkor $\psi(g)^\alpha\psi(h)^\beta \in p^2\mathbb{Z}_p^d$. $p > 2$ esetén $[g,h] \in$ $\in G_2 = \overline{G^p}$, tehát G hatványteljes.

Ha $p = 2$, és még az is teljesül, hogy $g \in G_k$, akkor $\psi(g)^\alpha\psi(h)^\beta \in 2^{k+3}\mathbb{Z}_p^d$, ezért $[g,h] \in G_{k+2}$. Megmutatjuk, hogy ha $x \in G_{k+1}$, akkor minden $n > k$-ra van olyan $y \in G_k$, hogy $y^2 \equiv x \pmod{G_n}$. Az $n = k+1$ esetben az $y = 1$ teljesíti a feltételt. Tegyük fel, hogy n-re teljesül az állítás, azaz van olyan $y \in G_k$, hogy $y^2 \equiv x \pmod{G_n}$. Ekkor $y^{-2}x \in G_n$, így a 3.2.4. lemma miatt van olyan $z \in G_{n-1}$, hogy $z^2 \equiv y^{-2}x \pmod{G_{n+1}}$. $[z,y] \in G_{n+1}$, ezért

$$(yz)^2 = y^2z[z,y]z \equiv y^2z^2 \equiv x \pmod{G_{n+1}}.$$

Világos, hogy $yz \in G_k$. Ezzel megmutattuk, hogy $n+1$-re is igaz az állítás.

Ha $g, h \in G$, akkor $[g,h] \in G_3$, ezért elég nagy n-re van olyan $x \in G_2$, hogy $x^2 \equiv [g,h] \pmod{G_n}$, és hasonlóan van olyan $y \in G$, hogy $y^2 \equiv x \pmod{G_n}$. Ekkor $y^4 \equiv [g,h] \pmod{G_n}$. Az n tetszőlegesen nagy lehet, ezért $[g,h] \in \overline{G^4}$, ezzel megmutattuk, hogy G hatványteljes.

Egy hatványteljes csoportban $G_{i+1} = \overline{G_i^p}$, ezért a most definiált G_i-k megegyeznek a 2.4. szakaszban definiált G_i-kkel. $|G_i : G_{i+1}| = p^d$ minden i-re, tehát G egyenletes. □

3.2.6. Következmény. *Minden p-adikus Lie-csoport tartalmaz nyílt egyenletes pro-p-csoportot.*

3.3. Egyenletes csoport csoportalgebrája

3.3.1. Definíció. Legyen R kommutatív egységelemes gyűrű, és legyen G csoport. Az RG *csoportalgebra* a $\sum_{g\in G} a_g g$ alakú formális összegekből áll, ahol véges sok a_g nem nulla. Az összeadást a

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g)g,$$

a szorzást pedig a

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right)g$$

képlettel definiáljuk (ellenőrizhető, hogy ezek valóban RG-beli elemek). A fenti műveletekkel RG egy R feletti algebra.

Az RG-be R és G beágyazhatóak az $r \mapsto r \cdot 1$, illetve $g \mapsto 1 \cdot g$ képletekkel. Ezeket az elemeket egyszerűen r-rel, illetve g-vel jelöljük.

Rögzítsünk egy G egyenletes pro-p-csoportot. A $G \to G/G_k$ természetes homomorfizmus indukál egy

$$\mathbb{Z}_pG \to \mathbb{Z}_p(G/G_k)$$

homomorfizmust. Látható, hogy ennek a magja $I_k = (G_k - 1)$, a $\{g-1 \mid g \in G_k\}$ halmaz által generált ideál.

3.3.2. Állítás. $\bigcap_{k=1}^{\infty}(I_k + p^k\mathbb{Z}_pG) = 0$.

Bizonyítás. Egy $x \in \mathbb{Z}_pG \setminus \{0\}$-t felírható $\sum a_i g_i$ alakú véges összegként, ahol $a_i \in \mathbb{Z}_p$, $g_i \in G$, és a g_i-k páronként különbözőek. Feltehető, hogy $a_1 \neq 0$. A G Hausdorff-tulajdonsága és a 2.3.4. állítás miatt elég nagy k-ra bármely két g_iG_k/G_k különböző. Elég nagy k-ra az is teljesül, hogy $a_1 \notin p^k\mathbb{Z}_p$. Ha alkalmazzuk x-re a $G \to G/G_k$ és $\mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}$ természetes homomorfizmusok által indukált $\varphi : \mathbb{Z}_pG \to (\mathbb{Z}/p^k\mathbb{Z})(G/G_k)$ homomorfizmust, akkor a tagok nem vonódnak össze, ezért a g_1G_k/G_k együtthatója $a_1 \bmod p^k \neq 0$. Emiatt $\varphi(x) \neq 0$. Ellenőrizhető, hogy $\ker\varphi = I_k + p^k\mathbb{Z}_pG$, amiből következik, hogy $x \notin I_k + p^k\mathbb{Z}_pG$. □

3.3.3. Lemma. *Legyen P véges p-csoport. Ha $n \geq |P|$, akkor bármely $g_1, \ldots, g_n \in P$-re teljesül, hogy az $\mathbb{F}_pP$ csoportalgebrában*

$$(g_1 - 1) \cdots (g_n - 1) = 0.$$

Bizonyítás. Az $\mathbb{F}_pP$ csoportalgebra egy $\mathbb{F}_p$ feletti $d = |P|$ dimenziós vektortér. Rögzítsük egy bázisát, és legyen $\varphi(g) \in \mathrm{GL}(d,p)$ az $x \mapsto gx$ lineáris leképezés mátrixa. Ekkor $\varphi : P \to GL(d,p)$ homomorfizmus, ami egyértelműen kiterjed egy $\mathbb{F}_pP \to M_d(\mathbb{F}_p)$ gyűrűhomomorfizmussá. Így elég lenne azt megmutatni, hogy $(\varphi(g_1)-I)\cdots(\varphi(g_n)-I)=0$, mert az $\mathbb{F}_pP$ egységelemén való hatást vizsgálva ebből következik a bizonyítandó állítás.

Jelöljük $\mathrm{UT}(d,p)$-vel az

$$\begin{pmatrix} 1 & * & \cdots & * & * \\ 0 & 1 & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & * \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

alakú *felső unitrianguláris* mátrixok halmazát (a $*$-gal jelölt helyekre bármilyen $\mathbb{F}_p$-beli elemet írhatunk). Látható, hogy $\mathrm{UT}(d,p) \leq \mathrm{GL}(d,p)$ részcsoport, és $|\mathrm{UT}(d,p)| = p^{d(d-1)/2}$. A $\mathrm{GL}(d,p)$ azokat a mátrixokat tartalmazza, ahol a sorok lineárisan függetlenek. Ha az első k sort már kiválasztottuk, akkor a következő sor $p^d - p^k$ féle lehet. Emiatt

$$|\mathrm{GL}(d,p)| = \prod_{k=0}^{d-1}(p^d - p^k) = p^{d(d-1)/2} \cdot \prod_{k=0}^{d-1}(p^{d-k} - 1).$$

Vegyük észre, hogy itt a p kitevője $\frac{d(d-1)}{2}$, ezért $\mathrm{UT}(d,p)$ a $\mathrm{GL}(d,p)$ egyik p-Sylowja. A $\varphi(P)$ p-csoport, ezért a Sylow-tételek miatt van olyan $A \in \mathrm{GL}(d,p)$, amelyre $A^{-1}\varphi(P)A \subseteq \mathrm{UT}(d,p)$. Az A-val való konjugálás egy másik bázisra való áttérés, ezért feltehető, hogy $\mathbb{F}_pP$ bázisát úgy választottuk meg, hogy $\varphi : P \to \mathrm{UT}(d,p)$ homomorfizmus. Ekkor a $\varphi(g) - 1$ minden g-re

$$\begin{pmatrix} 0 & * & \cdots & * & * \\ 0 & 0 & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & * \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

alakú. Könnyen ellenőrizhető, hogy legalább d darab ilyen mátrix szorzata nulla. □

3.3.4. Állítás. *Legyen*

$$J = I_1 + p\mathbb{Z}_pG = (G-1) + p\mathbb{Z}_pG.$$

Ekkor minden $k \geq 1$-re van olyan n, hogy

$$J^n \subseteq I_k + p^k\mathbb{Z}_pG.$$

Bizonyítás. Ellenőrizhető, hogy $(G-1)$ pontosan a $B = \{x(g-1)y \mid x,g,y \in G\}$ által generált $\mathbb{Z}_p$-modulus. Vegyük észre, hogy

$$xy\big(g^y - 1\big) = x(g-1)y = \big(g^{y^{-1}} - 1\big)xy,$$

emiatt

$$B = \{x(g-1) \mid x, g \in G\} = \{(g-1)y \mid g, y \in G\}. \qquad (*)$$

A J-t, mint $\mathbb{Z}_p$-modulust generálja a $B' = B \cup \{px \mid x \in \mathbb{Z}_p G\}$, ezért J^n-et a $B'_n = \{b_1 \cdots b_n \mid b_i \in B'\}$ generálja. A $(*)$ egyenletet felhasználva minden $r \in B'_n$ átírható

$$r = p^{n-m} x(g_1 - 1) \cdots (g_m - 1)$$

alakba, ahol $x, g_1, \ldots, g_m \in G$ és $0 \leq m \leq n$. Elég lenne azt megmutatni, hogy $r \in I_k + p^k \mathbb{Z}_p G$.

Látható, hogy a $\mathbb{Z}_p G \to \mathbb{F}_p(G/G_k)$ természetes homomorfizmus magja $I_k + p\mathbb{Z}_p G$. A 3.3.3. lemma miatt ha $m \geq |G : G_k|$, akkor $(g_1 - 1) \cdots (g_m - 1) \in I_k + p\mathbb{Z}_p G$. $(I_k + p\mathbb{Z}_p G)^k \subseteq I_k + p^k \mathbb{Z}_p G$, ezért $m \geq k|G : G_k|$-ra $(g_1 - 1) \cdots (g_m - 1) \in I_k + p^k \mathbb{Z}_p G$. Ha $n \geq k(|G : G_k| + 1)$, akkor $n - m \geq k$ vagy $m \geq k|G : G_k|$. Mindkét esetben teljesül, hogy $r \in I_k + p^k \mathbb{Z}_p G$. □

3.3.5. Következmény. $\bigcap_{k=1}^{\infty} J^k = 0$.

3.3.6. Definíció. Legyen $r \in \mathbb{Z}_p G$. Ha $r = 0$, akkor legyen $\|r\| = 0$. Ha $r \in J^k \setminus J^{k+1}$ $(k \geq 0)$, akkor pedig legyen $\|r\| = p^{-k}$ (a J^0-t definiáljuk $\mathbb{Z}_p G$-nek).

Mivel minden $r \neq 0$-ra van olyan maximális k, amelyre $r \in J^k$, ez a definíció értelmes. Ellenőrizhető, hogy $\|r\| \leq p^{-k}$ pontosan akkor, ha $r \in J^k$. $1 \notin J$, ezért $\|1\| = p^0 = 1$. A szubmultiplikativitás is világos, hiszen $J^k J^l = J^{k+l}$. Az ultrametrikus egyenlőtlenség pedig onnan látható, hogy J^k zárt az összeadásra és kivonásra. Tehát az előbb definiált $\|\cdot\|$ norma $\mathbb{Z}_p G$-n.

3.3.7. Állítás. *Tetszőleges $k \geq 1$-re $I_k \subseteq J^k$.*

Bizonyítás. k szerinti indukciót alkalmazunk. $k = 1$-re az állítás J definíciójából triviális. Ha $k \geq 2$, akkor a a 2.4.14. állítás miatt a $G_k = G_{k-1}^p$ minden eleme előáll x^p alakban, ahol $x \in G_{k-1}$. Emiatt elég azt igazolni, hogy $x^p - 1 \in J^k$. Legyen $y = x - 1$, ekkor az indukciós feltevés szerint $y \in J^{k-1}$. A binomiális tétel miatt

$$x^p - 1 = (y+1)^p - 1 = \sum_{i=2}^{p} \binom{p}{i} y^i + py.$$

$p \in J$, ezért $py \in J^k$. Az összes többi tagból kiemelhető $y^2 \in J^{2k-2} \subseteq J^k$, tehát $x^p - 1 \in J^k$. □

3.3.8. Állítás. *A norma $G \subseteq \mathbb{Z}_p G$-n az eredeti topológiát indukálja.*

Bizonyítás. G kompakt, és $\mathbb{Z}_p G$ Hausdorff, ezért elég azt ellenőrizni, hogy a $G \to \mathbb{Z}_p G$ beágyazás folytonos. Ha $x \in G$ és $y \in xG_k$, akkor a 3.3.7. állítás következtében $y^{-1}x - 1 \in I_k \subseteq J^k$. Emiatt

$$\|x - y\| = \|y(y^{-1}x - 1)\| \leq \|y\| \|y^{-1}x - 1\| \leq p^{-k}.$$

Ebből következik a folytonosság, mert xG_k nyílt. □

Rögzítsük G-nek egy $\mathbf{a} = (a_1, \ldots, a_d)$ minimális topologikus generátorrendszerét. Legyen $b_i = a_i - 1$, és $\mathbf{b} = (b_1, \ldots, b_d)$. Ekkor $\|b_i\| \leq p^{-1}$ minden i-re.

Ha $\mathbf{x} = (x_1, \ldots, x_n)$, $x_i \in \mathbb{Z}_p G$, és $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, akkor az $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ és $\langle \alpha \rangle = \alpha_1 + \ldots \alpha_d$ jelöléseket most is fogjuk alkalmazni. Világos, hogy $\mathbf{b}^\alpha \in J^{\langle \alpha \rangle}$ minden $\alpha \in \mathbb{N}^n$-re.

3.3.9. Lemma. *Legyen $k \geq 1$-re $T_k = \{\alpha \in \mathbb{N}^d \mid \alpha_1, \ldots, \alpha_d < p^{k-1}\}$. Ekkor*

$$\mathbb{Z}_p G = I_k \oplus \bigoplus_{\alpha \in T_k} \mathbb{Z}_p \mathbf{b}^\alpha.$$

Bizonyítás. Térjünk át $\mathbb{Z}_p G$ helyett $\mathbb{Z}_p(G/G_k) \cong \mathbb{Z}_p G / I_k$-ra. G/G_k hatványteljes, de már nem feltétlenül egyenletes. Azt kell megmutatnunk, minden elem pontosan egyféleképpen áll elő $\sum_{\alpha \in T_k} \lambda_\alpha \mathbf{b}^\alpha$ alakban. A 2.4.16. állítás szerint minden $g \in G/G_k$ előáll $\mathbf{a}^\beta$ alakban, ahol $\beta_i \in \mathbb{Z}_p$. $a_i^{p^{k-1}} = 1$, ezért az $a_i^{\beta_i}$ csak $\beta_i \bmod p^{k-1}$-től függ. Így minden β_i választható a $\{0, \ldots, p^{k-1} - 1\}$ halmazból.

A $a_i = b_i + 1$, ezért a binomiális tétel miatt

$$\mathbf{a}^\beta = \prod_{i=1}^{d} (b_i + 1)^{\beta_i} = \prod_{i=1}^{d} \sum_{\alpha_i = 0}^{p^{k-1}-1} \binom{\beta_i}{\alpha_i} b_i^{\alpha_i} = \sum_{\alpha \in T_k} \binom{\beta_1}{\alpha_1} \cdots \binom{\beta_d}{\alpha_d} \mathbf{b}^\alpha.$$

(Ha $\beta_i<\alpha_i$, akkor $\binom{\beta_i}{\alpha_i}=0$.) A $\mathbb{Z}_p(G/G_k)$-nak, mint $\mathbb{Z}_p$-modulusnak az $\mathbf{a}^\beta$-k egy generátorrendszerét alkotják, tehát a $\mathbf{b}^\alpha$-k is.

G egyenletes, ezért $|G/G_k|=p^{d(k-1)}$. A T_k is $p^{d(k-1)}$ elemű, ezért a $\mathbf{b}^\alpha$-k $\mathbb{Q}_p$ felett lineárisan függetlenek $\mathbb{Q}_p(G/G_k)$-ban (különben $\mathbb{Q}_p$ felett nem generálnák G/G_k minden elemét), így nyilván $\mathbb{Z}_p$ felett is lineárisan függetlenek. Ebből következik, hogy az előállítás egyértelmű. □

3.3.10. Lemma. *Tetszőleges $1\le i,j\le d$-re*

$$b_ib_j-b_jb_i\in J^3+pJ.$$

Bizonyítás. Ellenőrizhető, hogy

$$b_ib_j-b_jb_i=(a_i-1)(a_j-1)-(a_j-1)(a_i-1)=a_ia_j-a_ja_i=a_ja_i([a_i,a_j]-1).$$

Ha $p>2$, akkor $[a_i,a_j]\in G_2$, ezért a 2.4.14. állítás miatt $[a_i,a_j]=y^p$ alakú, ahol $y\in G$. Legyen $z=y-1\in J$, ekkor

$$[a_i,a_j]-1=y^p-1=z^p+\sum_{l=1}^{d-1}\binom{p}{l}z^l\in J^p+pJ\subseteq J^3+pJ.$$

Ha $p=2$, akkor a hatványteljesség miatt $[a_i,a_j]\in\overline{G^4}=G_3$. a 2.4.15. állítás miatt $[a_i,a_j]=y^2$ valamilyen $y\in G_2$-re. Most is legyen $z=y-1$. $z\in I_2$, ezért a 3.3.7. állítás miatt $z\in J^2$, tehát

$$[a_i,a_j]-1=y^2-1=z^2+2z\in J^4+2J^2\subseteq J^3+2J.$$

Mindkét esetben azt kaptuk, hogy $[a_i,a_j]-1\in J^3+pJ$, ahonnan következik, hogy $b_ib_j-b_jb_i\in J^3+pJ$. □

3.3.11. Lemma. *Legyen $W_k=\sum_{\langle\alpha\rangle\le k}p^{k-\langle\alpha\rangle}\mathbb{Z}_p\mathbf{b}^\alpha$. Ekkor minden $k\ge 0$-ra*

$$J^k=J^{k+1}+W_k.$$

Bizonyítás. Nyilvánvaló, hogy $W_k\subseteq J^k$, emiatt $J^k\supseteq J^{k+1}+W_k$. A másik irányt k szerinti indukcióval bizonyítjuk.

A $k=0$ esetben a 3.3.9. lemma következtében

$$J^0=\mathbb{Z}_pG=I_1+\mathbb{Z}_p\subseteq J+W_0.$$

Legyen $x\in I_1$. A 3.3.9. lemma miatt $x=y+\sum_{\alpha\in T_2}\lambda_\alpha\mathbf{b}^\alpha$ alakú, ahol $y\in I_2$. $b_i\in I_1$ minden i-re, ezért ha $\alpha\ne\mathbf{0}$, akkor $\mathbf{b}^\alpha\in I_1$. Emiatt $y+\sum_{\alpha\in T_2\setminus\{\mathbf{0}\}}\lambda_\alpha\mathbf{b}^\alpha\in I_1$. Az egyértelműség miatt $\lambda_{\mathbf{0}}=0$. A 3.3.7. állítás miatt $I_2\subseteq J^2$. Ha $\langle\alpha\rangle\ge 2$, akkor $\mathbf{b}^\alpha\in J^2$, ezért $x\in J^2+\sum_{i=1}^d\mathbb{Z}_pb_i$. A 3.3.9. lemmát ismét alkalmazva

$$J=I_1+p\mathbb{Z}_pG=I_1+p(I_1+\mathbb{Z}_p)=I_1+p\mathbb{Z}_p\subseteq J^2+\sum_{i=1}^d\mathbb{Z}_pb_i+p\mathbb{Z}_p,$$

ami éppen a bizonyítandó állítás a $k=1$ esetben.

Most tegyük fel, hogy $k\ge 2$. Az indukciós feltevés miatt

$$J^k=JJ^{k-1}=J(J^k+W_k)=J^{k+1}+\sum_{\langle\alpha\rangle\le k-1}p^{k-\langle\alpha\rangle-1}J\mathbf{b}^\alpha,$$

így elég lenne azt megmutatni, hogy $p^{k-\langle\alpha\rangle-1}J\mathbf{b}^\alpha\subseteq J^{k+1}+W_k$. Látható, hogy

$$p^l(J^{m+1}+W_m)=p^lJ^{m+1}+p^lW_m\subseteq J^{m+l+1}+W_{m+l}$$

minden $l,m\ge 0$-ra. Emiatt az is elég lenne, hogy

$$J\mathbf{b}^\alpha\subseteq J^{\langle\alpha\rangle+2}+W_{\langle\alpha\rangle+1}$$

minden α-ra. Ehelyett azt az erősebb állítást igazoljuk, hogy ha $x_1\dots,x_n$ mindegyike valamelyik b_i, és $1\le m\le n$, akkor

$$x_1\cdots x_{m-1}Jx_{m+1}\cdots x_n\subseteq J^{n+1}+W_n, \tag{1}$$

illetve

$$x_1\cdots x_n\in J^{n+1}+W_n. \tag{2}$$

A két állítást egyszerre bizonyítjuk n szerinti indukcióval.

A $k=1$ eset miatt $J=J^2+\sum_{i=1}^d\mathbb{Z}_pb_i+p\mathbb{Z}_p$, az (1) állítást elég J helyett ezekre a tagokra ellenőrizni. Világos, hogy $x_1\cdots x_{m-1}J^2x_{m+1}\cdots x_n\subseteq J^{n+1}$. A (2) állítást az indukciós feltevés szerint alkalmazhatjuk $n-1$-re, emiatt

$$x_1\cdots x_{m-1}px_{m+1}\cdots x_n=px_1\cdots x_{m-1}x_{m+1}\cdots x_n\subseteq p(J^n+W^{n-1})\subseteq J^{n+1}+W_n.$$

Az (1) állítás bizonyításához már csak az $x_1\cdots x_{m-1}b_ix_{m+1}\cdots x_n\in J^{n+1}+W_n$ kell, ez a (2) állítás speciális esete.

A (2) állítás az n=1 esetben triviális, feltesszük, hogy $n\ge2$. Vizsgáljuk meg, hogy mit történik, ha az x_i-t és x_{i+1}-et felcseréljük. Legyen $y=x_1\cdots x_{i-1}$ és $z=x_{i+2}\cdots x_n$. A 3.3.10. lemma szerint $x_ix_{i+1}-x_{i+1}x_i\in J^3+pJ$, emiatt

$$yx_ix_{i+1}z-yx_{i+1}x_iz=y(x_ix_{i+1}-x_{i+1}x_i)z\in y(J^3+pJ)z=yJ^3z+pyJz.$$

$y\in J^{i-1}$ és $z\in J^{n-i-1}$, ezért $yJ^3z\subseteq J^{n+1}$. Az (1) állítást $n-1$-re alkalmazva kapjuk, hogy $yJz\subseteq J^n+W_{n-1}$, ezért $pyJz\subseteq J^{n+1}+W_n$. Tehát az x_i és x_{i+1} felcserélése egy $J^{n+1}+W_n$-beli elem hozzáadását jelenti. Mivel minden x_i valamelyik b_j, a szomszédos tényezők cserélgetésével az $x_1\cdots x_n$-et $\mathbf{b}^\alpha$ alakra hozhatjuk, ami benne van W_n-ben, mert $\langle\alpha\rangle=n$. Ezzel megmutattuk, hogy $x_1\cdots x_n\in J^{n+1}+W_n$. □

3.3.12. Tétel. *Minden $x\in\mathbb{Z}_pG$ egyértelműen előáll*

$$x=\sum_{\alpha\in\mathbb{N}^d}\lambda_\alpha\mathbf{b}^\alpha$$

alakban, ahol $\lambda_\alpha\in\mathbb{Z}_p$. Továbbá teljesül, hogy

$$\|x\|=\sup_{\alpha\in\mathbb{N}^d}|\lambda_\alpha|_pp^{-\langle\alpha\rangle}.$$

Bizonyítás. Először megmutatjuk az egyértelműséget. Ha x kétféleképpen is felírható, akkor a folytonosság miatt tagonként kivonhatjuk egymásból a két sort. Így elég azt bizonyítani, hogy ha $\sum_{\alpha\in\mathbb{N}^d}\lambda_\alpha\mathbf{b}^\alpha=0$, akkor $\lambda_\alpha=0$ minden α-ra. Tegyük fel, hogy van olyan α, amelyre $\lambda_\alpha\ne0$. Feltehető, hogy $|\lambda_\alpha|_p=p^{-n}$ maximális. Legyen $k>n$ olyan nagy, hogy $\alpha\in T_k$. A 3.3.4. állítás miatt van olyan m, amelyre $J^m\subseteq I_k+p^k\mathbb{Z}_pG$. T_k véges, ezért van olyan $S\supseteq T_k$, amelyre $\left\|\sum_{\beta\in S}\lambda_\beta\mathbf{b}^\beta\right\|\le p^{-m}$, emiatt

$$\sum_{\beta\in S}\lambda_\beta\mathbf{b}^\beta\in I_k+p^k\mathbb{Z}_pG\subseteq I_k+p^{n+1}\mathbb{Z}_pG.$$

Ha $\beta\in S\setminus T_k$, akkor $\beta_i\ge p^{k-1}$ valamelyik i-re. Tetszőleges $g\in G$-re

$$(g-1)^p=g^p+(-1)^p+\sum_{j=1}^{p-1}\binom{p}{j}g^j\equiv g^p-1\pmod{p\mathbb{Z}_pG},$$

ebből indukcióval látható, hogy $b_i^{p^{k-1}}\equiv a_i^{p^{k-1}}-1\pmod{p\mathbb{Z}_pG}$, így $b_i^{p^{k-1}}\in I_k+p\mathbb{Z}_pG$. A $|\lambda_\alpha|_p$ minimalitása miatt $\lambda_\beta\in p^n\mathbb{Z}_p$, ezért $\lambda_\beta\mathbf{b}^\beta\in I_k+p^{n+1}\mathbb{Z}_pG$. Ebből következik, hogy

$$\sum_{\beta\in T_k}\lambda_\beta\mathbf{b}^\beta=\sum_{\beta\in S}\lambda_\beta\mathbf{b}^\beta-\sum_{\beta\in S\setminus T_k}\lambda_\beta\mathbf{b}^\beta\in I_k+p^{n+1}\mathbb{Z}_pG.$$

A 3.3.9. lemmában szereplő egyértelműség miatt minden $\beta\in T_k$-ra $\lambda_\beta\in p^{n+1}\mathbb{Z}_p$, speciálisan $\lambda_\alpha\in p^{n+1}\mathbb{Z}_p$, ami ellentmondás.

Legyen $x \in \mathbb{Z}_pG$ tetszőleges. Világos, hogy elég $\mathbb{Z}_pG$ teljessé tételében bizonyítani az x előállíthatóságát. Legyen $x_0 = x$. Az $x_k \in J^k$-t rekurzívan definiáljuk a következőképpen: az x_k-t állítsuk elő a 3.3.11. lemma szerint $x_k = x_{k+1} + y_k$ alakban, ahol

$$y_k = \sum_{\langle\alpha\rangle \le k} p^{k-\langle\alpha\rangle} \lambda_{k,\alpha} \mathbf{b}^\alpha,$$

$x_{k+1} \in J^{k+1}$ és $\lambda_{k,\alpha} \in \mathbb{Z}_p$. Ekkor $\sum_{k=0}^{n} y_k = x - x_{n+1}$, ezért $\sum_{k=0}^{\infty} y_k = x$. Ellenőrizhető, hogy $p^{k-\langle\alpha\rangle}\lambda_{k,\alpha}\mathbf{b}^\alpha \in J^k$. Ebből következik, hogy

$$\lim_{\substack{k\ge 0 \\ \langle\alpha\rangle \le k}} p^{k-\langle\alpha\rangle} \lambda_{k,\alpha} \mathbf{b}^\alpha = 0,$$

mert minden k-hoz véges sok α tartozik. Az 1.2.1. és 1.2.4. állítás miatt

$$x = \sum_{k=0}^{\infty} y_k = \sum_{\substack{k\ge 0 \\ \langle\alpha\rangle \le k}} p^{k-\langle\alpha\rangle} \lambda_{k,\alpha} \mathbf{b}^\alpha = \sum_{\alpha \in \mathbb{N}^d} \sum_{k \ge \langle\alpha\rangle} p^{k-\langle\alpha\rangle} \lambda_{k,\alpha} \mathbf{b}^\alpha$$

Legyen $\lambda_\alpha = \sum_{k=\langle\alpha\rangle}^{\infty} p^{k-\langle\alpha\rangle}\lambda_{k,\alpha}$, ez nyilvánvalóan konvergens $\mathbb{Z}_p$-ben. $p^k \in J^k$, emiatt a konvergencia $\mathbb{Z}_pG$-ben is teljesül. Ezzel megmutattuk, hogy $x = \sum_{\alpha\in\mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha$.

Az $\|x\|$-ra vonatkozó állítás $x=0$ esetén triviális. Ha $\|x\| = p^{-n}$, akkor a $\lambda_{k,\alpha}$-t minden $k<n$-re választhatjuk 0-nak, ekkor $x = x_0 = \cdots = x_n$. Ha $k \ge \langle\alpha\rangle$, akkor $p^{k-\langle\alpha\rangle}\lambda_\alpha \in p^{n-\langle\alpha\rangle}$, emiatt $\lambda_\alpha \in p^{n-\langle\alpha\rangle}\mathbb{Z}_p$, vagyis $|\lambda_\alpha|_p p^{-\langle\alpha\rangle} \le$ $\le p^{-n} = \|x\|$. Az egyenlőtlenség másik iránya az 1.2.3. állításból triviális. □

3.3.13. Következmény. *Tetszőleges $\lambda \in \mathbb{Z}_p$ és $x \in \mathbb{Z}_pG$ esetén $\|\lambda x\| = |\lambda|_p \|x\|$.*

3.3.14. Következmény. *A $\mathbb{Z}_p \to \mathbb{Z}_pG$ beágyazás normatartó.*

3.3.15. Definíció. Legyen $x \in \mathbb{Q}_pG$. Ha n elég nagy, akkor $p^n x \in \mathbb{Z}_pG$. Ekkor legyen $\|x\|_{\mathbb{Q}_p} = p^n \|p^n x\|$.

A 3.3.13. állítás miatt $\|x\|_{\mathbb{Q}_p}$ nem függ az n választásától. Könnyen ellenőrizhető, hogy a $\|\cdot\|_{\mathbb{Q}_p}$ norma, ami kiterjesztése a $\mathbb{Z}_pG$-n definiált normának, emiatt ezt a normát is $\|\cdot\|$-val fogjuk jelölni. A továbbiakban a $\mathbb{Q}_pG$ csoportalgebrában dolgozunk.

3.3.16. Definíció. Ha $\lambda \in \mathbb{Z}_p$ és $k \in \mathbb{N}$, akkor legyen

$$\binom{\lambda}{k} = \frac{\lambda(\lambda-1)\cdots(\lambda-k+1)}{k!}.$$

3.3.17. Állítás. *Minden $\lambda \in \mathbb{Z}_p$ és $k \in \mathbb{N}$ esetén $\binom{\lambda}{k} \in \mathbb{Z}_p$.*

Bizonyítás. Világos, hogy a $\lambda \mapsto \binom{\lambda}{k}$ folytonos. Az $\mathbb{N}$ sűrű $\mathbb{Z}_p$-ben, ezért választhatunk egy (x_n) sorozatot $\mathbb{N}$-ben, amelyre $x_n \to \lambda$. Ekkor $\binom{x_n}{k} \to \binom{\lambda}{k}$, ezért elég azt megmutatni, hogy $\binom{x}{k}$ minden $x \in \mathbb{N}$-re egész. Ha $x \ge k$, akkor $\binom{x}{k}$ a szokásos binomiális együttható, ha pedig $0 \le x < k$, akkor $\binom{x}{k} = 0$, ami szintén egész. □

3.3.18. Állítás. *Legyen $u \in G$ és $v = u - 1$. Ekkor*

$$u^\lambda = \sum_{k=0}^{\infty} \binom{\lambda}{k} v^k.$$

Bizonyítás. Válasszunk $\mathbb{N}$-ben egy (x_n) sorozatot, amelyre $x_n \to \lambda$. A 3.3.8. állítás miatt $u^{x_n} \to u^\lambda$ a csoportalgebrában. Tetszőleges k-ra és n-re $\left\|\binom{x_n}{k} v^k\right\| \le \|v\|^k \le p^{-k}$ (felhasználva, hogy $\binom{x_k}{k} \in \mathbb{Z}_p$). $p^{-k} \to 0$, ha $k \to \infty$, ezért alkalmazható az 1.2.7. állítás:

$$u^\lambda = \lim_{n\to\infty} (v+1)^{x_n} = \lim_{n\to\infty} \sum_{k=0}^{\infty} \binom{x_n}{k} v^k = \sum_{k=0}^{\infty} \lim_{n\to\infty} \binom{x_n}{k} v^k = \sum_{k=0}^{\infty} \binom{\lambda}{k} v^k.$$

□

3.3.19. Lemma. *Tetszőleges $\lambda \in \mathbb{Z}_p$ és $k \in \mathbb{N}$ esetén*

$$\left|\frac{1}{k!}\right|_p \leq p^k.$$

Bizonyítás. Azt kell megmutatnunk, hogy $|k!|_p \geq p^{-k}$. Jelöljük $v_p(x)$-szel az x prímtényezős felbontásában p kitevőjét. A Legendre-formula miatt

$$v_p(k!) = \sum_{n=1}^{\infty} \left\lfloor \frac{k}{p^n} \right\rfloor \leq \sum_{n=1}^{\infty} \frac{k}{p^n} = \frac{k}{p-1} \leq k,$$

ebből nyilvánvaló az állítás. □

3.3.20. Lemma. *Legyen $\mathbf{u} = (u_1, \ldots, u_r)$, ahol $u_1, \ldots, u_r \in G_2$ tetszőlegesek. A 2.5.6. állítás szerint bármely $\mu \in \mathbb{Z}_p^r$-re egyértelműen van olyan $\lambda \in \mathbb{Z}_p^d$, amelyre $\mathbf{u}^\mu = \mathbf{a}^\lambda$. Ekkor a $\mu \mapsto \lambda$ leképezés analitikus.*

Bizonyítás. Az 1.2.6 és 3.3.18. állítás miatt

$$\mathbf{u}^\mu = \prod_{i=1}^{r} \sum_{\beta_i=0}^{\infty} \binom{\mu_i}{\beta_i} v_i^\beta = \sum_{\beta \in \mathbb{N}^r} \binom{\mu_1}{\beta_1} \cdots \binom{\mu_r}{\beta_r} \mathbf{v}^\beta.$$

Hasonlóan látható, hogy

$$\mathbf{a}^\lambda = \sum_{\alpha \in \mathbb{N}^r} \binom{\lambda_1}{\alpha_1} \cdots \binom{\lambda_d}{\alpha_d} \mathbf{b}^\alpha.$$

A 3.3.12. tétel szerint vannak olyan $c_{\alpha,\beta} \in \mathbb{Z}_p$ együtthatók, amelyre

$$\mathbf{v}^\beta = \sum_{\alpha \in \mathbb{N}^d} c_{\alpha,\beta} \mathbf{b}^\alpha.$$

Ekkor tetszőleges α, β-ra $\|c_{\alpha,\beta}\| \leq \|\mathbf{u}^\beta\| \leq p^{-2\langle\beta\rangle}$, hiszen $\|v_i\| \leq p^{-2}$ minden i-re. Az 1.2.5. állítás miatt

$$\mathbf{a}^\lambda = \mathbf{u}^\mu = \sum_{\beta \in \mathbb{N}^r} \sum_{\alpha \in \mathbb{N}^d} \binom{\mu_1}{\beta_1} \cdots \binom{\mu_r}{\beta_r} c_{\alpha,\beta} \mathbf{b}^\alpha = \sum_{\alpha \in \mathbb{N}^d} \sum_{\beta \in \mathbb{N}^r} \binom{\mu_1}{\beta_1} \cdots \binom{\mu_r}{\beta_r} c_{\alpha,\beta} \mathbf{b}^\alpha,$$

de előbb ellenőriznünk kell, hogy

$$\lim_{\substack{\alpha \in \mathbb{N}^d \\ \beta \in \mathbb{N}^r}} \binom{\mu_1}{\beta_1} \cdots \binom{\mu_r}{\beta_r} c_{\alpha,\beta} \mathbf{b}^\alpha = 0.$$

A 3.3.19. lemma miatt $\left\|\frac{1}{\beta_i!}\right\| \leq p^{\beta_i}$, ezért $\left\|\frac{1}{\beta_1! \cdots \beta_r!}\right\| \leq p^{\langle\beta\rangle}$. A $\binom{\mu_i}{\beta_i}$ számlálója $\mathbb{Z}_p$-beli, emiatt

$$\left\| \binom{\mu_1}{\beta_1} \cdots \binom{\mu_r}{\beta_r} c_{\alpha,\beta} \right\| \leq \left\| \frac{c_{\alpha,\beta}}{\beta_1! \cdots \beta_r!} \right\| \leq p^{\langle\beta\rangle} \cdot p^{-2\langle\beta\rangle} \leq p^{-\langle\beta\rangle},$$

tehát

$$\left\| \binom{\mu_1}{\beta_1} \cdots \binom{\mu_r}{\beta_r} c_{\alpha,\beta} \mathbf{b}^\alpha \right\| \leq p^{-(\langle\beta\rangle + \langle\alpha\rangle)},$$

ahonnan nyilvánvaló a konvergencia. Az 1.2.1. állításból a

$$\sum_{\beta \in \mathbb{N}^r} \binom{\mu_1}{\beta_1} \cdots \binom{\mu_r}{\beta_r} c_{\alpha,\beta}$$

konvergenciája is világos, emiatt

$$\mathbf{a}^\lambda = \sum_{\alpha \in \mathbb{N}^d} \left(\sum_{\beta \in \mathbb{N}^r} \binom{\mu_1}{\beta_1} \cdots \binom{\mu_r}{\beta_r} c_{\alpha,\beta} \right) \mathbf{b}^\alpha.$$

A 3.3.12. tételben szereplő egyértelműség miatt az $\mathbf{a}^\lambda$ kétféle felírásában az együtthatók megegyeznek, azaz tetszőleges α-ra

$$\binom{\lambda_1}{\alpha_1}\cdots\binom{\lambda_d}{\alpha_d}=\sum_{\beta\in\mathbb{N}^r}\binom{\mu_1}{\beta_1}\cdots\binom{\mu_r}{\beta_r}c_{\alpha,\beta}.$$

Rögzítsünk egy $1\le j\le d$-t, és legyen $\alpha_i=\delta_{i,j}$, ahol $\delta_{i,j}$ a Kronecker-delta. Ekkor

$$\lambda_j=\sum_{\beta\in\mathbb{N}^r}\binom{\mu_1}{\beta_1}\cdots\binom{\mu_r}{\beta_r}c_{\alpha,\beta}.$$

A $\binom{\mu_i}{\beta_i}$ számlálója a μ_i-nek egész együtthatós polinomja. Emiatt van olyan $\nu_{\beta,\gamma}\in\mathbb{Z}$, amelyre

$$\binom{\mu_1}{\beta_1}\cdots\binom{\mu_r}{\beta_r}=\sum_{\gamma\in\mathbb{N}^r}\frac{\nu_{\beta,\gamma}}{\beta_1!\cdots\beta_r!}\mu^\gamma.$$

Itt a konvergencia triviális, mert minden β-ra véges sok γ kivételével $\nu_{\beta,\gamma}=0$. Az 1.2.5. állítás következtében

$$\lambda_j=\sum_{\beta\in\mathbb{N}^r}\sum_{\gamma\in\mathbb{N}^r}\frac{\nu_{\beta,\gamma}c_{\alpha,\beta}}{\beta_1!\cdots\beta_r!}\mu^\gamma=\sum_{\gamma\in\mathbb{N}^r}\sum_{\beta\in\mathbb{N}^r}\frac{\nu_{\beta,\gamma}c_{\alpha,\beta}}{\beta_1!\cdots\beta_r!}\mu^\gamma=\sum_{\gamma\in\mathbb{N}^r}\left(\sum_{\beta\in\mathbb{N}^r}\frac{\nu_{\beta,\gamma}c_{\alpha,\beta}}{\beta_1!\cdots\beta_r!}\right)\mu^\gamma.$$

A konvergenciát most is ellenőriznünk kell. $\mu\in\mathbb{Z}_p^r$ és $\nu_{\beta,\gamma}\in\mathbb{Z}_p$, ezért

$$\left\|\frac{\nu_{\beta,\gamma}c_{\alpha,\beta}}{\beta_1!\cdots\beta_r!}\mu^\gamma\right\|\le\left\|\frac{\nu_{\beta,\gamma}c_{\alpha,\beta}}{\beta_1!\cdots\beta_r!}\right\|\le\left\|\frac{c_{\alpha,\beta}}{\beta_1!\cdots\beta_r!}\right\|\le p^{-\langle\beta\rangle}.$$

Ebből következik, hogy

$$\lim_{\beta,\gamma\in\mathbb{N}^r}\frac{\nu_{\beta,\gamma}c_{\alpha,\beta}}{\beta_1!\cdots\beta_r!}\mu^\gamma=0,$$

hiszen rögzített β-ra csak véges sok $\nu_{\beta,\gamma}$ nem nulla, illetve tetszőleges γ-ra

$$\lim_{\beta\in\mathbb{N}^r}\frac{\nu_{\beta,\gamma}c_{\alpha,\beta}}{\beta_1!\cdots\beta_r!}=0.$$

Ezzel a λ_j-t előállítottuk a μ hatványsoraként. Mivel $\mu\in\mathbb{Z}_p^r$ tetszőleges volt, az 1.4.11. lemma szerint a $\mu\mapsto\lambda_j$ függvény analitikus. □

3.3.21. Tétel. *Ha egy topologikus csoportnak van olyan nyílt részcsoportja, ami egyenletes pro-p-csoport, akkor megadható rajta egy olyan atlasz, amellyel p-adikus Lie-csoport.*

Bizonyítás. Először G_2-n megadunk egy sokaságstruktúrát. A 2.5.3. állítás szerint az a_i^p alakú elemek a G_2-nek egy minimális topologikus generátorrendszerét alkotják, ezért a 2.5.6. állítás következtében $G_2=\{\mathbf{a}^\lambda\mid\lambda\in p\mathbb{Z}_p^d\}$. A 2.5.7. állítás miatt az $\mathbf{a}^\lambda\mapsto\lambda$ leképezés egy $G_2\to p\mathbb{Z}_p^d$ homeomorfizmus, ez lesz az egyetlen térkép az atlaszban. Ellenőriznünk kell, hogy a szorzás és az inverzképzés analitikusak. Legyen $\mu_1,\mu_2\in p\mathbb{Z}_p^d$ tetszőleges. Ha $\mathbf{a}^{\mu_1}\mathbf{a}^{\mu_2}=\mathbf{a}^\lambda$, akkor a 3.3.20. lemma szerint a $(\mu_1,\mu_2)\mapsto\lambda$ leképezés analitikus. Ha $\mu\in p\mathbb{Z}_p^d$ és $(\mathbf{a}^\mu)^{-1}=\mathbf{a}^\lambda$, akkor $(a_d^{-1})^{\mu_d}\cdots(a_1^{-1})^{\mu_1}=\mathbf{a}^\lambda$. A $\mu\mapsto(\mu_d,\dots,\mu_1)$ leképezés analitikus, és a 3.3.20. lemma szerint a $(\mu_d,\dots,\mu_1)\mapsto\lambda$ is analitikus, tehát a $\mu\mapsto\lambda$ is. Ezzel megmutattuk, hogy G_2 egy p-adikus Lie-csoport.

Legyen H topologikus csoport, és tegyük fel, hogy $G\le_o H$. A 3.1.9. lemmát fogjuk alkalmazni a sokaságstruktúra kiterjesztéséhez. Legyen $g\in G$ tetszőleges. Mivel $G_2\cap G_2^{g^{-1}}$ nyílt, a 2.3.4. állítás miatt $G_k\le G_2^{g^{-1}}$ valamilyen $k\ge 2$-re. A 2.5.3. állítást felhasználva az eddigiekhez hasonlóan látható, hogy minden $\mathbf{a}^\mu\in G_k$-ra $\mu\in p^{k-1}\mathbb{Z}_p^d$. Ha $(\mathbf{a}^\mu)^g=\mathbf{a}^\lambda$, akkor

$$\mathbf{a}^\lambda=(\mathbf{a}^\mu)^g=\left(\left(a_1^{p^{k-1}}\right)^g\right)^{\mu_1/p^{k-1}}\cdots\left(\left(a_d^{p^{k-1}}\right)^g\right)^{\mu_d/p^{k-1}}.$$

$a_i^{p^{k-1}}\in G_k$, ezért $\left(a_1^{p^{k-1}}\right)^g\in G_2$. Így a 3.3.20. lemma alkalmazható, tehát a $\frac{\mu}{p^{k-1}}\mapsto\lambda$ leképezés analitikus. A $\mu\mapsto\frac{\mu}{p^{k-1}}$ is analitikus, ezért a kompozíciójuk, a $\mu\mapsto\lambda$ is analitikus. Ezzel beláttuk, hogy az $x\mapsto x^g$ leképezés analitikus a G_k-n, tehát a sokaságstruktúra kiterjed H-ra. □

Irodalomjegyzék

[1] Joseph Bernstein – Stephen Gelbart (szerk.): *An Introduction to the Langlands Program*. 2004, Birkhäuser Boston.

[2] J. D. Dixon – M. P. F. du Sautoy – A. Mann – D. Segal: *Analytic Pro-p Groups*. 2. kiad. 1999, Cambridge University Press.

[3] C. R. Leedham-Green: The structure of finite p-groups. *Journal of the London Mathematical Society*, 50. évf. (1994. aug) 1. sz., 49–67. p.

[4] Peter Schneider: *p-Adic Lie Groups*. 2011, Springer Berlin Heidelberg.

[5] Jean-Pierre Serre: *Galois Cohomology*. 1997, Springer Berlin Heidelberg.

[6] Aner Shalev: The structure of finite p-groups: Effective proof of the coclass conjectures. *Inventiones Mathematicae*, 115. évf. (1994. dec) 1. sz., 315–345. p.