A Nottingham csoport részcsoportjai

Zábrádi Gergely,
ELTE TTK matematikus szak
zger@cs.elte.hu

Témavezető: Hegedűs Pál,
vendégkutató
ELTE TTK, Algebra és Számelmélet Tanszék

Tartalomjegyzék

1. fejezet

Bevezetés

A Nottingham csoportot az utóbbi időben egyre többet vizsgálják a matematikusok, csoportelméleti és számelméleti szempontból egyaránt. Ennek oka egyrészt az, hogy Camina belátta, hogy minden megszámlálható bázisú pro-p csoport beágyazható a Nottingham csoportba, tehát speciálisan minden véges p-csoport is. Másrészt a kommutátor-struktúrája – kissé leegyszerűsítve – viszonylag könnyen kezelhető, ezért a csoport vizsgálható Lie-elméleti, illetve pusztán kombinatorikus eszközökkel is. Továbbá a Nottingham csoport épp végtelen, azaz minden valódi (folytonos) homomorf képe véges. Ezek a csoportok a pro-p csoportok építőkövei, csakúgy mint a véges csoportok között az egyszerűek. Így a Nottingham csoport és részcsoportjai rendkívül fontos szerepet játszanak pro-p csoportokkal kapcsolatos sejtések tesztelésében.

A számelméletben a Nottingham csoport (a továbbiakban $\mathcal{N}$) úgy volt ismert, mint egy lokális test vad automorfizmusainak csoportja. A csoportelméleti köztudatba Johnson [21] (akit Jennings [20] cikke inspirált) és tanítványa, York [40] hozta be 1988-ban. Ők a nottinghami egyetemen dolgoztak, innen ered a név. A Nottingham csoport megjelenítése mint formális hatványsorok a kompozícióra nézve, alkalmas volt arra, hogy a legtöbb csoportelméleti tulajdonságot belássák. Ezeket az eredményeket foglalom össze a második fejezetben.

A Hausdorff dimenzió fogalmát Barnea és Shalev [5], illetve Abercrombie [1] alkalmazta először algebrai struktúrákra. Ez a mennyiség rendkívül jól méri a részcsoportok méretét. Ahogy véges csoportok esetén érdekes tudni, hogy egy adott csoportnak milyen rendű részcsoportjai vannak, ugyanúgy fontos vizsgálni egy pro-véges csoport Hausdorff spektrumát, azaz azon 0 és 1 közötti valós számok halmazát, melyek előállnak egy részcsoport Hausdorff dimenziójaként. Az úgynevezett index-részcsoportok adják az eddig ismert legtöbb pontot a Nottingham csoport Hausdorff spektrumában. A további pontok meghatározásában a Nottingham csoport Lie-algebrája (a továbbiakban Lie($\mathcal{N}$)) segít: egy részcsoport Lie-algebrájának Hausdorff dimenziója megegyezik a részcsoportéval. A Lie-algebra pedig sokkal könnyebben kezelhető, mert a Lie-szorzáson kívül van rajta vektortér struktúra is. Ez az oka annak, hogy míg $\mathcal{N}$ Hausdorff spektrumára csak becsléseket tudunk, addig Lie($\mathcal{N}$)-é ismert. A maximális nem-nyílt részcsoportok fogalma új megvilágításba helyez néhány korábban is ismert állítást, de a rájuk vonatkozó eredmények újak. Ezek – bizonyos szempontból – a véges csoportok maximális részcsoportjainak általánosításai.

Valójában a maximális nem-nyílt részcsoportokat valószínűségi kérdések vizsgálatára vezettem be. Az ebbe a témakörbe tartozó problémák többsége Shalevtől [31], [32] ered. Aszimptotikus és valószínűségi módszereket véges csoportok vizsgálatára is használnak. Egy pro-p

(vagy általánosabban egy pro-véges) csoporton a valószínűségi mező nem más, mint az 1-re normált Haar-mérték. Az ezzel a témakörrel foglalkozó fejezetben Szegedy Balázs egy eredményét tárgyalom, mely szerint a Nottingham csoportban két elem 1 valószínűséggel szabad részcsoportot generál. Ennek a problémának a „társsejtése”, hogy két elem 1 valószínűséggel nyílt részcsoportot generál (topologikusan). Ezt egyelőre nem sikerült bebizonyítani, de talán a maximális nem-nyílt részcsoportok további vizsgálata segíthet a kérdés megválaszolásában.

Ha a Nottingham csoportra úgy tekintünk, mint egy $\mathbb{F}_q$ véges test feletti formális Laurent-sorok $\mathbb{F}_q((t))$ testének azon automorfizmusainak csoportjára, melyek t-t fixen hagyják modulo t^2, akkor a részcsoportokat vizsgálhatjuk Galois-elméleti módszerekkel. Az ezzel foglalkozó fejezetben közlöm Fesenko bizonyítását Camina tételére. A módszernek fontos felhasználásai vannak: a mélyen elágazó bővítéseket alkalmazni lehet az Abel-féle varietások Kummer-elméletében [8], [34]. Így a Nottingham csoport részcsoportjainak segítségével lehet választ kapni bizonyos számelméleti eredetű problémákra.

Ezúton is szeretném megköszönni témavezetőmnek, Hegedűs Pálnak az érdekes témát, a sok értékes megjegyzést, segítséget, illetve a p-adikus analitikus csoportokról szóló kurzust.

1.1. Pro-véges- és pro-p csoportok

A pro-véges csoportok a véges-, a pro-p csoportok a p-csoportok általánosításai. Ebben az alfejezetben alapvető tulajdonságaikat tekintem át, melyekre szükség lesz a későbbiekben.

1.1.1. Definíció. Egy G topologikus csoportot pro-véges csoportnak nevezünk, ha kompakt, Hausdorff, és az egységelemnek van nyílt részcsoportokból álló környezetbázisa.

1.1.2. Jelölés. Legyen G egy tetszőleges topologikus csoport! Ekkor egy H nyílt, illetve zárt részcsoportot rendre $H \leq_o G$-vel, illetve $H \leq_c G$-vel jelölök. Egy N nyílt (zárt) normálosztóra a jelölés $N \lhd_o G$ ($N \lhd_c G$). Egy $X \subseteq G$ halmaz lezártja $\overline{X}$.

1.1.1. Állítás. *Legyen G egy pro-véges csoport! Ekkor igazak az alábbi kijelentések:*

(i) G minden nyílt részcsoportja zárt, véges indexű, és tartalmaz egy nyílt normálosztót. Egy zárt részcsoport G-ben pontosan akkor nyílt, ha véges indexű. A nyílt részcsoportok metszete csak az egységelemből áll.

(ii) G egy részhalmaza pontosan akkor nyílt, ha nyílt részcsoportok szerinti mellékosztályok egyesítése.

(iii) Egy tetszőleges $X \subseteq G$ részhalmazra

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

Ha X egy részcsoport, akkor

$$\overline{X} = \bigcap \{K : X \leq K \leq_o G\}.$$

(iv) Ha X és Y zárt részhalmazai G-nek, akkor az $XY = \{xy : x \in X, y \in Y\}$ halmaz is az.

(v) *Legyen H egy zárt részcsoportja G-nek! Ekkor H (az indukált topológiával) egy pro-véges csoport. H minden nyílt részcsoportja $H \cap K$ alakú, ahol $K \leq_o G$.*

(vi) *Legyen N egy zárt normálosztó G-ben! Ekkor G/N (a hányadostér topológiával) egy pro-véges csoport, és a természetes homomorfizmus egy nyílt és zárt folytonos leképezés.*

(vii) *Egy $(g_i) \subseteq G$ sorozat pontosan akkor konvergens, ha Cauchy-sorozat, azaz ha minden $N \lhd_o G$-re van olyan $n = n(N)$, amelyre $g_i^{-1} g_j \in N$ minden $i, j \geq n$-re.*

Bizonyítás. Az első két állításhoz vegyük észre, hogy a csoportelemekkel való eltolás folytonossága miatt egy nyílt részcsoport minden (bal- és jobb oldali) mellékosztálya nyílt, ezért egy nyílt részcsoport zárt is, a kompaktság miatt véges sok mellékosztály van, és egy tetszőleges elem környezetbázisát a nyílt részcsoportok megfelelő mellékosztályai alkotják. Egy nyílt részcsoportnak véges sok konjugáltja van, ezek metszete egy véges indexű nyílt normálosztó. Vegyük észre, hogy ebből az állításból következik, hogy a nyílt normálosztók is környezetbázisát alkotják az egységelemnek.

A (iii)-as állításnak elegendő az első felét belátni. Az hogy egy $y \in G$ elem nincs benne X lezártjában azzal ekvivalens, hogy van olyan $N \lhd_o G$ nyílt normálosztó, melyre $yN \cap X = \emptyset$, azaz $y \notin XN$.

A (iv)-es állításhoz vegyük észre, hogy mivel G kompakt Hausdorff, ezért egy részhalmaz zártsága ekvivalens a kompaktságával. Tehát ha X és Y zárt, akkor $X \times Y \subseteq G \times G$ kompakt, továbbá a

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g_1, g_2) & \longmapsto & g_1 g_2 \end{array}$$

leképezés folytonos, tehát XY is zárt, hiszen egy kompakt halmaz folytonos képe.

Az (v)-ös és a (vi)-os állítás a definíció közvetlen következménye. A (vii)-es állításban egy konvergens sorozat nyilván Cauchy. A megfordításhoz legyen $(g_i) \subseteq G$ egy Cauchy-sorozat. Ha a $\{g_i : i \in \mathbb{N}\}$ halmaz véges, akkor a sorozat egy elég nagy indextől kezdve konstans, hiszen Cauchy. Ha viszont ez a halmaz végtelen, akkor mivel G kompakt és Hausdorff, ezért ennek a halmaznak van egy $g \in G$ torlódási pontja. Most legyen $N \lhd_o G$ tetszőleges. Ekkor a gN környezet a (g_i) sorozat végtelen sok pontját tartalmazza, azaz van egy olyan $i \geq n(N)$, melyre $g_i \in gN$. Node ekkor minden $j \geq n(N)$-re $g_j \in g_j N = g_i N = gN$, tehát $g_i \to g$, ha $i \to \infty$. □

A pro-véges csoportok egy másik definíciója az inverz limesz fogalmán alapul. Ezt idézem most fel. *Irányított halmaz*on egy $(\Lambda, \leq)$ részbenrendezett halmazt értek azzal a tulajdonsággal, hogy minden $\lambda, \mu \in \Lambda$ esetén van egy olyan $\nu \in \Lambda$, melyre $\nu \geq \lambda$ és $\nu \geq \mu$. Halmazok (vagy csoportok, gyűrűk, topologikus terek) Λ indexelésű *inverz rendszer*én halmazoknak egy $(G_\lambda)_{\lambda \in \Lambda}$ családját értem minden $\lambda \geq \mu$ esetén a $\pi_{\lambda\mu} : G_\lambda \to G_\mu$ leképezésekkel (homomorfizmusokkal, illetve folytonos függvényekkel) együtt, melyek teljesítik a természetes kompatibilitási feltételeket:

$$\begin{aligned} \pi_{\lambda\lambda} &= \mathrm{id}_{G_\lambda}, \text{ és} \\ \pi_{\lambda\mu}\pi_{\mu\nu} &= \pi_{\lambda\nu}, \text{ ha } \lambda \geq \mu \geq \nu. \end{aligned}$$

A $\varprojlim G_\lambda = \varprojlim (G_\lambda)_{\lambda\in\Lambda}$ *inverz limesz* az összes olyan (g_λ) „vektor"-ból álló részhalmaza (részcsoportja, stb.) a $\prod_{\lambda\in\Lambda} G_\lambda$ direkt szorzatnak, melyekre $g_\lambda \pi_{\lambda\mu} = g_\mu$, ha $\lambda \geq \mu$.

Ha a G_λ halmazok véges csoportok, akkor a diszkrét topológiával topologikus terek is, így $\varprojlim G_\lambda$ egy topologikus csoport lesz.

Ha Λ egy adott G csoport normálosztóinak egy családja, akkor Λ-t rendezhetjük a forditott tartalmazással. Így egy $(G/N)_{N\in\Lambda}$ inverz rendszert kapunk a természetes $G/N \to G/M$ $(N \leq M)$ epimorfizmusokkal.

1.1.2. Állítás. *Ha G egy pro-véges csoport, akkor $G \cong \varprojlim (G/N)_{N\lhd_o G}$. Megfordítva, véges csoportok egy inverz rendszerének inverz limesze egy pro-véges csoport.*

Bizonyítás. Legyen $\hat{G} := \varprojlim (G/N)_{N\lhd_o G}$, továbbá

$$\begin{aligned} \iota\colon G &\to \prod G/N \\ g\iota &= (gN)_{N\lhd_o G} \end{aligned}$$

a természetes homomorfizmus. Mivel $\bigcap_{N\lhd_o G} N = 1$, ezért ι injektív, és az is világos, hogy $G\iota \leq \hat{G}$. A szürjektivitás igazolásához vegyünk egy $(g_N N) \in \hat{G}$ elemet. Ekkor a $g_N N$ mellékosztályok közül bármely véges sok metszete nemüres, hiszen Λ-ban bármely véges sok elemnek van felső korlátja. Így

$$\bigcap_{N\lhd_o G} g_N N \neq \emptyset,$$

mert ezek zárt részhalmazok egy kompakt térben. Ha g-t ebben a metszetben választjuk, akkor $g\iota = (g_N N)$.

Mivel kompakt Hausdorff terek között egy folytonos bijekció mindig homeomorfizmus, ezért elég belátni, hogy ι folytonos. Egy $M \lhd_o G$ nyílt normálosztóra legyen

$$U(M) := \prod_{N\ngeq M} G/N \times \prod_{N\geq M} \{1\} \leq \prod_{N\lhd_o G} G/N!$$

Ekkor a $U(M) \cap \hat{G}$ csoportok az egységelem egy környezetbázisát alkotják $\hat{G}$-ban, és minden M-re $U(M)\iota^{-1} = M$, ami nyílt G-ben. Tehát ι folytonos.

A megfordításhoz tekintsük véges csoportok egy G_λ inverz rendszerét, mindegyiket a diszkrét topológiával! Ekkor $\prod_{\lambda\in\Lambda} G_\lambda$ Hausdorff, és Tyihonov tétele miatt kompakt. A szorzattopológia definíciójából következik, hogy az egységelem tetszőleges nyílt környezete tartalmaz egy

$$U(S) := \prod_{\lambda\notin S} G_\lambda \times \prod_{\lambda\in S} \{1\}$$

alakú részcsoportot valamilyen $S \subset \Lambda$ véges halmazra. Tehát $\prod_{\lambda\in\Lambda} G_\lambda$ egy pro-véges csoport, ezért csak azt kell belátnunk, hogy $\hat{G} := \varprojlim G_\lambda$ egy zárt részcsoport. Most legyen $g \in \prod G_\lambda \setminus \hat{G}$! Ekkor van egy olyan $\nu > \mu \in \Lambda$, melyre $g_\nu \pi_{\nu\mu} \neq g_\mu$, ezért $gU(\{\nu,\mu\})$ egy olyan nyílt környezete g-nek, melynek $\hat{G}$-pal vett metszete üres. Tehát $\prod G_\lambda \setminus \hat{G}$ nyílt, és készen vagyunk. $\square$

1.1.3. Definíció. Egy G pro-véges csoportot *pro-p csoportnak* nevezünk, ha minden nyílt normálosztójának indexe p-hatvány.

A definíció és az 1.1.2-es állítás egyszerű alkalmazása a következő eredmény:

1.1.3. Állítás. *Egy G topologikus csoport pontosan akkor pro-p csoport, ha véges p-csoportok egy inverz limeszével topologikusan izomorf.*

Generált részcsoporton (illetve részalgebrán) ezentúl mindig topologikus generátumot értek, azaz a hagyományos generátum lezártját – kivéve néhány esetben, ahol ezt hangsúlyozom.

1.1.4. Definíció. Legyen G egy végesen generált pro-p csoport! Ekkor a $P_1(G) := G$, $P_n(G) := P_{n-1}(G)^p[P_{n-1}(G), G]$ filtrálást G *alsó centrális p-lánc*ának nevezzük.

1.1.5. Definíció. Legyen G végesen generált pro-p csoport! Ekkor

(*i*) G *hatványteljes* (powerful), ha $G^p \geq [G, G]$ és $p > 2$, vagy ha $G^4 \geq [G, G]$ és $p = 2$.

(*ii*) G *egyenletesen hatványteljes* (uniformly powerful), vagy röviden *egyenletes*, ha hatványteljes, és az alsó centrális p-láncának $P_i(G)/P_{i+1}(G)$ $(i \geq 1)$ szeletei mind egyenlő, p^d rendűek. G *dimenzió*ja ekkor definíció szerint d.

Az egyenletes pro-p csoportok azért fontosak, illetve viszonylag könnyen kezelhetők, mert bevezethető rajtuk egy $\mathbb{Z}_p$ feletti Lie-algebra struktúra. Az összeadás és a Lie-szorzás a csoportműveletből közvetlenül – és természetes módon – definiálható ([10] Chapter 4). A Lie-algebra dimenziója megegyezik az eredeti egyenletes csoport dimenziójával.

1.1.6. Definíció. Egy pro-p csoport *rang*ja a zárt részcsoportjai minimális generátorszámának szuprémuma. Egy pro-p csoport *véges rangú*, ha ez a szuprémum véges.

1.1.7. Definíció. Legyen (τ) egy csoportelméleti tulajdonság. Egy G csoport *virtuálisan* (τ), ha van (τ) tulajdonságú véges indexű részcsoportja. Egy G topologikus csoport *öröklődően* (τ), ha minden nyílt részcsoportja (τ).

1.1.4. Tétel ([10]). *Egy pro-p csoport pontosan akkor véges rangú, ha virtuálisan egyenletes.*

A pro-p csoportok körében rendkívül fontos szerepet játszanak az úgynevezett p-adikus analitikus csoportok. Fontos alkalmazásaik vannak a számelméletben. A p-adikus egészek feletti csoportalgebrájukat (igazság szerint csak csoportgyűrű, mivel $\mathbb{Z}_p$ nem test) nevezik Iwasawa-algebráknak. Ezek moduluselmélete mostanában rendkívül gyorsan fejlődő ága az algebrának.

1.1.8. Definíció. Egy topologikus teret n-dimenziós *p-adikus analitikus sokaság*nak nevezünk, ha van olyan nyílt fedése, melyben a lefedő halmazok $\mathbb{Z}_p^n$ egy-egy nyílt részhalmazával homeomorfak, továbbá az áttérési függvények p-adikus értelemben analitikusak.

1.1.9. Definíció. Egy topologikus csoportot *p-adikus analitikus*nak hívunk, ha van rajta egy p-adikus analitikus sokaság struktúra, és a szorzás, illetve az invertálás művelete analitikus.

Megjegyzés: Egy p-adikus analitikus csoport nem feltétlenül pro-p csoport. Viszont igaz az alábbi – pusztán csoportelméleti tulajdonságaikkal való – jellemzés:

1.1.5. Tétel ([10]). *Egy G topologikus csoport pontosan akkor p-adikus analitikus, ha nyílt részcsoportként tartalmaz egy véges rangú pro-p csoportot.*

Ez a feltétel az 1.1.4-es tétel szerint ekvivalens azzal, hogy G-nek van egy nyílt, egyenletes pro-p részcsoportja. A p-adikus analitikus csoport dimenziója megegyezik ezen egyenletes részcsoport dimenziójával.

2. fejezet

A Nottingham csoport és tulajdonságai

2.1. A Nottingham csoport megadása

2.1.1. Definíció. Legyen R kommutatív, egységelemes gyűrű! Az

$$f = t\left(1 + \sum_{k=1}^{\infty} \alpha_k t^k\right) \in R[[t]]$$

alakú alakú formális hatványsorok halmazát a kompozícióra nézve az *R Notthingam csoport*jának nevezzük, és $\mathcal{N}(R)$-rel jelöljük.

Azt, hogy ez tényleg egy csoport, először S. Jennings [20] látta be. Ezzel ekvivalensen tekinthetjük $\mathcal{N}(R)$-et úgy is, mint az $R[[t]]$ gyűrű automorfizmuscsoportjának egy részcsoportját: $(t)f := f$, és ez már meghatározza $R[[t]]$ egy folytonos automorfizmusát, amely R-et fixen hagyja. Könnyű ellenőrizni, hogy ez a leképezés csoporthomomorfizmus: $(t)fg = ((t)f)g$. Szakdolgozatomban azzal a speciális esettel foglalkozom, ha R egy $\mathbb{F}_q$ $(q = p^f)$ véges test, és különösképp azzal, amikor $q = p$ prím. Legyen $A(\mathbb{F}_q)$ az

$$f = \sum_{k=1}^{\infty} \alpha_k t^k \in \mathbb{F}_q[[t]] \;\; \alpha_1 \neq 0$$

alakú hatványsorok csoportja a kompozícióra. Ekkor érvényes az alábbi tétel:

2.1.1. Tétel.
$$A(\mathbb{F}_p) \cong \mathrm{Aut}(\mathbb{F}_p[[t]]) \cong \mathrm{Aut}^c(\mathbb{F}_p((t))) \cong \mathrm{Aut}(\mathbb{F}_p((t))),$$
ahol Aut^c *a folytonos automorfizmusok csoportját jelöli.*

Bizonyítás. Egy σ gyűrűautomorfizmus nyilván kiterjed a hányadostestre:

$$\sigma\left(\left(\sum_{k=0}^{\infty} \alpha_k t^k\right)^{-1}\right) = \left(\sigma\left(\sum_{k=0}^{\infty} \alpha_k t^k\right)\right)^{-1}.$$

A visszafelé irányhoz használjuk azt a tényt, hogy $\mathbb{F}_p((t))$-nek csak egyetlen olyan értékelése van, melyre nézve teljes, mégpedig a szokásos:

$$v\left(\sum_{k=-n}^{\infty} \alpha_k t^k\right) = -n, \text{ ha } \alpha_{-n} \neq 0.$$

Node, ha σ egy testautomorfizmus, akkor

$$v_\sigma\left(\sum_{k=-n}^{\infty}\alpha_k t^k\right) := v\left(\sigma\left(\sum_{k=-n}^{\infty}\alpha_k t^k\right)\right)$$

is egy értékelése $\mathbb{F}_p((t))$-nek, melyre nézve teljes, ezért $v_\sigma = v$, azaz σ megtartja az értékelést, tehát folytonos, és megszorítható $\mathbb{F}_p[[t]]$-re. $\square$

Hasonlóan $A(\mathbb{F}_q)$ megegyezik $\mathbb{F}_q((t))$ azon folytonos automorfizmusainak a csoportjával, melyek $\mathbb{F}_q$-t fixen hagyják.

Most definiálom $A(\mathbb{F}_q)$ egy filtrálását: Legyen

$$\mathcal{N}_k(\mathbb{F}_q) = \{\sigma \in A(\mathbb{F}_q) : \sigma(t) - t \in t^{k+1}\mathbb{F}_q[[t]]\}!$$

Ekkor $\mathcal{N}_1 = \mathcal{N}$, és $\mathcal{N}_n \lhd A(\mathbb{F}_q)$, hiszen megegyezik a következő homomorfizmus magjával: Jelölje

$$A_n(\mathbb{F}_q) := \{f : (t)f = \sum_{k=1}^{n}\alpha_k t^k, \text{ ahol } \alpha_k \in \mathbb{F}_q \text{ és } \alpha_1 \neq 0\}$$

$\mathrm{Aut}(\mathbb{F}_q[[t]]/t^{n+1}\mathbb{F}_q[[t]])$ egy $(q-1)q^{n-1}$-rendű részcsoportját, és Φ_n a természetes vetítést:

$$\begin{array}{rcl}\Phi_n : A(\mathbb{F}_q) & \longrightarrow & A_n(\mathbb{F}_q)\\ \left(f : t \mapsto \sum_{k=1}^{\infty}\alpha_k t^k\right) & \longmapsto & \left(f_n : t \mapsto \sum_{k=1}^{n}\alpha_k t^k\right)!\end{array}$$

Ekkor $\mathcal{N}_n = \mathrm{Ker}(\Phi_n)$, $|A(\mathbb{F}_q) : \mathcal{N}| = q-1$ és $|\mathcal{N}_n : \mathcal{N}_{n+1}| = q$. Könnyű látni, hogy $\mathcal{N} = \varprojlim(\mathcal{N}/\mathcal{N}_n)$ egy pro-p csoport, mégpedig $A(\mathbb{F}_q)$ (egyetlen) pro-p-Sylowja.

2.1.2. Definíció. Ha $1 \neq g \in \mathcal{N}$, akkor létezik egy olyan $n \in \mathbb{Z}^+$ egész szám, hogy $g \in \mathcal{N}_n \backslash \mathcal{N}_{n+1}$. Ezt az n-et nevezzük g *mélységének*, és $D(g)$-vel jelöljük. Az egységelem mélysége ∞.

2.1.3. Jelölés. Ha $n \in \mathbb{Z}^+$ és $\alpha \in \mathbb{F}_q$, akkor jelölje $e_n[\alpha] \in \mathcal{N}_n$ azt az elemet, melyre $(t)e_n[\alpha] = t(1+\alpha t^n)$! Legyen továbbá $q = p^f$, és $\mathbb{F}_q$ egy bázisa $\mathbb{F}_p$ fölött $\gamma_1, \gamma_2, \ldots, \gamma_f$.

$\mathcal{N}(\mathbb{F}_q)$ úgy is ismert a számelméletben, mint $\mathbb{F}_q((t))$ vad automorfizmusainak a csoportja. Erre még visszatérek az 5. fejezetben.

2.2. Kommutátor-struktúra

2.2.1. Állítás. *Legyen* $(t)a = t(1+\sum_{k=n}^{\infty}\alpha_k t^k)$, *és* $(t)b = t(1+\sum_{j=l}^{\infty}\beta_j t^j)$ *két tetszőleges elem a Nottingham csoportból! Ekkor* $(t)[a,b] = t(1+(n-l)\alpha_n\beta_l t^{n+l} + \ldots)$.

Bizonyítás.

$$\begin{aligned}(t)ab &= (t)b\left(1+\sum_{k=n}^{\infty}\alpha_k((t)b)^k\right) = t\left(1+\sum_{j=l}^{\infty}\beta_j t^j\right)\left(1+\sum_{k=n}^{\infty}\alpha_k t^k\left(1+\sum_{j=l}^{\infty}\beta_j t^j\right)^k\right) \equiv\\ &\equiv t\left(1+\sum_{k=n}^{n+l}\alpha_k t^k + \sum_{j=l}^{n+l}\beta_j t^j + (n+1)\alpha_n\beta_l t^{n+l}\right) \pmod{t^{n+l+2}\mathbb{F}_q[[t]]}.\end{aligned}$$

Hasonlóan

$$(t)ba \equiv t\left(1+\sum_{j=l}^{n+l}\beta_j t^j+\sum_{k=n}^{n+l}\alpha_k t^k+(l+1)\alpha_n\beta_l t^{n+l}\right) \pmod{t^{n+l+2}\mathbb{F}_q[[t]]}.$$

Legyen most $s \in \mathcal{N}$ olyan, hogy $(t)s = t(1+(n-l)\alpha_n\beta_l t^{n+l})$! Ekkor

$$\begin{aligned}
(t)bas &\equiv (t)s\left(1+\sum_{j=l}^{n+l}\beta_j((t)s)^j+\sum_{k=n}^{n+l}\alpha_k((t)s)^k+(l+1)\alpha_n\beta_l((t)s)^{n+l}\right)\equiv\\
&\equiv t\left(1+(n-l)\alpha_n\beta_l t^{n+l}\right)\left(1+\sum_{j=l}^{n+l}\beta_j t^j+\sum_{k=n}^{n+l}\alpha_k t^k+(l+1)\alpha_n\beta_l t^{n+l}\right)\equiv\\
&\equiv t\left(1+\sum_{j=l}^{n+l}\beta_j t^j+\sum_{k=n}^{n+l}\alpha_k t^k+(l+1)\alpha_n\beta_l t^{n+l}+(n-l)\alpha_n\beta_l t^{n+l}\right)\equiv\\
&\equiv t\left(1+\sum_{j=l}^{n+l}\beta_j t^j+\sum_{k=n}^{n+l}\alpha_k t^k+(n+1)\alpha_n\beta_l t^{n+l}\right)\equiv (t)ab \pmod{t^{n+l+2}\mathbb{F}_q[[t]]},
\end{aligned}$$

mert

$$((t)s)^i = t^i\left(1+(n-l)\alpha_n\beta_l t^{n+l}\right)^i \equiv t^i \pmod{t^{n+l+1}\mathbb{F}_q[[t]]},$$

ha $i \geq 1$. Node ekkor tetszőleges $f \in \mathbb{F}_q[[t]]$-re

$$(f)bas \equiv (f)ab \pmod{t^{n+l+2}\mathbb{F}_q[[t]]},$$

speciálisan $f = (t)a^{-1}b^{-1}$-re is:

$$(t)[a,b] = (t)a^{-1}b^{-1}ab = t(1+(n-l)\alpha_n\beta_l t^{n+l}+\dots),$$

ahogy állítottam. □

2.2.2. Következmény. *Legyen $a, b \in \mathcal{N}$! Ekkor*

$$\begin{aligned}
D([a,b]) &= D(a)+D(b),\ \textit{ha}\ D(a)\not\equiv D(b) \pmod p\\
D([a,b]) &> D(a)+D(b),\ \textit{ha}\ D(a)\equiv D(b) \pmod p.
\end{aligned}$$

2.2.3. Következmény. *Ha $p > 2$, akkor*

$$[\mathcal{N}_n,\mathcal{N}_m] = \overline{[\mathcal{N}_n,\mathcal{N}_m]} = \begin{cases}\mathcal{N}_{n+m}, & \textit{ha}\ n\not\equiv m \pmod p\\ \mathcal{N}_{n+m+1}, & \textit{ha}\ n\equiv m \pmod p.\end{cases}$$

Bizonyítás. Legyen $l \geq n+m$, ha $n \not\equiv m$, és $l > n+m$, ha $n \equiv m \pmod p$. Ekkor van olyan $r \geq n$ és $s \geq m$, melyre $r \not\equiv s$, és $r+s = l$. Ha $\alpha \in \mathbb{F}_q$ tetszőleges, akkor

$$(t)[e_n[1], e_m[\alpha]] = t(1+\alpha t^l+\dots),$$

azaz $[\mathcal{N}_n,\mathcal{N}_m]$-ben van l mélységű, α főegyütthatójú elem, ezért

$$\overline{[\mathcal{N}_n,\mathcal{N}_m]} = \begin{cases}\mathcal{N}_{n+m}, & \text{ha}\ n\not\equiv m \pmod p\\ \mathcal{N}_{n+m+1}, & \text{ha}\ n\equiv m \pmod p.\end{cases}$$

Node egy pro-véges csoportban bármely két zárt részcsoport kommutátora is zárt, azaz $[\mathcal{N}_n,\mathcal{N}_m] = \overline{[\mathcal{N}_n,\mathcal{N}_m]}$. □

2.2.1. Definíció. Egy pro-p csoportot *épp végtelen*nek (just infinite) nevezünk, ha minden nemtriviális zárt normálosztója nyílt, vagy ekvivalensen ha minden valódi homomorf képe véges. Egy pro-p csoport *öröklődően épp végtelen* (hereditarily just infinite), ha minden nyílt részcsoportja épp végtelen.

A pro-p csoportok építőkövei az épp végtelenek, hasonló szerepet játszanak, mint a véges csoportok körében az egyszerűek.

2.2.4. Állítás. *Legyen $p > 2$, és $1 \neq g \in \mathcal{N}$ tetszőleges, $D(g) = n$! Ekkor*

$$\overline{\langle g \rangle^{\mathcal{N}}} = \begin{cases} \langle g, \mathcal{N}_{n+1} \rangle, & \text{ha } n \not\equiv 1 \pmod p \\ \langle g, \mathcal{N}_{n+2} \rangle, & \text{ha } n \equiv 1 \pmod p, \end{cases}$$

így mindenképpen nyílt, azaz $\mathcal{N}$ épp végtelen.

Bizonyítás. Ha $m > n$ (illetve $n \equiv 1 \pmod p$ esetén $m > n+1$), akkor ismételt kommutálással elő tudunk állítani g-ből egy adott főegyütthatójú, m mélységű elemet. □

2.2.5. Tétel. *$\mathcal{N}$ öröklődően épp végtelen.*

Bizonyítás. Csak $p > 2$-re bizonyítom. Legyen $H \leq_o \mathcal{N}$ egy tetszőleges nyílt részcsoport! Ekkor van olyan $n \in \mathbb{Z}^+$, hogy $\mathcal{N}_n \leq H$. Ha $1 \neq g \in H$, $D(g) = m$, akkor $\overline{\langle g \rangle^H} \geq \mathcal{N}_{m+2n+2p-2}$, hiszen ha $m + n \leq k \not\equiv 2m \pmod p$, akkor g-t egy megfelelő $\mathcal{N}_n$-beli elemmel kommutálva egy $t \mapsto t(1 + \alpha t^k + \dots)$ alakú elemet kapunk, ha pedig $m + 2n + 2p - 2 \leq k \equiv 2m$, akkor kommutálhatunk két lépésben. Tehát H minden nemtriviális zárt részcsoportja nyílt, azaz H épp végtelen. □

Megjegyzés: A 2 karakterisztikájú eset Hegedűs Pál [16] eredménye.

2.3. Hatvány-struktúra

A Nottingham csoport hatvány-struktúrájának vizsgálatához bevezetek egy végtelen $M(g)$ mátrixot minden $g \in \mathcal{N}$-re [40]. Mégpedig legyen $M(g) = \{m_{ij}\}$, ahol

$$m_{ij} = t^j \text{ együtthatója } (t^i)g\text{-ben.}$$

Ezt úgy is interpretálhatjuk, hogy g egy lineáris transzformációja a $t\mathbb{F}_p[[t]]$ topologikus vektortérnek, melynek (topologikus) bázisa $t, t^2, t^3, \dots$ Világos, hogy $M(g) = I + U(g)$, ahol I az identitás, $U(g)$ pedig egy szigorúan felső háromszögmátrix. Mivel $\mathrm{char}(\mathbb{F}_q) = p$, ezért $M(g^p) = (I + U(g))^p = I + U(g)^p$.

2.3.1. Lemma. *Ha $D(g) = n$, akkor*

$$\begin{aligned} D(g^p) &= np, \text{ ha } n \equiv 0 \pmod p, \text{ és} \\ &> np, \text{ ha } n \not\equiv 0 \pmod p. \end{aligned}$$

Bizonyítás. Legyen $h \in \mathbb{F}_q[[t]]$ egy tetszőleges formális hatványsor, amely főtagja

$$h \equiv \alpha t^j \pmod{t^{j+1}\mathbb{F}_q[[t]]}$$

valamilyen $\alpha \in \mathbb{F}_q$-ra! Tegyük fel továbbá, hogy $(t)g = t(1 + \sum_{k=n}^{\infty} \beta_k t^k)$! Ekkor

$$\begin{aligned} hM(g) &\equiv \alpha t^j \left(1 + \sum_{k=n}^{\infty} \beta_k t^k\right)^j \equiv \alpha t^j + j\alpha\beta_n t^{n+j} \pmod{t^{n+j+1}\mathbb{F}_q[[t]]}, \text{ ezért} \\ hU(g) &\equiv j\alpha\beta_n t^{n+j} \pmod{t^{n+j+1}\mathbb{F}_q[[t]]}, \text{ és így} \\ hU(g)^p &\equiv j(j+n)(j+2n)\dots(j+(p-1)n)\alpha\beta_n^p t^{pn+j} \pmod{t^{pn+j+1}\mathbb{F}_q[[t]]}. \end{aligned}$$

Ha ez utóbbit alkalmazzuk $h = t$-re, akkor a kívánt állítást kapjuk. □

Megjegyzések:

1. Ha $D(g)$ osztható p-vel, akkor g végtelen rendű. Persze a Nottingham csoportban vannak véges rendű elemek is, sőt, ahogy az 5. fejezetben látni fogjuk, minden véges p-csoport beágyazható $\mathcal{N}$-be.

2. Világos, hogy $\mathcal{N}_n^p \le \overline{\mathcal{N}_n^p} \le \mathcal{N}_{np}$ illetve $p > 2$ esetén $\mathcal{N}_{np} \le \mathcal{N}_{2n+1} = [\mathcal{N}_n, \mathcal{N}_n]$. Így $\mathcal{N}_n$ Frattini részcsoportja

   $$\Phi(\mathcal{N}_n) = [\mathcal{N}_n, \mathcal{N}_n]\mathcal{N}_n^p = [\mathcal{N}_n, \mathcal{N}_n] = \mathcal{N}_{2n+1},$$

   tehát $d(\mathcal{N}_n) = (n+1)f$, azaz $\mathcal{N}_n$ végesen generált minden n-re. Speciálisan $\mathcal{N} = \mathcal{N}_1$ egy $2f$ generátorszámú pro-p csoport és

   $$\mathcal{N} = \overline{\langle e_1[\gamma_i], e_2[\gamma_i] : 1 \le i \le f\rangle}.$$

3. Az előző megjegyzés és a 2.2.1-es állítás miatt:

   $$\Phi(\mathcal{N}(\mathbb{F}_{2^f})_n) \le \mathcal{N}(\mathbb{F}_{2^f})_{2n}.$$

4. $\mathcal{N}$ nem p-adikus analitikus, hiszen az előző két megjegyzés szerint nem véges a rangja.

2.3.2. Tétel. *Ha p páratlan, és $n \equiv 0 \pmod p$, akkor $\mathcal{N}_n^p = \overline{\mathcal{N}_n^p} = \mathcal{N}_{np}$.*

Bizonyítás. A 2.3.1-es lemma miatt $\mathcal{N}_n^p \le \mathcal{N}_{np}$, sőt a bizonyításból az is látszik, hogy

$$e_n[\alpha]^p \equiv e_{np}[\alpha^p] \pmod{\mathcal{N}_{np+1}}.$$

A 2.2.4-es állítás tétel szerint

$$\mathcal{N}_{np} = \overline{\langle e_n[\gamma_i]^p : 1 \le i \le f\rangle^{\mathcal{N}}} \le \overline{\mathcal{N}_n^p} = \mathcal{N}_n^p,$$

hiszen $\mathcal{N}_n$ egy végesen generált pro-p csoport, ezért $\mathcal{N}_n^p$ zárt. (Martinez tétele: [10], p. 34) □

Vegyük észre, hogy g^p felcserélhető g-vel, tehát ha $D(g) = n$, akkor $D(g^p) \equiv D(g)$ a 2.2.2-es következmény szerint, és ezért $D(g^p) \ge np + \bar{n}$, ahol $n \equiv \bar{n} \pmod p$ és $0 \le \bar{n} \le p-1$. Gondosabb számolással belátható a következő tétel [7]:

2.3.3. Tétel. *Ha p páratlan, akkor $\mathcal{N}_n^p = \overline{\mathcal{N}_n^p} = \mathcal{N}_{np+\bar{n}}$, ahol $n \equiv \bar{n} \pmod p$ és $0 \le \bar{n} \le p-1$.*

3. fejezet

A Lie-elméleti módszer és a Hausdorff dimenzió

3.1. A Hausdorff dimenzió és az index-részcsoportok

3.1.1. Definíció. Egy pro-véges csoportra azt mondjuk, hogy megszámlálható bázisú, ha az egységelemnek létezik megszámlálható környezetbázisa.

3.1.2. Definíció. Legyen G egy megszámlálható bázisú pro-véges csoport, és $\{G_n\}$ egy rögzített filtrálása, D a hozzá tartozó mélység! Ekkor megadhatunk egy metrikát G-n, mint topologikus téren: ha $g_1, g_2 \in G$, akkor távolságuk $d(g_1, g_2) = 1/D(g_1^{-1}g_2)$.

Ez valóban metrika, sőt ultrametrika hiszen

1. Szimmetrikus: $D(g_1^{-1}g_2) = D((g_1^{-1}g_2)^{-1}) = D(g_2^{-1}g_1)$
2. $d(g_1, g_2) = 0 \Leftrightarrow D(g_1^{-1}g_2) = \infty \Leftrightarrow g_1 = g_2$
3. Nemcsak a háromszögegyenlőtlenség, hanem az ultrametrikus egyenlőtlenség is teljesül:

$$d(g_1, g_3) = 1/D(g_1^{-1}g_3) \leq \max(1/D(g_1^{-1}g_2), 1/D(g_2^{-1}g_3)) = \max(d(g_1, g_2), d(g_2, g_3)).$$

Így G egy kompakt, teljes metrikus tér, hiszen minden Cauchy-sorozat konvergens, és a topológia megegyezik G eredeti topológiájával. Egy $H \subseteq G$ zárt részhalmaz *Hausdorff dimenzió*ját értelmezhetjük a valós függvénytanból megismert módon. Ha H részcsoport is, akkor dimenziója kiszámolható az alábbi formulával:

$$\mathrm{hdim}(H) = \mathrm{hdim}_G(H) = \liminf_{n\to\infty} \frac{\log|HG_n : G_n|}{\log|G : G_n|} = \liminf_{n\to\infty} \frac{\log|H : H \cap G_n|}{\log|G : G_n|}.$$

Tulajdonságok:

1. Egy zárt részcsoport Hausdorff dimenziója tehát egy 0 és 1 közötti valós szám.
2. Ha $H_1 \leq H_2$, akkor $\mathrm{hdim}(H_1) \leq \mathrm{hdim}(H_2)$.
3. H pontosan akkor nyílt, ha $\mathrm{hdim}(H) = 1$.

4. Ha H véges, akkor $\mathrm{hdim}(H) = 0$.

3.1.3. Definíció. Egy G pro-véges csoport *Hausdorff spektruma* a $[0,1]$ intervallum egy részhalmaza: $\mathrm{hspec}(G) := \{\mathrm{hdim}(H) : H \leq_c G\}$.

A Nottingham csoport Hausdorff spektrumának meghatározásában fontos szerepet játszanak az ún. index-részcsoportok, melyeket Barnea és Klopsch definiált épp erre a célra [3]:

3.1.4. Definíció. Egy $I \subseteq \mathbb{Z}^+$ részhalmazhazhoz értelmezzük

$$\mathcal{N}[I] := \left\{ t\left(1 + \sum_{i \in I} a_i t^i\right)\right\}$$

zárt részhalmazát $\mathcal{N}$-nek. Ha $\mathcal{N}[I] \leq \mathcal{N}$ egy részcsoport, akkor I-t *megengedett indexhalmaz*nak, $\mathcal{N}[I]$-t pedig (az I-hez tartozó) *indexrészcsoport*nak nevezzük.

A következő elemi lemma a későbbi példákban lesz fontos:

3.1.1. Lemma. *Legyen $i, n \in \mathbb{Z}^+$ pozitív egészek p-es számrendszerbeli alakja $i = \sum_{m=0}^{\infty} i_m p^m$ illetve $n = \sum_{m=0}^{\infty} n_m p^m$! Ekkor $p \nmid \binom{i}{n}$ akkor és csak akkor, ha minden $m \in \mathbb{N}$-re $i_m \geq n_m$.*

Bizonyítás. Közismert állítás, hogy $k!$ prímtényezős felbontásában p a

$$\left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \cdots + \left[\frac{k}{p^j}\right] + \cdots = \sum_{j=1}^{\infty} \left[\frac{k}{p^j}\right] \text{-edik}$$

kitevőn szerepel, ahol a szögletes zárójel az egészrészt jelöli. Tehát $\binom{i}{n} = \frac{i!}{n!(i-n)!}$-ban p a

$$\sum_{j=1}^{\infty} \left(\left[\frac{i}{p^j}\right] - \left[\frac{n}{p^j}\right] - \left[\frac{i-n}{p^j}\right] \right) \text{-edik}$$

hatványon szerepel. Viszont $[a] + [b] \leq [a+b]$, és egyenlőség pontosan akkor áll fenn, ha $\{a\} + \{b\} < 1$ (ahol a kapcsos zárójel a törtrészt jelöli). Tehát $p \nmid \binom{i}{n}$ ekvivalens azzal, hogy $\left\{\frac{n}{p^j}\right\} + \left\{\frac{i-n}{p^j}\right\} < 1$ minden $j \geq 1$ egész számra. Ez pedig könnyen láthatóan ekvivalens az állításban szereplő feltétellel. $\square$

3.1.2. Lemma. *Legyen G egy pro-véges csoport, és H egy zárt részfélcsoportja! Ekkor H részcsoportja is G-nek.*

Bizonyítás. Ha $h \in H$, akkor $\lim\limits_{s \to \infty} h^{p^s - 1} = h^{-1} \in H$. $\square$

3.1.3. Tétel. *$I \subseteq \mathbb{Z}^+$ pontosan akkor megengedett indexhalmaz, ha minden $i \in I$ és $1 \leq n \leq i+1$, $\binom{i+1}{n} \not\equiv 0 \pmod{p}$-re $\{i + nj : j \in I\} \subseteq I$.*

Bizonyítás. Egyik irány: Ha I megengedett indexhalmaz, és $i, j \in I$, akkor $e_i[1]e_j[1] \in \mathcal{N}[I]$, azaz

$$(t)e_i[1]e_j[1] = t + t^{j+1} + (t + t^{j+1})^{i+1} = t + t^{j+1} + \sum_{n=0}^{i+1} \binom{i+1}{n} t^{i+nj+1} \text{ miatt}$$

$\binom{i+1}{n} \not\equiv 0 \pmod{p}$ esetén $i + nj \in I$.
Másik irány: Tegyük fel, hogy I kielégíti a feltételt! Legyen $H := \mathcal{N}[I]$,

$$S := \{e_i[a] : i \in I, a \in \mathbb{F}_q\} \subseteq H,$$

és az S által generált részfélcsoport

$$\hat{S} := \{f_1 f_2 \dots f_r : r \in \mathbb{N} \text{ és } f_m \in S, \text{ ha } 1 \leq m \leq r\}!$$

Elég belátni, hogy $\overline{\hat{S}} = H$, mert részfélcsoport lezártja szintén részfélcsoport, sőt a 3.1.2-es lemma szerint részcsoport is.
Állítás: $\overline{\hat{S}} \subseteq H$.
Bizonyítás. Mivel H zárt, ezért elég belátni, hogy $\hat{S} \subseteq H$, sőt $S \subseteq H$ miatt azt kell megmutatni, hogy $HS \subseteq H$. Tehát legyen $(t)h = t(1 + \sum_{i \in I} h_i t^i) \in H$ és $(t)f = t(1 + at^j) \in S$. Ekkor

$$(t)hf = t + at^{j+1} + \sum_{i \in I} h_i (t + t^{j+1})^{i+1} = t + at^{j+1} + \sum_{i \in I} h_i \sum_{n=0}^{i+1} \binom{i+1}{n} a^n t^{i+nj+1} \in H,$$

azaz az állítást beláttuk.

A bizonyításból az is látszik, hogy $(H \cap \mathcal{N}_n)/\mathcal{N}_{n+1} = (\hat{S} \cap \mathcal{N}_n)/\mathcal{N}_{n+1}$ és így $H\mathcal{N}_{n+1}/\mathcal{N}_{n+1} = \hat{S}\mathcal{N}_{n+1}/\mathcal{N}_{n+1}$ minden $n \in \mathbb{Z}^+$-re. Tehát $H = \overline{\hat{S}}$. □

3.1.4. Példa. *Néhány fontos index-részcsoportja a Nottingham csoportnak:*

1. $\mathfrak{A}_s := \mathcal{N}[s\mathbb{Z}^+]$, *ahol* $s \in \mathbb{Z}^+$*;*
2. $\mathfrak{B}_{r,s} := \mathcal{N}[p^r\mathbb{Z}^+ \cup (p^s\mathbb{Z}^+ - 1)]$, *ahol* $r, s \in \mathbb{Z}^+$, *és* $r \geq s$*;*
3. $\mathfrak{C}_s := \mathcal{N}[p^s\mathbb{Z}^+ - 1]$, *ahol* $s \in \mathbb{Z}^+$*;*
4. $\mathfrak{D} := \mathcal{N}[\{p^n - 1 : n \in \mathbb{Z}^+\}]$.

Bizonyítás. Használjuk a 3.1.3-as tétel feltételét a megengedett indexhalmazokra! Ebből az könnyen látszik, hogy $\mathfrak{A}_s$ és $\mathfrak{D}$ index-részcsoport. $\mathfrak{B}_{r,s}$-hez és $\mathfrak{C}_s$-hez legyen először $i \equiv -1 \pmod{p^s}$ és $n \in \mathbb{Z}^+$ olyan, hogy $p \nmid \binom{i+1}{n}$! Ekkor a 3.1.1-es lemma miatt $n \equiv 0 \pmod{p^s}$, tehát tetszőleges j-re $i + nj \in p^s\mathbb{Z}^+ - 1 \subseteq p^r\mathbb{Z}^+ \cup (p^s\mathbb{Z}^+ - 1)$, így a 3-ast már be is láttuk. A 2-es fennmaradó részéhez legyen most $i \equiv 0 \pmod{p^r}$! Ekkor a 3.1.1-es lemma szerint 3 eset van:

(i) Ha $n \equiv 0 \pmod{p^r}$, akkor $i + nj \equiv 0 \pmod{p^r}$.

(ii) Ha $n \equiv 1 \pmod{p^r}$ és $j \equiv -1 \pmod{p^r}$, akkor $r \geq s$-ből következik, hogy $i + nj \equiv nj \equiv j \equiv -1 \pmod{p^s}$.

(iii) Ha $n \equiv 1 \pmod{p^r}$ és $j \equiv 0 \pmod{p^r}$, akkor $i + nj \equiv 0 \pmod{p^r}$.

Tehát mindhárom esetben $i + nj \in p^r\mathbb{Z}^+ \cup (p^s\mathbb{Z}^+ - 1)$, és épp ezt akartuk. □

Megjegyzések:

1. Ha s és p relatív prímek, akkor $\mathfrak{A}_s \cong \mathfrak{A}_1 = \mathcal{N}$, sőt, $\mathfrak{A}_{sp^r} \cong \mathfrak{A}_{p^r}$.
2. Ha $p \mid s$, akkor a 2.3.1-es lemma szerint $\mathfrak{A}_s$ torziómentes. I. Fesenko belátta, hogy $\mathfrak{A}_{p^r}$ öröklődően épp végtelen [13]. Erre még visszatérek az 5. fejezetben.

3.2. A Nottingham csoport Lie-algebrája

3.2.1. Definíció. Legyen

$$L(\mathcal{N}) := \bigoplus_{i=1}^{\infty} \mathcal{N}_i/\mathcal{N}_{i+1}!$$

Ez természetes módon egy $\mathbb{F}_q$ feletti vektortér, melynek (topologikus) generátorain megadhatunk egy Lie-szorzást az alábbi módon: Ha $D(g) = i$, és $D(h) = j$, akkor $[g\mathcal{N}_{i+1}, h\mathcal{N}_{j+1}] := [g,h]\mathcal{N}_{i+j+1}$. Az így kapott fokszámozott Lie-algebrát nevezzük az $\mathcal{N}$ Nottingham csoport (kongruencia filtrálásra vonatkozó) *diszkrét Lie-algebrá*jának. A részalgebrák miatt kényelmesebb lesz $L(\mathcal{N})$-et csak $\mathbb{F}_p$, és nem $\mathbb{F}_q$ feletti Lie-algebraként tekinteni.

A 2.2.1-es állítás szerint $L(\mathcal{N}(\mathbb{F}_q))$ izomorf a Witt algebra pozitív részével:

$$W^+ = \mathrm{Der}^+\mathbb{F}_q[t] = \bigoplus_{i=1}^{\infty} \mathbb{F}_q e_i\text{-vel},$$

ahol $e_i = t^{i+1}\partial_t$, és $[e_i, e_j] = (j-i)e_{i+j}$. Egy izomorfizmust megadhatunk az alábbi módon:

$$\mathrm{LT}\colon t(1+\alpha t^n + \dots)\mathcal{N}_n \mapsto \alpha e_n.$$

3.2.2. Definíció. Tegyük teljessé $L(\mathcal{N})$-et az $\{L^n\}$ filtrálásra nézve, ahol $L^n = \bigoplus_{k=n}^{\infty} \mathbb{F}_q e_k$, a kapott Lie-algebrát jelöljük $\mathrm{Lie}(\mathcal{N})$-nel, és nevezzük a Nottingham csoport *(teljes) Lie-algebrá*jának.

Ekkor $\mathrm{Lie}(\mathcal{N})$-et interpretálhatjuk úgy is, mint az $\mathbb{F}_q[[t]]$ pronilpotens gyűrű pronilpotens deriválásainak a pozitív része ($\mathrm{Der}^+(\mathbb{F}_q[[t]])$): minden $u \in \mathrm{Lie}(\mathcal{N})$ felírható $u = f\partial_t$ alakban, ahol $f \in t^2\mathbb{F}_q[[t]]$, és $[f\partial_t, g\partial_t] = (f\partial_t g - g\partial_t f)\partial_t$. Így ezen a Lie-algebrán természetes módon hat a Nottingham csoport: ha $u \in \mathrm{Der}^+(\mathbb{F}_q[[t]])$ egy deriválás, és $g \in \mathcal{N}(\mathbb{F}_q)$, akkor

$$(gu)(r) := u(rg)g^{-1}.$$

Ez a hatás megadható az alábbi formulával is, és könnyű ellenőrizni, hogy hű:

$$g(p(t)\partial_t) = \frac{p(tg)}{\partial_t(tg)}\partial_t.$$

Ebből az is látszik, hogy $\mathcal{N}$ hatása nem tartja meg a fokszámot, de az $\{L^n\} = \{\prod_{i=n}^{\infty} \mathbb{F}_q e_i\}$ filtrálást igen, hiszen ha $u \in L(\mathcal{N}) \subset \mathrm{Lie}(\mathcal{N})$ egy homogén elem, akkor $g(u) = u + [\mathrm{LT}g, u]+$ magasabb fokú tagok.

Most definiálom néhány természetes részalgebráját $\mathrm{Lie}(\mathcal{N})$-nek.

3.2.3. Definíció. Ha $s \in \mathbb{Z}^+$, $0 < r < p^s/2$, és $p \nmid r$, továbbá $H \leq \mathcal{N}$, akkor legyen

$$\begin{aligned}
\mathrm{Lie}_s(\mathcal{N}) &:= \prod_{i=1}^{\infty} \mathbb{F}_q e_{si}, \\
\mathfrak{q}(s,r) &:= \prod_{n \equiv 0, \pm r\ (p^s)} \mathbb{F}_q e_n, \\
\mathrm{LT}(H) := \overline{\langle \mathrm{LT}(h) : h \in H \rangle} &= \prod_{n=1}^{\infty} (H \cap \mathcal{N}_n)\mathcal{N}_{n+1}/\mathcal{N}_{n+1}!
\end{aligned}$$

Megjegyzések:

1. Ha $\mathrm{Lie}(\mathcal{N})$-et $\mathbb{F}_q$ és nem $\mathbb{F}_p$ feletti Lie-algebrának tekintenénk, akkor $\mathrm{LT}(H)$ nem feltétlenül lenne részalgebra.
2. $\mathrm{LT}(\mathcal{N}_n) = L^n$.
3. Ha $(s,p)=1$, akkor $\mathrm{Lie}_s(\mathcal{N}) \cong \mathrm{Lie}(\mathcal{N})$.

A Hausdorff dimenzió fogalma analóg módon kiterjeszthető a Lie-algebra részalgebráira is:

3.2.4. Definíció. Legyen K egy teljes Lie-algebra az K^n véges kodimenziós részalgebrákból álló filtrálásra nézve, és $L \leq K$ egy zárt részalgebra! Ekkor L *Hausdorff dimenzió*ja

$$\mathrm{hdim} L = \mathrm{hdim}_K L := \liminf_{n\to\infty} \frac{\dim((L+K^n)/K^n)}{\dim(K/K^n)}.$$

Speciálisan ha $K = \mathrm{Lie}(\mathcal{N})$, és a filtrálás a szokásos $L^n = \prod_{i=n}^{\infty} \mathbb{F}_q e_i$, akkor

$$\mathrm{hdim}_{\mathrm{Lie}(\mathcal{N})} = \liminf_{n\to\infty} \frac{\dim((L+L^n)/L^n)}{\dim(\mathrm{Lie}(\mathcal{N})/L^n)} = \liminf_{n\to\infty} \frac{\log|(L+L^n)/L^n|}{\log|\mathrm{Lie}(\mathcal{N})/L^n|}.$$

Az alábbi állítás összekapcsolja a részalgebrák Hausdorff dimenzióját a részcsoportok Hausdorff dimenziójával.

3.2.1. Állítás. *Ha $H \leq \mathcal{N}$, akkor $\mathrm{hdim} H = \mathrm{hdim}_{\mathrm{Lie}(\mathcal{N})}\mathrm{LT}(H)$, sőt minden $n \in \mathbb{Z}^+$-re*

$$\frac{\log|H\mathcal{N}_n/\mathcal{N}_n|}{\log|\mathcal{N}/\mathcal{N}_n|} = \frac{\log|(\mathrm{LT}(H)+L^n)/L^n|}{\log|\mathrm{Lie}(\mathcal{N})/L^n|}.$$

Bizonyítás. Legyen $H \leq \mathcal{N}$ egy tetszőleges zárt részcsoportja a Nottingham csoportnak! Elég belátni, hogy $\dim((\mathrm{LT}(H)+L^n)/L^n) = k$ esetén $|H\mathcal{N}_n : \mathcal{N}_n| = p^k$. Mivel $(\mathrm{LT}(H) + L^n)/L^n$ egy homogén elemek által generált részalgebra $\mathrm{Lie}(\mathcal{N})/L^n$-ben, ezért vehetjük egy homogén elemekből álló ($\mathbb{F}_p$ feletti) bázisát. Rendezzük sorba a bázis elemeit úgy, hogy a nagyobb mélységű elem legyen hátrébb (az azonos mélységű elemeket egymás között bárhogy rendezhetjük):

$$D(u_1) \leq D(u_2) \leq \cdots \leq D(u_k).$$

Ekkor minden $1 \leq i \leq k$-ra van olyan $h_i \in H$, hogy $\mathrm{LT}(h_i) = u_i$. Vegyük tehát a

$$\pi : (\mathrm{LT}(H)+L^n)/L^n \longrightarrow H\mathcal{N}_n/\mathcal{N}_n$$

$$\pi(\lambda_1 u_1 + \lambda_2 u_2 \cdots + \lambda_k u_k) = h_1^{\lambda_1} h_2^{\lambda_2} \ldots h_k^{\lambda_k}\mathcal{N}_n$$

leképezést (ahol $0 \leq \lambda_i \leq p-1$), és legyen $D(h_1^{\lambda_1} h_2^{\lambda_2} \ldots h_k^{\lambda_k}) = D(u_r) < D(u_{r+1})$ (valójában ez esetben $D(u_1) = D(u_2) = \cdots = D(u_r)$)! Ekkor

$$\mathrm{LT}(h_1^{\lambda_1} h_2^{\lambda_2} \ldots h_k^{\lambda_k}) = \lambda_1 u_1 + \cdots + \lambda_r u_r \neq 0,$$

hiszen a nagyobb mélységű tagok nem számítanak az LT függvénynél. Ha belátom, hogy π kölcsönösen egyértelmű, akkor kész a bizonyítás, mert $|(\mathrm{LT}(H)+L^n)/L^n| = p^k$.
Injektivitás: Tegyük fel indirekten, hogy valamely ($0 \leq \lambda_i, \mu_j \leq p-1$)-re

$$h_1^{\lambda_1} h_2^{\lambda_2} \ldots h_k^{\lambda_k}\mathcal{N}_n = h_1^{\mu_1} h_2^{\mu_2} \ldots h_k^{\mu_k}\mathcal{N}_n!$$

Vegyük azt az ellenpéldát, melyre az első nem nulla együttható a legnagyobb indexű! Node

$$\lambda_1 u_1 + \cdots + \lambda_r u_r = \mathrm{LT}(h_1^{\lambda_1} h_2^{\lambda_2} \dots h_k^{\lambda_k}) = \mathrm{LT}(h_1^{\mu_1} h_2^{\mu_2} \dots h_k^{\mu_k}) = \mu_1 u_1 + \cdots + \mu_s u_s,$$

ezért $r = s$, és $1 \le i \le r$ esetén $\lambda_i = \mu_i$, azaz az első nem nulla tagok megegyeznek, ami ellentmondás, mert egyszerűsíthetünk velük.
Szürjektivitás: Tegyük fel indirekten, hogy π nem szürjektív, és vegyük a legnagyobb mélységű $h\mathcal{N}_n$ elemet, mely nem áll elő képként! Ekkor $\mathrm{LT}(h) = \lambda_{r_1} u_{r_1} + \lambda_{r_1+1} u_{r_1+1} + \cdots + \lambda_{r_2} u_{r_2}$ egy homogén elem $(\mathrm{LT}(H) + L^n)/L^n$-ben, melyre

$$D(u_{r_1-1}) < D(h) = D(u_{r_1}) = \cdots = D(u_{r_2}) < D(u_{r_2+1}).$$

Vegyük $h_{r_2}^{-\lambda_{r_2}} \dots h_{r_1}^{-\lambda_{r_1}} h\mathcal{N}_n$-et. Ennek mélysége nagyobb, mint $D(h)$, tehát előáll

$$h_{r_2}^{-\lambda_{r_2}} \dots h_{r_1}^{-\lambda_{r_1}} h\mathcal{N}_n = h_{r_2+1}^{\lambda_{r_2+1}} \dots h_k^{\lambda_k} \mathcal{N}_n$$

alakban, ahol az első szorzótényező azért csak $h_{r_2+1}^{\lambda_{r_2+1}}$, mert egy elem előállításában nem szerepelhetnek kisebb mélységű elemek. Ez viszont ellentmondás, mert $h_{r_2}^{\lambda_{r_2}} \dots h_{r_1}^{\lambda_{r_1}}$-nel átszorozva $h\mathcal{N}_n$ egy elölállítását kapjuk. $\square$

3.3. Nem-nyílt részcsoportok

Ebben és a következő alfejezetben legyen $q = p \ge 5$ prím, és $\mathcal{N} = \mathcal{N}(\mathbb{F}_p)$!

3.3.1. Lemma. *Legyen $L \le \mathrm{Lie}(\mathcal{N})$ index-részalgebra a Nottingham csoport Lie-algebrájában. Ekkor ha L nem nyílt, akkor részalgebrája valamely $p' \ne p$ prímre $\mathrm{Lie}_{p'}(\mathcal{N})$-nek, vagy valamely $0 < r < p$-re $\mathfrak{q}(1, r)$-nek.*

Bizonyítás. Tegyük fel, hogy $L \not\le \mathfrak{q}(1, r)$ semmilyen $0 < r < p$ egészre. Ekkor léteznek olyan $a, b \in L$ elemek, melyekre

$$D(a), D(b) \not\equiv 0 \text{ és } D(a) \not\equiv \pm D(b) \pmod p.$$

Legyen $s = (D(a), D(b))$ a mélységek legnagyobb közös osztója! Azt állítom, hogy ekkor minden elég nagy $m \in \mathbb{Z}$ egészre van L-ben ms mélységű elem. Ehhez definiálom egy pozitív egész szám megengedhető partícióját. Egy $\{b_i\}_{i=1}^t$ sorozatot $m_0 \in \mathbb{Z}^+$ pozitív egész szám *megengedhető partíció*jának nevezünk, ha az alábbi feltételek teljesülnek:

(*i*) minden b_i $D(a)$-val vagy $D(b)$-vel egyenlő,

(*ii*) ha $s_k = \sum_{i=1}^k b_i$, akkor $s_k \not\equiv b_{k+1} \pmod p$,

(*iii*) $s_t = m_0$.

Először belátom, hogy létezik olyan M és l, hogy minden $m > M$-re ms-nek van egy (*i*)-et és (*iii*)-at kielégítő partíciója, melyre $|u - v| \le l$, ahol u a $D(a)$-val, v pedig a $D(b)$-vel egyenlő b_i-k száma. Mivel $(D(a), D(b)) = s$, ezért minden elég nagy, s-sel osztható számot elő tudunk állítani $uD(a) + vD(b)$ alakban, sőt, u-t $D(b)$-vel csökkentve (növelve), és v-t $D(a)$-val növelve (csökkentve) ugyanannak a számnak a partícióját kapjuk, tehát elérhető, hogy $|u - v| \leq D(a) + D(b)$ legyen. Így l-et választhatjuk $D(a) + D(b)$-nek.

Ha megvan ez a partíciója ms-nek, akkor meg tudjuk konstruálni ms-nek egy megengedhető partícióját is. Vegyük $D(a)$-knak és $D(b)$-knek egy sorozatát úgy, hogy (i) és (ii) teljesüljön, és amikor csak lehet, válasszunk $D(a)$-t! Ekkor minden $D(b)$ után következik legalább két $D(a)$:

$$D(a), D(b), D(a), D(a), \ldots, D(b), D(a), D(a), \ldots$$

Tehát korlátos sok lépés után épp $(u - v)$-vel több $D(a)$ van a sorozatban, mint $D(b)$. Mivel $(u-v)$ korlátos m-től függetlenül, ezért feltehetjük, hogy a b_i-k összege kisebb, mint ms. Most egészítsük ki a sorozatot váltakozó $D(a)$-kkal és $D(b)$-kkel úgy, hogy közben (ii)-t figyelmen kívül hagyjuk, és az összeg ms legyen. Végül cseréljük meg a szomszédos $D(a)$-kat és $D(b)$-ket a párokon belül úgy, hogy (ii) teljesüljön. Ezt megtehetjük, hiszen ha $x \equiv D(a)$ vagy $x + D(a) \equiv D(b) \pmod p$, akkor $x \not\equiv D(b)$ és $x + D(b) \not\equiv D(a) \pmod p$.

Tehát van egy olyan $N \in \mathbb{N}$, hogy $N < ms$ esetén ms-nek van megengedhető partíciója. Mivel a 2.2.1-es következmény szerint $D(x) \not\equiv D(y)$ esetén $D([x,y]) = D(x) + D(y)$, ezért L-ben van ms mélységű elem minden ilyen m-re. Most ha $L \not\leq \mathrm{Lie}_{p'}(\mathcal{N})$ semmilyen $p' \neq p$ prímre, akkor van L-ben s-sel nem osztható mélységű elem, sőt $(s,p) = 1$ miatt (esetleg további kommutátorképzéssel) olyan is, aminek mélysége p-vel sem osztható, és az előbbi módszer ismételt alkalmazásával látható, hogy minden elég nagy m-re L-ben van m mélységű elem is, azaz L nyílt. □

3.3.2. Következmény. *$\mathrm{Lie}(\mathcal{N})$ maximális nem-nyílt index-részalgebrái pontosan a $\mathrm{Lie}_{p'}(\mathcal{N})$ és a $\mathfrak{q}(1,r)$ alakú részalgebrák.*

Bizonyítás. A 3.3.1-es lemma bizonyításából az is látszik, hogy ezek a részalgebrák maximálisak a nem-nyíltak között. □

3.3.3. Következmény. *Ha $L \leq \mathrm{Lie}(\mathcal{N})$ egy nem-nyílt részalgebra, akkor minden $\varepsilon > 0$-ra létezik olyan $n_0 \in \mathbb{Z}^+$, melyre $n_0 < n$ esetén*

$$\frac{\log |(L + L^n)/L^n|}{\log |\mathrm{Lie}(\mathcal{N})/L^n|} \leq \max\left(\frac{3}{p} + \varepsilon, \frac{1}{2}\right).$$

Bizonyítás. Alkalmazzuk a 3.3.1-es lemmát, és vegyük észre, hogy

$$\lim_{n\to\infty} \frac{\log |(\mathrm{Lie}_{p'}(\mathcal{N}) + L^n)/L^n|}{\log |\mathrm{Lie}(\mathcal{N})/L^n|} = \frac{1}{q} - 0 \leq \frac{1}{2}, \text{ és}$$

$$\lim_{n\to\infty} \frac{\log |(\mathfrak{q}(1,r) + L^n)/L^n|}{\log |\mathrm{Lie}(\mathcal{N})/L^n|} = \frac{3}{p}.$$

□

3.3.4. Következmény. *Legyen $H \leq \mathcal{N}$ egy nem-nyílt részcsoportja a Notthingam csoportnak! Ekkor minden $\varepsilon > 0$ pozitív számra létezik olyan $n_0 \in \mathbb{Z}^+$, melyre $n_0 < n$ esetén*

$$\frac{\log |H\mathcal{N}_n/\mathcal{N}_n|}{\log |\mathcal{N}/\mathcal{N}_n|} \leq \max\left(\frac{3}{p} + \varepsilon, \frac{1}{2}\right).$$

Bizonyítás. Legyen H Lie-algebrája $\mathrm{LT}(H)$! Ekkor $\mathrm{LT}(H) \leq \mathrm{Lie}(\mathcal{N})$ egy nem-nyílt részalgebra, tehát a 3.3.3-as következmény és a 3.2.1-es állítás szerint ha n elég nagy, akkor

$$\frac{\log |H\mathcal{N}_n/\mathcal{N}_n|}{\log |\mathcal{N}/\mathcal{N}_n|} = \frac{\log |(\mathrm{LT}(H) + L^n)/L^n|}{\log |\mathrm{Lie}(\mathcal{N})/L^n|} \leq \max\left(\frac{3}{p} + \varepsilon, \frac{1}{2}\right),$$

ahogy állítottam. □

3.3.5. Tétel. *A Nottingham csoport minden nem-nyílt részcsoportja benne van egy maximális nem-nyílt részcsoportban.*

Bizonyítás. Legyen $H \leq \mathcal{N}$ egy nem-nyílt részcsoportja a Notthingam csoportnak! Ekkor H Hausdorff dimenziója $\mathrm{hdim}H \leq \max(\frac{3}{p}, \frac{1}{2})$, sőt, minden $n_0(\varepsilon) < n$ pozitív egész számra

$$\frac{\log |H\mathcal{N}_n/\mathcal{N}_n|}{\log |\mathcal{N}/\mathcal{N}_n|} \leq \max\left(\frac{3}{p} + \varepsilon, \frac{1}{2}\right)$$

a 3.3.4-es következmény szerint. Alkalmazzuk a Zorn-lemmát a H-t tartalmazó nem-nyílt részcsoportokra! Azt kell ellenőrizni, hogy ha $\{H_i | i \in I\}$ egy felszálló lánca (H-t tartalmazó) nem-nyílt részcsoportoknak, akkor $\cup_{i\in I} H_i$ is egy nem-nyílt részcsoport. Ez a feltétel teljesül, hiszen $\cup_{i\in I} H_i$ triviálisan részcsoport, és

$$\frac{\log |H_i\mathcal{N}_n/\mathcal{N}_n|}{\log |\mathcal{N}/\mathcal{N}_n|} \leq \max\left(\frac{3}{p} + \varepsilon, \frac{1}{2}\right)$$

minden $n_0 < n$ pozitív egészre és $i \in I$-re, tehát

$$\frac{\log |(\cup_{i\in I} H_i)\mathcal{N}_n/\mathcal{N}_n|}{\log |\mathcal{N}/\mathcal{N}_n|} \leq \max\left(\frac{3}{p} + \varepsilon, \frac{1}{2}\right)$$

is teljesül, azaz $\cup_{i\in I} H_i$ sem lehet nyílt, mert a Hausdorff dimenziója

$$\mathrm{hdim}(\cup_{i\in I} H_i) = \liminf_{n\to\infty} \frac{\log |(\cup_{i\in I} H_i)\mathcal{N}_n/\mathcal{N}_n|}{\log |\mathcal{N}/\mathcal{N}_n|} \leq \max\left(\frac{3}{p}, \frac{1}{2}\right) < 1.$$

□

3.3.6. Állítás. *Minden maximális nem-nyílt részcsoport megegyezik a normalizátorával.*

Bizonyítás. Legyen $H < \mathcal{N}$ egy maximális nem-nyílt részcsoport! Ekkor nyilván $H \leq N_{\mathcal{N}}(H)$, tehát ha $H \neq N_{\mathcal{N}}(H)$, akkor H maximalitása miatt $N_{\mathcal{N}}(H)$ nyílt lenne. De $\mathcal{N}$ öröklődően épp végtelen (2.2.5-ös tétel), ezért $N_{\mathcal{N}}(H)$ is épp végtelen, ami azt jelenti, hogy minden zárt normálosztója – speciálisan H is – nyílt. □

3.3.7. Tétel ([6]). *Ha $p \geq 5$, akkor $\mathcal{N}(\mathbb{F}_p)$ alsó rangja 2, azaz $\mathcal{N}(\mathbb{F}_p)$-ben van az egységelemnek két elemmel (de eggyel nem) generált részcsoportokból álló környezetbázisa.*

Bizonyítás. Mivel $\mathcal{N}_n$ nem kommutatív, ezért $\mathcal{N}$ alsó rangja nagyobb, mint 1. Ha H egy nyílt részcsoportja $\mathcal{N}$-nek, akkor $H \geq \mathcal{N}_n$ valamilyen $p \mid n$-re. Ekkor $H \geq \overline{\langle e_{n+1}, e_{n+2}\rangle}$. Node $\mathrm{LT}(\overline{\langle e_{n+1}, e_{n+2}\rangle})$ nyílt a 3.3.1-es lemma miatt, hiszen $(n+1, n+2) = 1$, és sem nullával, sem egymással, sem egymás ellentettjével nem kongruensek modulo p, tehát $\mathrm{LT}(\overline{\langle e_{n+1}, e_{n+2}\rangle})$ nincs benne egyik maximális nem-nyílt részalgebrában sem. Így $\overline{\langle e_{n+1}, e_{n+2}\rangle}$ is nyílt. □

Megjegyzések:

1. Ha $p=3$, akkor $\mathfrak{q}(1,r)=\mathrm{Lie}(\mathcal{N})$, ezért nem maximális részalgebra. Viszont a 3.4.1-es tétel bizonyításában levő gondolatmenet működik, tehát minden nem-nyílt részalgebra részalgebrája $\mathrm{Lie}^+(\mathcal{N})$-nek, $\mathrm{Lie}^-(\mathcal{N})$-nek, vagy valamely $p'\neq 3$ prímre és $0\leq r<p'$-re $\mathrm{Lie}_{p',r}(\mathcal{N})$-nek ahol

$$\begin{aligned}
\mathrm{Lie}^+(\mathcal{N}) &:= \prod_{i\equiv 0,1\ (3)} \mathbb{F}_3 e_i,\\
\mathrm{Lie}^-(\mathcal{N}) &:= \prod_{i\equiv 0,-1\ (3)} \mathbb{F}_3 e_i, \text{ illetve}\\
\mathrm{Lie}_{p',r}(\mathcal{N}) &:= \prod_{\substack{3p'|i \text{ vagy}\\ 3\nmid i\equiv r\ (p')}} \mathbb{F}_3 e_i.
\end{aligned}$$

Ezek a maximális nem-nyílt részalgebrák, így a 3.3.3-as és a 3.3.4-es következmény érvényben marad, csak $\max\left(\frac{3}{p}+\varepsilon,\frac{1}{2}\right)$ helyett $\left(\frac{2}{3}+\varepsilon\right)$-nal.

2. A 3.3.5-ös tétel minden kitétel nélkül érvényes $p=3$-ra is.

3. A Nottingham csoport alsó rangja $p=2$ és 3 esetén is 2 [17]. A $p=3$ eset igazolásához $\langle e_{n+1},e_{n+2}\rangle$ helyett $\langle e_{n+1},g\rangle$-t kell tekinteni, ahol $D(g)=n+2$ és $D(g^3)=3n+8$ (Hegedűs Pál). Ilyen g létezik a 2.3.3-as tétel szerint.

3.4. A Hausdorff spektrum becslése

3.4.1. Tétel. *A Nottingham csoport Lie-algebrájának Hausdorff spektruma:*

$$\mathrm{hspecLie}(\mathcal{N})=\left[0,\frac{2}{p}\right]\cup\left\{\frac{3}{p}\right\}\cup\left\{\frac{1}{s}:s\in\mathbb{Z}^+\right\}.$$

Bizonyítás. Egyik irány: $\mathrm{hspecLie}(\mathcal{N})\supseteq\left[0,\frac{2}{p}\right]\cup\left\{\frac{3}{p}\right\}\cup\left\{\frac{1}{s}:s\in\mathbb{Z}^+\right\}$.
A definícióból nyilvánvaló, hogy $\mathrm{hdimLie}_s(\mathcal{N})=\frac{1}{s}$ és $\mathrm{hdim}\mathfrak{q}(1,r)=\frac{3}{p}$. Másrészt ha $I\subseteq p\mathbb{Z}^+$ tetszőleges, és $J=I\cup(p\mathbb{Z}^++1)$, akkor

$$\begin{aligned}
\mathrm{Lie}(\mathcal{N})[I] &:= \prod_{i\in I}\mathbb{F}_p e_i, \text{ illetve}\\
\mathrm{Lie}(\mathcal{N})[J] &:= \prod_{j\in J}\mathbb{F}_p e_j
\end{aligned}$$

index-részalgebrái $\mathrm{Lie}(\mathcal{N})$-nek, hiszen két tetszőleges modulo p kongruens mélységű homogén elem Lie-szorzata 0 (speciálisan $\mathrm{Lie}(\mathcal{N})[I]$ kommutatív Lie-algebra), egyébként pedig a mélység összeadódik, ezért a szorzás nem vezet ki $\mathrm{Lie}(\mathcal{N})[J]$-ből sem. Ha I-t megfelelően választjuk, akkor $\mathrm{hdimLie}(\mathcal{N})[I]$ tetszőleges $\left[0,\frac{1}{p}\right]$-beli, $\mathrm{hdimLie}(\mathcal{N})[J]$ pedig tetszőleges $\left[\frac{1}{p},\frac{2}{p}\right]$-beli lehet.

Másik irány: hspecLie$(\mathcal{N}) \subseteq \left[0, \frac{2}{p}\right] \cup \left\{\frac{3}{p}\right\} \cup \left\{\frac{1}{s} : s \in \mathbb{Z}^+\right\}$.
Elég index-részalgebrákra belátni az állítást, mert ha $L_1 \leq \mathrm{Lie}(\mathcal{N})$ tetszőleges, akkor minden L_1-beli elem helyett a legkisebb fokú nem-0 homogén részét véve egy $L \leq \mathrm{Lie}(\mathcal{N})$ index-részalgebrát kapunk. Viszont ha egy L zárt index-részalgebra nem nyílt (azaz hdim$L < 1$), akkor a 3.3.1-es lemma szerint részalgebrája valamilyen $p' \neq p$ prímre $\mathrm{Lie}_{p'}(\mathcal{N})$-nek, vagy valamely $0 < r < p$-re $\mathfrak{q}(1, r)$-nek.
1. eset: $L \leq \mathrm{Lie}_{p'}(\mathcal{N})$. Legyen s az a legnagyobb egész szám, melyre $(s, p) = 1$ és $L \leq \mathrm{Lie}_s(\mathcal{N})$. Ekkor mivel $\mathrm{Lie}_s(\mathcal{N}) \cong \mathrm{Lie}(\mathcal{N})$ és s választása miatt nincs olyan $p'' \neq p$, melyre $L \leq \mathrm{Lie}_{p''s}(\mathcal{N})$, ezért a 3.3.1-es lemmát ismét alkalmazva azt kapjuk, hogy vagy $L \leq_o \mathrm{Lie}_s(\mathcal{N})$ és így hdim$L = \frac{1}{s}$, vagy $L \leq \mathrm{Lie}_s(\mathcal{N}) \cap \mathfrak{q}(1, r)$ valamilyen $0 < r < p$-re, azaz hdim$L \leq \frac{3}{ps} \leq \frac{3}{2p} < \frac{2}{p}$.
2. eset: $L \leq \mathfrak{q}(1, r)$. Tegyük fel, hogy hdim$L > \frac{2}{p}$. Ha belátom, hogy ez esetben hdim$L = \frac{3}{p}$, akkor kész a tétel bizonyítása. Ehhez vegyük észre, hogy L-ben kell lennie modulo p 0-val, r-rel, és $(-r)$-rel kongruens mélységű elemnek is, mert elég nagy n-re

$$\frac{\log |(L + L^n)/L^n|}{\log |\mathrm{Lie}(\mathcal{N})/L^n|} \geq \liminf_{k\to\infty} \frac{\log |(L + L^k)/L^k|}{\log |\mathrm{Lie}(\mathcal{N})/L^k|} - \varepsilon > \frac{2}{p},$$

tehát az L-beli mélységek nem lehetnek csak kétféle modulo p mellékosztályból. Sőt,

$$\mathrm{hdim}(L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]) = \mathrm{hdim}(L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N} + r]) = \mathrm{hdim}(L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+ - r]),$$

mert ha

$$\begin{aligned} u_0 &\in L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+], \\ u_r &\in L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N} + r], \text{ és} \\ u_{-r} &\in L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+ - r], \text{ akkor} \end{aligned}$$

$$\begin{aligned} \left[u_r, L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]\right] &\subseteq L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N} + r]; \\ \left[u_r, L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+ - r]\right] &\subseteq L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]; \\ \left[u_{-r}, L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]\right] &\subseteq L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+ - r]; \\ \left[u_{-r}, L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N} + r]\right] &\subseteq L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]. \end{aligned}$$

Másrészt mint vektorterek

$$\begin{aligned} \mathfrak{q}(1, r) &= \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+] \oplus \mathrm{Lie}(\mathcal{N})[p\mathbb{N} + r] \oplus \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+ - r], \text{ és így} \\ L &= L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+] \oplus L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N} + r] \oplus L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+ - r], \text{ tehát} \\ \mathrm{hdim}L &= \mathrm{hdim}(L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]) + \mathrm{hdim}(L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N} + r]) + \\ &+ \mathrm{hdim}(L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+ - r]) = 3\mathrm{hdim}(L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]). \end{aligned}$$

Ha $L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]$-ben az elemek mélységének legnagyobb közös osztója p-nél nagyobb lenne, akkor hdim$L = 3\mathrm{hdim}(L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]) \leq 3\frac{1}{2p} < \frac{2}{p}$ lenne, ami ellentmondás, azaz léteznek olyan $u_0^{(1)}, \ldots, u_0^{(r)} \in L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{Z}^+]$ homogén elemek, melyek mélységének legnagyobb közös osztója: $\left(D(u_0^{(1)}), \ldots, D(u_0^{(r)})\right) = p$. Ez pedig azt jelenti, hogy minden elég nagy p-vel osztható egész szám előáll $\sum_{j=1}^{r} n_j D(u_0^{(j)})$ alakban alkalmas $n_j \in \mathbb{N}$ számokkal. Node

$$\left[u_0^{(j)}, L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N} + r]\right] \subseteq L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N} + r]$$

miatt így minden elég nagy, p-vel osztva r maradékot adó n egész számra ismételt kommutálással kaphatunk egy n mélységű (homogén) elemet $L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N}+r]$-ben. Ebből pedig látszik, hogy $\mathrm{hdim} L = 3\mathrm{hdim}(L \cap \mathrm{Lie}(\mathcal{N})[p\mathbb{N}+r]) = \frac{3}{p}$, és épp ezt kellett bizonyítani. □

3.4.2. Következmény. $\mathrm{hspec}\mathcal{N} \subseteq \left[0, \frac{2}{p}\right] \cup \left\{\frac{3}{p}\right\} \cup \left\{\frac{1}{s} : s \in \mathbb{Z}^+\right\}$.

Bizonyítás. Ha $H \leq_c \mathcal{N}$, akkor $\mathrm{LT}(H) \leq \mathrm{Lie}(\mathcal{N})$ egy index-részalgebra, melyre $\mathrm{hdim} H = \mathrm{hdim}\mathrm{LT}(H)$. □

A Nottingham csoport spektrumának másik irányú becsléséhez részcsoportokat kell konstruálni. Az index-részcsoportok többé-kevésbé megfelelnek erre a célra:

3.4.3. Tétel (Barnea és Klopsch, [3]). *Tetszőleges* $c \in \left[0, \frac{1}{p}\right]$*-re van olyan* $H \leq \mathfrak{C}_1 \leq \mathcal{N}$ *index-részcsoport, melynek Hausdorff dimenziója* $\mathrm{hdim} H = c$. *Továbbá* $\mathrm{hdim}\mathfrak{A}_s = \frac{1}{s}$, *és* $\mathrm{hdim}\mathfrak{B}_{r,s} = \frac{1}{p^r} + \frac{1}{p^s}$.

Így $\left[0, \frac{1}{p}\right] \cup \left\{\frac{1}{p^r} + \frac{1}{p^s} : r, s \in \mathbb{Z}^+\right\} \cup \left\{\frac{1}{s} : s \in \mathbb{Z}^+\right\} \subseteq \mathrm{hspec}\mathcal{N}$. Tehát hiányzik még – néhány pont kivételével – az $\left(\frac{1}{p}, \frac{2}{p}\right)$ intervallum, és a $\frac{3}{p}$ pont. Ha egy H részcsoport Hausdorff dimenziója ebbe a hiányzó halmazba esik, akkor $\mathrm{hdim}\mathrm{LT}(H)$ is, és a 3.4.1-es tétel bizonyításából könnyen látható, hogy ekkor $\mathrm{LT}(H) \leq \mathfrak{q}(1,r)$ valamilyen $0 < r < p$-re. Ezen Lie-algebrák vizsgálatával jutott Ershov a következő eredményre:

3.4.4. Tétel (Ershov, [11]). *Legyen* $\mathcal{Q}(s,r) \leq \mathcal{N}$ *az a részcsoportja a Nottingham csoportnak, ami a*

$$t \mapsto \sqrt[r]{\frac{at^r + b}{ct^r + d}}$$

alakú elemekből áll, ahol $a, b, c, d \in \mathbb{F}_p[[t^{p^s}]]$ *formális hatványsorok, melyek konstans tagjaira teljesül, hogy* $a_0 = d_0 = 1$ *és* $b_0 = 0$. *Ekkor* $\mathcal{Q}(s,r)$ *teljesíti az alábbi tulajdonságokat:*

(*i*) $\mathcal{Q}(s,r) = \mathrm{Stab}_{\mathcal{N}}(\mathfrak{q}(s,r)) = \{\varphi \in \mathcal{N} : \varphi(\mathfrak{q}(s,r)) = \mathfrak{q}(s,r)\}$.

(*ii*) $\mathrm{LT}(\mathcal{Q}(s,r)) = \mathfrak{q}(s,r)$.

Bizonyítás. Először ellenőrizzük, hogy $\mathcal{Q}(s,r)$ részcsoport:

$$\sqrt[r]{\frac{a_2t^r + b_2}{c_2t^r + d_2}} \circ \sqrt[r]{\frac{a_1t^r + b_1}{c_1t^r + d_1}} = \left(\frac{a_2' \cdot \frac{a_1t^r+b_1}{c_1t^r+d_1} + b_2'}{c_2' \cdot \frac{a_1t^r+b_1}{c_1t^r+d_1} + d_2'}\right)^{1/r} = \sqrt[r]{\frac{(a_2'a_1 + b_2'c_1)t^r + (a_2'b_1 + b_2'd_1)}{(c_2'a_1 + d_2'c_1)t^r + (c_2'b_1 + d_2'd_1)}},$$

ahol $a_2' = a_2 \circ \sqrt[r]{\frac{a_1t^r+b_1}{c_1t^r+d_1}}$, stb. Mivel $a_2 \in \mathbb{F}_p[[t^{p^s}]]$, ezért $a_2 \circ w \in \mathbb{F}_p[[t^{p^s}]]$ minden $w \in \mathbb{F}_p[[t]]$-re, tehát $\mathcal{Q}(s,r)$ egy félcsoport. Ugyanakkor zárt is, tehát a 3.1.2-es lemma miatt $\mathcal{Q}(s,r) \leq \mathcal{N}$.

Most megmutatjuk, hogy $\mathcal{Q} \leq K$, ahol $K = \mathrm{Stab}_{\mathcal{N}}(\mathfrak{q}(s,r))$:

$$\begin{aligned}
\sqrt[r]{\frac{at^r + b}{ct^r + d}}(e_i) &= \sqrt[r]{\frac{at^r + b}{ct^r + d}}(t^{i+1}\partial_t) = \frac{\left(\frac{at^r+b}{ct^r+d}\right)^{(i+1)/r}}{\partial_t\left(\sqrt[r]{\frac{at^r+b}{ct^r+d}}\right)}\partial_t = \\
&= \left(\frac{at^r + b}{ct^r + d}\right)^{(i+1)/r+1-1/r} \frac{(ct^r + d)^2}{t^{r-1}(ad - bc)}\partial_t = \\
&= \frac{(at^r + b)^{i/r+1}}{(ct^r + d)^{i/r-1}} \frac{t^{1-r}}{ad - bc}\partial_t,
\end{aligned}$$

hiszen $a' = b' = c' = d' = 0$. Most ha $i = kp^s - r$, akkor

$$\sqrt[r]{\frac{at^r + b}{ct^r + d}}(e_i) = (ct^r + d)^2 \cdot t^{1-r} \cdot R \cdot \partial_t,$$

ahol $R \in \mathbb{F}_p[[t^{p^s}]]$. A jobb oldal viszont

$$\sum_{n \equiv 1, 1+r, 1-r \ (p^s)} \lambda_n t^n \partial_t = \sum_{n \equiv 0, \pm r \ (p^s)} \lambda_{n+1} e_n$$

alakú, azaz eleme $\mathfrak{q}(s,r)$-nek. Az $i = kp^s$ és az $i = kp^s + r$ esetek hasonlóan kezelhetők.

Most azt állítom, hogy $\mathrm{LT}(\mathcal{Q}(s,r)) \geq \mathfrak{q}(s,r)$. Ez világos, hiszen

$$\mathrm{LT}\left(\sqrt[r]{t^r + t^{kp^s}}\right) = \frac{1}{r} e_{kp^s - r}, \quad \mathrm{LT}\left(t\left(1 + t^{kp^s}\right)\right) = e_{kp^s},$$

$$\mathrm{LT}\left(\frac{t}{\sqrt[r]{1 - t^{kp^s + r}}}\right) = \frac{1}{r} e_{kp^s + r}.$$

Végül belátjuk, hogy $\mathfrak{q}(s,r) \geq \mathrm{LT}(K)$. Vegyünk ugyanis egy tetszőleges $\varphi \in K$-t, és legyen $u = \mathrm{LT}\varphi$! Mivel tetszőleges homogén $x \in \mathrm{Lie}(\mathcal{N})$-re $\varphi(x) = x + [u,x]$+magasabb fokú tagok, ezért $[u, \mathfrak{q}(s,r)] \subseteq \mathfrak{q}(s,r)$, és így $u \in \mathfrak{q}(s,r)$, mert $\mathfrak{q}(s,r)$ nyilván megegyezik a normalizátorával. Tehát $\mathrm{LT}(K) \leq \mathfrak{q}(s,r)$. Így azt kaptuk, hogy $\mathrm{LT}(K) \leq \mathfrak{q}(s,r) \leq \mathrm{LT}(\mathcal{Q}(s,r))$, és $\mathcal{Q}(s,r) \leq K$. Ezekből pedig következik a tétel állítása. □

3.4.5. Következmény.

$$\left[0, \frac{1}{p}\right] \cup \left\{\frac{3}{2p}\right\} \cup \left\{\frac{3}{p}\right\} \cup \left\{\frac{1}{s}\right\}_{s=1}^{\infty} \cup \left\{\frac{1}{p} + \frac{1}{p^r}\right\}_{r=1}^{\infty} \subseteq \mathrm{hspec}\mathcal{N} \subseteq \left[0, \frac{2}{p}\right] \cup \left\{\frac{3}{p}\right\} \cup \left\{\frac{1}{s}\right\}_{s=1}^{\infty}.$$

Bizonyítás. A hiányzó két pont: $\mathrm{hdim}\mathcal{Q}(1,r) = \frac{3}{p}$, illetve mivel $\mathfrak{A}_2 \cong \mathcal{N}$, ezért vehetjük ennél az izomorfizmusnál a $\mathcal{Q}(1,r)$-nek megfelelő $\mathcal{Q}_2(1,r)$ részcsoportot, melynek Hausdorff dimenziója $\mathrm{hdim}\mathcal{Q}_2(1,r) = \mathrm{hdim}_{\mathcal{N}}\mathfrak{A}_2 \cdot \mathrm{hdim}_{\mathfrak{A}_2}\mathcal{Q}_2(1,r) = \frac{1}{2} \cdot \frac{3}{p} = \frac{3}{2p}$. □

Megjegyzés: Ez az eddig ismert legjobb eredmény a Nottingham csoport Hausdorff spektrumára. Az $\left(\frac{1}{p}, \frac{2}{p}\right)$ intervallum betöltésére esetleg alkalmas lehet további stabilizátorok meghatározása. Az csak véletlen, hogy a fenti esetben $\mathcal{Q}(s,r)$ megegyezik a Lie-algebrája stabilizátorával. Konjugált részcsoportok Lie-algebrája például azonos, hiszen a konjugálás nem változtat az elemek főtagján, de a Lie-algebrának legfeljebb egyik konjugált lehet csak a stabilizátora, sőt általában egyik sem. Az alábbi példa mutatja, hogy egy részalgebra stabilizátorának Lie-algebrája nem feltétlenül egyezik meg az eredeti részalgebrával:

3.4.6. Példa. *Legyen $\mathfrak{p}_r \leq \mathrm{Lie}(\mathcal{N})$ a modulo p r-rel kongruens mélységű homogén elemek által kifeszített (kommutatív) részalgebra:*

$$\mathfrak{p}_r := \prod_{i \equiv r \ (p)} \mathbb{F}_p e_i!$$

Ekkor $\mathfrak{p}_r$ *stabilizátora:*

$$\begin{aligned}\mathrm{Stab}_{\mathcal{N}}(\mathfrak{p}_r) &= \left\{ t\sqrt[r]{\frac{1+t^p a}{1+t^r b}} : a,b \in \mathbb{F}_p[[t^p]] \right\}, \textit{ ha } 1 \le r \le p-1, \textit{ illetve} \\ \mathrm{Stab}_{\mathcal{N}}(\mathfrak{p}_0) &= \mathfrak{A}_p.\end{aligned}$$

Továbbá $\mathrm{LT}(\mathrm{Stab}_{\mathcal{N}}(\mathfrak{p}_1)) = \prod_{i \equiv 0,1 \ (p)} \mathbb{F}_p e_i$*, tehát* $\mathrm{LT}(\mathrm{Stab}_{\mathcal{N}}(\mathfrak{p}_1)) \neq \mathfrak{p}_1$.

Bizonyítás. Vizsgáljuk meg, hogy egy adott $g \in \mathcal{N}$ elem hová viszi $t^{i+1}\partial_t = e_i$-t. A 3.2-es alfejezetben található képlet szerint:

$$g(t^{i+1}\partial_t) = \frac{((t)g)^{i+1}}{\partial_t((t)g)}.$$

Először legyen $1 \le r \le p-1$. Ekkor $i = kp + r$ választással ha g stabilizálja $\mathfrak{p}_r$-et, akkor

$$\frac{((t)g)^{kp+r+1}}{\partial_t((t)g)} = t^{kp+r+1}(1 + t^p f(t^p))$$

alakú, ahol $f \in \mathbb{F}_p[[t]]$ tetszőleges. Ezt átrendezve

$$\begin{aligned}\frac{1}{t^{kp+r+1}(1+t^p f(t^p))} &= \frac{\partial_t((t)g)}{((t)g)^{kp+r+1}}, \text{ és integrálva} \\ \frac{-r}{t^{kp+r}(1+t^p f(t^p))} &= \frac{-r}{((t)g)^{kp+r}} + h(t^p),\end{aligned}$$

hiszen ha egy formális hatványsor deriváltja 0, akkor $h(t^p)$ alakba írható. Mivel $r \not\equiv 0 \pmod p$, ezért leoszthatunk vele. Ha r-edik gyököt vonunk és felhasználjuk, hogy $((t)g)^{kp}$ csak p-vel osztható kitevőjű tagokat tartalmaz, akkor $(t)g$-nek épp egy kívánt előállítását kapjuk. Másrészt ha $(t)g = \sqrt[r]{\frac{1+t^p a}{1+t^r b}}$, akkor könnyű számolás mutatja, hogy

$$\frac{((t)g)^{kp+r+1}}{\partial_t((t)g)} = t^{r+1}((t)g)^{kp}(1+t^p a) \in t^{r+1}\mathbb{F}_p[[t^p]].$$

Mivel $r = 1$ esetén nem kell gyököt vonni, ezért könnyű ellenőrizni, hogy a stabilizátorban csak nullával és eggyel kongruens mélységű tagok szerepelnek.

A második állításhoz legyen $(t)g = t(1 + \sum_{j=1}^{\infty} a_j t^j)$! Az előzőekhez hasonlóan azt kapjuk, hogy g pontosan akkor stabilizálja $\mathfrak{p}_0$-t, ha

$$\begin{aligned}\frac{(t)g}{\partial_t((t)g)} &\in t\mathbb{F}_p[[t^p]], \text{ azaz ha} \\ 1 + \sum_{j=1}^{\infty} a_j t^j &= \left(1 + \sum_{j=1}^{\infty}(j+1)a_j t^j\right) h(t^p),\end{aligned}$$

ahol $h \in \mathbb{F}_p[[t]]$. Tegyük fel az állítással ellentétben, hogy $g \notin \mathfrak{A}_p$! Most ha k az a legkisebb p-vel nem osztható szám, melyre $a_k \neq 0$, akkor a két oldalt összehasonlítva azt kapjuk, hogy $a_k = (k+1)a_k$, ami ellentmondás. A visszafelé irány – miszerint $\mathfrak{A}_p$ stabilizálja $\mathfrak{p}_0$-t – triviális. □

Megjegyzések:

1. Könnyű igazolni, hogy ez a stabilizátor $r = p - 1$ esetén nem más, mint $\mathfrak{B}_{1,1}$.
2. A bizonyításból látható, hogy a stabilizátor nem változik, ha $\mathfrak{p}_r$ helyett $\mathfrak{p}_r \cap L^n$-et vesszük.

A következő példára az 5.5-ös alfejezetben lesz szükség:

3.4.7. Példa. *Az egydimenziós homogén részalgebrák stabilizátora:*

$$\mathrm{Stab}_{\mathcal{N}}(\mathbb{F}_p e_n) = \begin{cases} \left\{ t \sqrt[n]{\frac{1}{1+t^n a}} : a \in \mathbb{F}_p[[t]] \right\}, & ha\ n \not\equiv 0 \pmod p \\ \{\mathrm{id}\}, & ha\ n \equiv 0 \pmod p). \end{cases}$$

Bizonyítás. Legyen először $n \not\equiv 0 \pmod p$! Ekkor egy $(t)g \in \mathcal{N}$ elem pontosan akkor stabilizálja $\mathbb{F}_p e_n$-et, ha

$$\begin{aligned} t^{n+1}\partial_t = e_n &= g e_n = \frac{((t)g)^{n+1}}{\partial_t((t)g)}\partial_t, \text{ és átrendezve} \\ \partial_t \frac{1}{((t)g)^n} &= \partial_t \frac{1}{t^n}. \end{aligned}$$

Az előző példához hasonlóan integrálva és átrendezve a kívánt állítást kapjuk.

Ha $n \equiv 0 \pmod p$, akkor tegyük fel, hogy egy adott $(t)g = t(1 + \sum_{i=1}^{\infty} g_k t^k) \in \mathcal{N}$ elem stabilizálja $\mathbb{F}_p e_n$-et! Ekkor

$$\begin{aligned} t^{np+1} &= \frac{t^{np+1}\left(1 + \sum_{k=1}^{\infty} g_k t^k\right)^{np+1}}{1 + \sum_{k=1}^{\infty}(k+1) g_k t^k}, \text{ és átrendezve} \\ 1 + \sum_{k=1}^{\infty}(k+1) g_k t^k &= \left(1 + \sum_{k=1}^{\infty} g_k t^k\right)\left(1 + \sum_{k=1}^{\infty} g_k t^{kp}\right)^n \\ \sum_{k=1}^{\infty} k g_k t^k &= \left(1 + \sum_{k=1}^{\infty} g_k t^k\right)\left(\left(1 + \sum_{k=1}^{\infty} g_k t^{kp}\right)^n - 1\right) \end{aligned}$$

Ez pedig azt jelenti, hogy az utolsó egyenletben mindkét oldal 0, azaz $(t)g = t$, mert a bal oldalon nincsen p-vel osztható fokú tag, a jobb oldalon viszont a legkisebb fokú tag p-vel osztható fokú. ☐

Megjegyzés: A fenti két példa állítása igaz marad, ha $\mathbb{F}_p$-t mindenütt egy másik p-karakterisztikájú véges testre, $\mathbb{F}_q$-ra cseréljük.

4. fejezet

Valószínűségi kérdések

4.1. A valószínűségi mező

4.1.1. Definíció. Legyen G egy pro-véges csoport! Ekkor G Borel halmazain megadhatunk egy eltolásinvariáns valószínűségi mértéket, mégpedig a normált Haar-mértéket. Egy részhalmaz mértéke nem más, mint a nyílt normálosztók szerinti faktorokban levő képei mértékének a limesze. A faktorokon a mérték pedig a normált számláló mérték, hiszen azok véges halmazok.

Speciálisan a Nottingham csoporton az így megadott valśzínűségi mérték olyan, hogy $(t)g$ minden együtthatója egymástól függetlenül minden $\mathbb{F}_q$-beli értéket $\frac{1}{q}$ valószínűséggel vesz fel. Az ebben a fejezetben vizsgált kérdéseket A. Shalev vetette fel [32]. Egy adott G pro-véges csoport esetén jelöljük $Q(G,k)$-val azt a valószínűséget, hogy k véletlen elem G-ben nyílt részcsoportot generál. Mann [27] belátta, hogy $Q(G,k) = 1$ valamilyen k-ra, ha G-ben a részcsoportnövekedés polinomiális. Ez utóbbi feltétel pro-p csoportokra azzal ekvivalens, hogy a csoport p-adikus analitikus [10], ezért egy p-adikus analitikus csoportban elég sok (rögzített számú) elem 1 valószínűséggel nyílt részcsoportot generál. A megfordítás már nem igaz: $\mathrm{SL}_d^1(\mathbb{F}_p[[t]])$ ellenpélda [4], ahol ez a csoport $\mathrm{SL}_d(\mathbb{F}_p[[t]])$ első kongruencia részcsoportja, tehát modulo $\mathrm{M}_d(t\mathbb{F}_p[[t]])$ az identitással kongruens mátrixokból áll.

4.1.1. Tétel (Barnea és Larsen, [4]). *Legyen G egy egyszeresen összefüggő egyszerű algebrai csoport egy F p-karakterisztikájú nem-arkhimédeszi lokális test fölött. Ha $p \geq 5$, és Γ egy kompakt, nyílt részcsoportja $G(F)$-nek, akkor $Q(\Gamma, 2) = 1$.*

Ez az eredmény felfogható úgy is, mint Dixon sejtésének (ami azóta már tétel) a lokális testekre vonatkozó analogonja, mely szerint két véletlen eleme egy egyszerű csoportnak 1-hez tartó valószínűséggel generálja az egész csoportot, ha a csoport rendje tart végtelenhez (lásd: [9], [22], [26]). Így természetes a kérdés, hogy vajon a Nottingham csoportban két (vagy esetleg több) véletlen elem nyílt részcsoportot generál-e. Ezt eddig nem sikerült megválaszolnom, de esetleg a maximális nem-nyílt részcsoportok további vizsgálata segíthet. Ugyanis ha sikerülne (konjugált osztály erejéig) osztályozni a maximális nem-nyílt részcsoportokat, akkor (ha – ahogy sejthető – csak megszámlálható sok osztály van), akkor elég lenne megvizsgálni, hogy két elem mekkora valószínűséggel esik egy adott maximális nem-nyílt részcsoport ugyanazon konjugáltjába.

4.2. Szabad részcsoportok

Ebben az alfejezetben azt fogom belátni, hogy 2 véletlen elem $\mathcal{N}$-ben 1 valószínűséggel egy (absztrakt) szabad csoportot generál. Itt természetesen nem topologikus generátumot értek, hiszen a szabad csoport nem pro-p csoport. Ez Szegedy Balázs eredménye [33], az ő bizonyítását közlöm. Az egyszerűség kedvéért legyen $q = p$ prím!

4.2.1. Lemma. *Ha $g \in \mathcal{N}$ és $h \in \mathcal{N}_n$, akkor*

$$(t)g^{-1}hg \equiv t + \frac{(t)hg - (t)g}{\partial_t((t)g)} \pmod{t^{2n+2}\mathbb{F}_p[[t]]}.$$

Bizonyítás. Legyen $f = g^{-1}hg$! Ekkor $(t)hg = (t)gf$. Node felírva a Taylor-formulát:

$$\begin{aligned} g(t + (f(t) - t)) &= g(t) + (f(t) - t)g'(t) + \mathrm{O}((f(t) - t)^2), \text{ és más jelöléssel} \\ (t)gf &\equiv (t)g + ((t)f - t)\partial_t((t)g) \pmod{t^{2n+2}\mathbb{F}_q[[t]]}. \end{aligned}$$

Ezt átrendezve épp az állítást kapjuk. □

4.2.1. Definíció. Ha A egy elemi Abel (nem feltétlenül véges) p-csoport, melyen hat egy G csoport, akkor ez a hatás kiterjed az $\mathbb{F}_pG$ csoportalgebrára, és ezért tekinthetjük A-t mint $\mathbb{F}_pG$ feletti modulust. Ezen a nyelven $u = \sum_{i=1}^{k} \lambda_i g_i$ hatása A-n:

$$v^u = \sum_{i=1}^{k} \lambda_i v^{g_i}.$$

A sűrűségi tétel következménye a következő állítás ([28], Chapter IV, (15.7) Theorem, p. 155):

4.2.2. Állítás. *Legyen X egy metrikus tér, és P_n partícióinak egy sorozata úgy, hogy P_n Borel halmazokból áll, P_n egy finomítása P_{n-1}-nek, és P_n halmazainak az átmérője legfeljebb d_n, ahol d_n tart 0-hoz. Ekkor minden $E \subset X$ Borel halmazra, és minden véges μ Borel mértékre*

$$\lim_{n\to\infty} \frac{\mu(E \cap H_n)}{\mu(H_n)} = 1 \text{ majdnem minden } x \in E\text{-re,}$$

ahol $x \in H_n \in P_n$.

Ezt alkalmazva kapjuk, hogy

4.2.3. Következmény. *Legyen G egy pro-p csoport a G_n filtrálással, $E \subseteq G$ egy Borel halmaz, és μ a (normált) Haar-mérték! Ekkor majdnem minden $x \in E$-re*

$$\lim_{n\to\infty} \frac{\mu(E \cap xG_n)}{\mu(xG_n)} = 1.$$

Megjegyzés: Majdnem minden $x \in E$ azt jelenti, hogy a kivételek halmaza nulla mértékű. Ha $\mu(E) = 0$, akkor az állítás nem mond semmit. Az eredményt csak abban a formában fogom használni, hogy ha $\mu(E) \neq 0$, akkor létezik ilyen x.

4.2.4. Lemma. *Legyen G egy pro-p csoport, G_i és M_i nyílt normálosztói ($i \in \mathbb{Z}^+$), melyekre az alábbi négy állítás teljesül:*

(i) A G_i sorozat G egy filtrálása,

(ii) $G_i > M_i$ minden $i \in \mathbb{Z}^+$-ra,

(iii) a G_i/M_i faktorok elemi Abel p-csoportok minden $i \in \mathbb{Z}^+$-ra,

(iv) a csoportelemek képei lineárisan függetlenek minden $k \in \mathbb{Z}^+$-ra az alábbi természetes leképezéseknél:

$$\begin{array}{rcl} G & \longrightarrow & \mathrm{End}_{\mathbb{F}_p}\left(\bigoplus_{i=k}^{\infty} G_i/M_i\right) \\ g & \longmapsto & ((v_k, v_{k+1}, \dots) \mapsto (v_k^g, v_{k+1}^g, \dots)). \end{array}$$

Ekkor G két véletlen eleme 1 valószínűséggel szabad részcsoportot generál (absztrakt módon).

Bizonyítás. Elég megmutatni, hogy az $F(x,y)$ szabad csoport egy tetszőleges w szavára a $w(a,b) = 1$ egyenlet 0 valószínűséggel teljesül G-ben. Ezt indirekten bizonyítom: tegyük fel az állítással ellentétben, hogy van egy olyan $w \in F(x,y)$, melyre $\mu(\{(a,b) : w(a,b) = 1,\ a,b \in G\}) > 0$, de $\mu(\{(a,b) : s(a,b) = 1,\ a,b \in G\}) > 0$ minden s w-nél rövidebb nemtriviális szóra. (Itt μ a $G \times G$ csoport Haar-mértékét jelöli.) Az általánosság megszorítása nélkül feltehetjük, hogy a w szó x-szel kezdődik. Legyen

$$H := \{(a,b) : w(a,b) = 1,\ a,b \in G\} \setminus \bigcup_{0<l(s)<l(w)} \{(a,b) : s(a,b) = 1,\ a,b \in G\},$$

ahol az l függvény a (redukált) szavak hosszát jelöli. Mivel $\mu(H) > 0$, ezért a 4.2.3-as következmény szerint van egy olyan $(c,d) \in H$ elem és egy pozitív egész k úgy, hogy

$$\frac{\mu(H \cap (cG_i \times dG_i))}{\mu(cG_i \times dG_i)} > \frac{1}{p}$$

minden $i \geq k$-ra.

Legyen $v \in G_i/M_i$ tetszőleges! Megszorozhatjuk c-t és d-t tetszőleges G_i/M_i faktorcsoportbeli elemekkel, és az eredmény szintén G_i/M_i-beli lesz. Könnyű számolás mutatja, hogy

$$w(cv, d) \equiv w(c,d) v^{\lambda_1 g_1 + \lambda_2 g_2 + \dots + \lambda_t g_t} \pmod{M_i},$$

ahol $\lambda = \pm 1$, és a g_i elemek úgy kaphatók, hogy w részszavaiba helyettesítjük c-t és d-t (lásd 4.2.1-es definíció). Ezek a részszavak w szerkezetétől függnek. Például, ha $w = xyx^{-1}yyx$, akkor

$$w(cv, d) \equiv w(c,d) v^{1 - c^{-1}ddc + dc^{-1}ddc} \pmod{M_i}.$$

Jelöljük a

$$\lambda_1 g_1 + \lambda_2 g_2 + \dots + \lambda_t g_t \in \mathbb{F}_p G$$

elemet u-val! Mivel $s(c,d) \neq 1$ semmilyen $0 < l(s) < l(w)$ szóra, ezért a g_i elemek különbözőek. Használva, hogy w x-szel kezdődik, azt kapjuk, hogy $t \geq 1$, és így $u \neq 0$. A lemma utolsó feltétele garantálja, hogy van egy olyan $k_2 \geq k$ egész szám, melyre u természetes hatása G_{k_2}/M_{k_2}-n nem a nulla leképezés. Ebből következik, hogy a

$$\varphi\colon G_{k_2}/M_{k_2} \times G_{k_2}/M_{k_2} \longrightarrow G_{k_2}/M_{k_2}$$

$$\varphi(v_1, v_2) = w(c,d)^{-1} w(cv_1, dv_2)$$

$\mathbb{F}_p$-lineáris leképezés nem tűnik el mindenhol. Node ekkor a magja legalább p indexű részcsoport, azaz

$$\frac{\mu(H \cap (cG_{k_2} \times dG_{k_2}))}{\mu(cG_{k_2} \times dG_{k_2})} \leq \frac{1}{p}.$$

Ez pedig ellentmondás. □

4.2.5. Tétel. *Két véletlen elem $\mathcal{N}(\mathbb{F}_p)$-ben 1 valószínűséggel szabad részcsoportot generál (absztrakt módon).*

Bizonyítás. A 4.2.4-es lemmát alkalmazzuk $G = \mathcal{N}$, $G_i = \mathcal{N}_i$, illetve $M_i = \mathcal{N}_{2i+1}$ választással. A 2.2.3-as következmény és a 2.3.1-es lemma miatt világos, hogy az első három feltétel teljesül. Tegyük fel, hogy egy $0 \neq u \in \mathbb{F}_p\mathcal{N}$ elem nulla leképezést indukál a $\mathcal{N}_i/\mathcal{N}_{2i+1}$ faktorokon minden $i \geq k$-ra! Speciálisan ekkor u a hatásnál a $t(1+t^i) + \mathcal{N}_{2i+1} \in \mathcal{N}_i/\mathcal{N}_{2i+1}$ alakú elemet $t + \mathcal{N}_{2i+1}$-be képezi minden $i \geq k$ esetén. Írjuk u-t

$$u = \lambda_1 g_1 + \lambda_2 g_2 + \cdots + \lambda_t g_t$$

formában, ahol g_i-k különböző csoportelemek, és $\lambda_i \in \mathbb{F}_p$! A 4.2.1-es lemmát alkalmazva kapjuk az alábbi egyenletet:

$$(t + t^{i+1})^u \equiv t + \sum_{j=1}^{n} \lambda_j \frac{((t)g_j)^{i+1}}{\partial_t((t)g_j)} \equiv t \pmod{t^{2i+2}\mathbb{F}_p[[t]]} \text{ minden } i \geq k\text{-ra.}$$

Vezessük be a $\mu_j := \frac{\lambda_j}{\partial_t((t)g_j)} \in \mathbb{F}_p[[t]]$ jelölést! Azt kapjuk, hogy

$$\sum_{j=1}^{n} \mu_j((t)g_j)^{i+1} \equiv 0 \pmod{t^{2i+2}\mathbb{F}_p[[t]]} \text{ minden } i \geq k\text{-ra.}$$

Most legyen $s \geq 0$ rögzített természetes szám, továbbá legyen $i = p^\alpha + s - 1 \geq k$ olyan, hogy $p^\alpha \geq s - 1$. Ezzel a jelöléssel

$$0 \equiv \sum_{j=1}^{n} \mu_j((t)g_j)^{i+1} \equiv \sum_{j=1}^{n} \mu_j((t)g_j)^{p^\alpha+s} \equiv \sum_{j=1}^{n} \mu_j((t)g_j)^s((t)g_j)^{p^\alpha} \pmod{t^{2i+2}\mathbb{F}_p[[t]]}.$$

Mivel $(t)g_j \equiv t \pmod{t^2\mathbb{F}_p[[t]]}$, ezért $((t)g_j)^{p^\alpha} \equiv t^{p^\alpha} \pmod{t^{2p^\alpha}\mathbb{F}_p[[t]]}$. Tehát

$$\begin{aligned} 0 &\equiv \sum_{j=1}^{n} \mu_j((t)g_j)^s t^{p^\alpha} \pmod{t^{2p^\alpha}\mathbb{F}_p[[t]]}, \text{ és} \\ 0 &\equiv \sum_{j=1}^{n} \mu_j((t)g_j)^s \pmod{t^{p^\alpha}\mathbb{F}_p[[t]]}. \end{aligned}$$

Node ez minden elég nagy p^α-ra teljesül rögzített $s \geq 0$ mellett, ami azt jelenti, hogy

$$0 = \sum_{j=1}^{n} \mu_j((t)g_j)^s \text{ minden } s \geq 0\text{-ra.}$$

Ezt $s = 0, 1, \ldots, n-1$-re alkalmazva $(\lambda_1, \ldots, \lambda_n)W = 0$, ahol $W \in \mathbb{F}_p((t))^{n\times n}$ az az $n \times n$-es Vandermonde mátrix, melynek elemei $W_{ji} = ((t)g_j)^{i-1}$. Ez viszont ellentmondás, mert $\det(W) \neq 0$, hiszen a g_j elemek különbözőek, és $(\lambda_1, \ldots, \lambda_n)$ nem nulla vektor az $\mathbb{F}_p((t))$ test feletti n dimenziós vektortérben. □

Megjegyzés: Abért Miklós [2] belátta a 4.2.5-ös tétel analogonját pro-véges facsoportokra (branch groups).

4.2.6. Következmény. *A Nottingham csoport tartalmaz egy két elemmel generált sűrű szabad részcsoportot.*

Bizonyítás. Mivel $\mathcal{N}(\mathbb{F}_p)$ topologikusan generálható két elemmel, mégpedig $(t)g = t(1+t)$-vel és $(t)h = t(1+t^2)$-tel, ezért két véletlen elem $\frac{(p^2-1)(p-1)}{p^3} > 0$ valószínűséggel sűrű részcsoportot generál $\mathcal{N}(\mathbb{F}_p)$-ben. Alkalmazva a 4.2.5-ös tételt készen vagyunk. □

5. fejezet

Számelméleti kapcsolatok

A Nottingham csoport a számelméletben úgy ismert, mint az $\mathbb{F}_p((t))$ test úgynevezett *vad automorfizmus*ainak csoportja. Az elágazási csoportok vizsgálatában fontos szerepet játszik, mert minden lokális test – melynek maradékteste $\mathbb{F}_p$ – tetszőleges teljesen elágazó bővítésésének Galois csoportja beágyazható $\mathcal{N}(\mathbb{F}_p)$-be a *normák teste* nevű funktor segítségével, feltéve, hogy az elágazási részcsoportok nyíltak a teljes Galois csoportban. Az ezzel a tulajdonsággal rendelkező testbővítéseket nevezik *aritmetikailag pro-véges* bővítéseknek. Ebben a fejezetben a Nottingham csoport számelméleti és csoportelméleti tulajdonságainak kapcsolatát igyekszem bemutatni.

5.1. Lokális testek

Ebben az alfejezetben felidézek néhány alapvető fogalmat lokális testekkel kapcsolatban.

5.1.1. Definíció. Legyen F egy test, és $v\colon F^* \to \mathbb{Z}$ egy a multiplikatív csoportból az egész számokba menő szürjektív homomorfizmus, melyre $v(\alpha+\beta) \geq \min(v(\alpha), v(\beta))$ minden $\alpha, \beta \in F^*$-ra! Továbbá legyen $v(0) := \infty$! Ekkor v-t F *diszkrét értékelés*ének, F-et pedig *diszkréten értékelt test*nek hívjuk (discrete valuation field). Az *egészek gyűrűje* $\mathcal{O} := \{\alpha \in F : v(\alpha) \geq 0\}$ és a *maximális ideál* $\mathcal{M} := \{\alpha \in F : v(\alpha) > 0\}$. F topologikus test az $\mathcal{M}$-adikus topológiával, melyben $\mathcal{M}$ hatványai alkotják a 0 egy környezetbázisát. Egy F diszkréten értékelt testet *teljes*nek hívunk (complete discrete valuation field), ha teljes az $\mathcal{M}$-adikus topológiára nézve.

Be lehet látni, hogy egy teljes, diszkréten értékelt testnek az értékelése egyértelműen meg van határozva (lásd [14] Exercise 6 Section 2 Chapter II), tehát v_F-fel, $\mathcal{O}_F$-fel, illetve $\mathcal{M}_F$-fel jelöljük rendre az értékelést, az egészek gyűrűjét, illetve a maximális ideált. Az $\mathcal{O}_F/\mathcal{M}_F$ faktortestet az F *maradéktest*ének nevezzük. Mindig feltesszük, hogy a maradéktest egy p-karakterisztikájú tökéletes test. Egy teljes, diszkréten értékelt testet, melynek maradékteste véges, *lokális test*nek hívunk. A maximális ideál egy $\pi = \pi_F$ generátorát F *prímelem*ének nevezzük.

Jelölje $v_p(n)$ a p kitevőjét egy n egész szám prímtényezős felbontásában. Erre az értékelésre nézve $\mathbb{Q}$ teljessé tettje a p-adikus számok teste, $\mathbb{Q}_p$. Egy $\mathbb{F}$ p-karakterisztikájú véges test feletti racionális törtfüggvények $\mathbb{F}(t)$ testének teljessé tettje a $v(a_n t^n + \text{magasabb fokú tagok}) = n$ $(a_n \neq 0)$ értékelésre nézve $\mathbb{F}((t))$, a „véges farkú” formális Laurent-sorok teste. Ez a két példa a legfontosabb osztálya a lokális testeknek.

Igazság szerint lényegében csak ez a két példa létezik. Nulla karakterisztikában minden lokális test $\mathbb{Q}_p$-nek véges bővítése. Ugyanakkor pozitív karakterisztikában egy lokális test izomorf $\mathbb{F}((t))$-vel, ahol $\mathbb{F}$ a véges maradéktest. Általában $t_F := t$-vel jelöljük egy F p-karakterisztikájú lokális test prímelemét.

Ha L egy véges bővítése az F teljes, diszkréten értékelt testnek, akkor v_F egyértelműen kiterjed L egy v_L diszkrét értékelésévé, melyre nézve L teljes (lásd [14] Section 2 Chapter II). Persze ezt úgy kell érteni, hogy $v_L\big|_F$ képe $\mathbb{Z} \cong v_L(\pi_F)\mathbb{Z} \leq \mathbb{Z} = v_L(L^*)$. Az $e(L/F) := v_L(\pi_F)$ számot az L/F bővítés *elágazási index*ének (ramification index) nevezzük. A k_F maradéktest azonosítható k_L egy résztestével. A k_L/k_F bővítés fokát *inerciafok*nak (inertia degree) vagy *maradékfok*nak (residue degree) hívjuk, és $f(L/F)$-fel jelöljük. Ekkor, ha $N_{L/F}$ a normaleképezés, akkor $f(L/F) = v_F(N_{L/F}(\pi_L))$, és $e(L/F)f(L/F) = (L : F)$, az eredeti bővítés foka.

Legyen F egy teljes, diszkréten értékelt test! Az $e(F) := v_F(p)$ véges vagy végtelen számot F *abszolút elágazási index*ének (absolute ramification index) nevezzük. Egy véges L/F bővítést *elágazásmentes*nek (unramified) hívunk, ha $e(L/F) = 1$. Ez azt jelenti, hogy egy π_F prímelem a bővebb testben is prím marad. A másik extrém esetben – amikor $f(L/F) = 1$ – azt mondjuk, hogy az L/F bővítés *teljesen elágazó* (totally ramified). Ez pontosan akkor áll fenn, ha $N_{L/F}(\pi_L)$ prím F-ben.

Rögzítsük most F-nek egy F_s szeparábilis lezártját! F összes elágazásmentes F_s-beli bővítésének a kompozícióját – F^{ur}-et – F maximális elágazásmentes bővítésének hívjuk. Ez egy diszkréten értékelt test, melynek maradékteste izomorf k_F szeparábilis lezártjával. Egy L/F szeparábilis bővítés esetén az $L \cap \tilde{F}$ testet L/F *inerciarésztest*ének (inertia subfield) nevezzük. Egy L/F (akár végtelen) szeparábilis bővítés – definíció szerint – *elágazásmentes*, illetve *teljesen elágazó*, ha az inerciarészteste megegyezik rendre L-lel, illetve F-fel. Ha L/F teljesen elágazó, akkor $L = F(\pi_L)$, és $\mathcal{O}_L$-et generálják mint $\mathcal{O}_F$-modulust a $\{\pi_L^j : 0 \leq j \leq e(L/F)\}$ elemek, azaz $\mathcal{O}_L = \mathcal{O}_F[\pi_L]$. Az inerciarésztestet pedig azonosíthatjuk az $x^q - x$ polinom F feletti felbontási testével, ahol $q = p^{f(L/F)}$.

$U_F = U_{0,F}$-fel jelöljük az $\mathcal{O}_F$ gyűrű egységeinek csoportját. (Ezt gyakran F egységcsoportjának is hívják.) Ezen megadhatunk egy $U_{i,F} := 1 + \pi_F^i\mathcal{O}_F$ $(i \geq 1)$ filtrálást. Ezek az egységelem egy környezetbázisát alkotják $U_{0,F}$-ben az F által indukált topológiára nézve. Az izomorfizmus tételek alkalmazásával adódik az alábbi állítás:

5.1.1. Állítás. *$U_{0,F} = \varprojlim U_{0,F}/U_{i,F}$, továbbá*

$$U_{i,F}/U_{i+1,F} \cong \begin{cases} k_F^*, \text{ ha } i = 0, \text{ illetve} \\ k_F^+, \text{ ha } i \geq 1. \end{cases}$$

Tehát az egységcsoport az $U_{1,F}$ pro-p csoport véges bővítése.

A következő lemma meghatározza az $U_{N,F}$ csoportok alsó centrális p-láncát (lásd 1.1.4-es definíció), ha a karakterisztika nulla, és N elég nagy. Mivel $U_{N,F}$ kommutatív, ezért az alsó centrális p-lánc meghatározásához elég megvizsgálni a p-edik hatványra emelés hatását a csoporton:

5.1.2. Lemma ([29]). *Legyen $n \geq 1$! Ekkor*

(i) *Ha $n \leq e(F)/(p-1)$ vagy F karakterisztikája p, akkor $U_n^p \leq U_{np}$.*

(*ii*) *Ha* $n > e(F)/(p-1)$ *és* F *karakterisztikája nulla, akkor az* $x \mapsto x^p$ *egy izomorfizmust definiál* U_n*-ből* $U_{n+e(F)}$*-re.*

(*iii*) *Ha* $N > e(F)/(p-1)$ *és* F *karakterisztikája nulla, akkor* $P_{n+1}(U_N) = U_{N+ne(F)}$.

Bizonyítás. Legyen F prímeleme $\pi = \pi_F$, és $1 + z\pi^n \in U_n$! Ekkor

$$(1 + z\pi^n)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} z^i \pi^{ni} + z^p \pi^{np}.$$

Ha char$F = p$, akkor készen vagyunk, hiszen a középső tagok eltűnnek. Legyen a továbbiakban tehát char$F = 0$! Ekkor $v_F\left(\binom{p}{i} z^i \pi^{ni}\right) \geq e(F) + ni$ és $v_F(z^p\pi^{np}) \geq np$.

(*i*) Ebben az esetben $(p-1)n \leq e(F)$ és így $v_F\left(\binom{p}{i} z^i \pi^{ni}\right) \geq (p-1)n + n = np$, azaz $U_n^p \leq U_{np}$.

(*ii*) Azt akarjuk belátni, hogy ha $pn > n + e(F)$, akkor minden $y = 1 + a\pi^{n+e(F)} \in U_{n+e(F)}$-re egyértelműen létezik egy $x = 1 + z\pi^n \in U_n$ az $x^p = y$ tulajdonsággal. Ebben az esetben $pz\pi^n$ határozza meg $(1 + z\pi^n)^p$ viselkedését. Mivel char$F = 0$, ezért p-t felírhatjuk $p = \pi^{e(F)}b$ alakban, ahol b egy egység. Válasszuk tehát z_1-et úgy, hogy $z_1 b = a$ legyen, és $x_1 := 1 + z_1\pi^n \in U_n$. Ezt megtehetjük, hiszen b egység. Ekkor $y_1 := yx_1^{-p} \in U_{n+e(F)+1}$. Ezt folytatva mindig találhatunk egy olyan $x_{j+1} \in U_{n+j}$-et, melyre $y_{j+1} := y_j x_{j+1}^{-p} \in U_{n+e(F)+j+1}$. Tehát $x := \prod_{j=1}^{\infty} x_j \in U_n$ választással $y = x^p$, és a szorzat konvergens F teljessége miatt.

A (*iii*)-as állítás már indukcióval könnyen következik a (*ii*)-esből. □

5.1.3. Következmény. *Nulla karakterisztikában* $N > e(F)/(p-1)$ *esetén* U_N *egy egyenletes pro-p csoport, melynek dimenziója*

$$\log_p |U_N : U_{N+e(F)}| = \log_p |k_F|^{e(F)} = \deg(F/\mathbb{Q}_p).$$

Így, mivel U_N *kommutatív,* $U_N \cong \mathbb{Z}_p^{\deg(F/\mathbb{Q}_p)}$.

Megjegyzés: Pozitív karakterisztikában ez nincs így. Az $U_1 = 1 + t \cdot \mathbb{F}[[t]]$ csoport még csak nem is végesen generált, hiszen Frattini-részcsoportja $\Phi(U_1) = U_1^p[U_1, U_1] = U_1^p = 1 + t^p\mathbb{F}[[t^p]]$ nem véges indexű.

5.2. Az elágazási részcsoportok

Legyen L/F lokális testeknek egy Galois-bővítése, és $G := \mathrm{Gal}(L/F)$ a Galois csoport! Ebben az alfejezetben definiálok egy természetes filtrálást G-n, melyet David Hilbert és tanítványai vezettek be körülbelül 90 évvel ezelőtt. Legyen $\sigma \in G$. Ekkor minden $n \geq 0$-ra a σ testautomorfizmus indukál egy gyűrűautomorfizmust:

$$\sigma_n \colon \mathcal{O}_L/(\mathcal{M}_L)^{n+1} \to \mathcal{O}_L/(\mathcal{M}_L)^{n+1},$$

mert, ahogy a 2.1.1-es tétel bizonyításából látható, egy lokális test minden automorfizmusa folytonos, sőt megtartja az értékelést. Tehát vannak $\sigma \mapsto \sigma_n$ homomorfizmusaink G-ből az $\mathcal{O}_L/(\mathcal{M}_L)^{n+1}$ gyűrűk automorfizmuscsoportjába.

5.2.1. Definíció. Jelöljük $G[n]$-nel a $\sigma \mapsto \sigma_n$ homomorfizmus magját:

$$G[n] := \left\{ \sigma \in G : \sigma(x) \equiv x \pmod{(\mathcal{M}_L)^{n+1}} \text{ minden } x \in \mathcal{O}_L\text{-re} \right\}.$$

A $G[n]$ ($n \geq 1$) csoportokat az *alsó számozású elágazási csoportok*nak (ramification groups in the lower numbering) hívjuk. Ezt a definíciót kiterjeszthetjük valós számokra is:

$$G[x] := \{\sigma \in G : v_L(\sigma(\alpha) - \alpha) \geq x + 1 \text{ minden } \alpha \in \mathcal{O}_L\text{-re}\}.$$

Ekkor $G[x]$ megegyezik $G[i]$-vel, ahol i a legkisebb olyan egész szám, melyre $i \geq x$. A $G[1]$ csoport az L/F bővítés *vad automorfizmusainak csoportja* (group of wild automorphisms).

Ez a filtrálás természetesen nemcsak a G csoporttól függ, hanem az L testtől is. Előfordulhat, hogy a G csoport különböző bővítések Galois-csoportjaként is előáll, és ezek különböző filtrálást indukálnak.

5.2.1. Állítás.

(i) A $G[n]$ sorozat normálosztókból áll, melyekre $G[-1] = G$, és $G[m] = 1$ elég nagy m-re.

(ii) $G[0] = \mathrm{Gal}(L/F_0)$, ahol F_0 az L/F bővítés inerciarészteste.

(iii) Ha $F \subset M \subset L$ és $H = \mathrm{Gal}(L/M)$, akkor $H[n] = H \cap G[n]$.

(iv) Minden $n \geq 0$-ra a $\sigma \mapsto (\sigma(\pi_L)/\pi_L)U_{n+1,L}$ leképezés egy injektív

$$G[n]/G[n+1] \to U_{n,L}/U_{n+1,L}$$

homomorfizmust indukál.

Bizonyítás. (i) Ha $\sigma \neq 1$, akkor van olyan $x \in \mathcal{O}_L$, amelyre $\sigma(x) \neq x$, és ezért elég nagy m-re $\sigma(x) \not\equiv x \pmod{(\mathcal{M}_L)^{n+1}}$, azaz $\sigma \notin G[m]$. Mivel G véges, ezért elég nagy m-re $G[m] = 1$. A másik két állítás nyilvánvaló.

(ii) Jelölje F_0 maradéktestét k_0! Ekkor kommutatív az alábbi diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L/F) & \xrightarrow{\alpha} & \mathrm{Gal}(k_L/k_F) \\ {\scriptstyle\beta}\big\downarrow & & {\scriptstyle\gamma}\big\downarrow \\ \mathrm{Gal}(F_0/F) & \xrightarrow{\delta} & \mathrm{Gal}(k_0/k_F). \end{array}$$

A vízszintes leképezéseket a $\sigma \mapsto \sigma_0$ indukálja. Ez értelmes, hiszen σ_0 fixen hagyja k_F-et. A függőleges leképezések pedig legyenek a megszorítások. Mivel L/F_0 teljesen elágazó, ezért $k_L = k_0$, és γ izomorfizmus. Továbbá F_0 nem más, mint az $x^{p^{f(L/F)}} - x$ polinom felbontási teste F felett, így δ is izomorfizmus (lásd [18] Proposition 2.11). Tehát

$$G[0] = \mathrm{Ker}(\alpha) = \mathrm{Ker}(\beta) = \mathrm{Gal}(L/F_0).$$

(iii) Ez világos $G[n]$ definíciójából.

(*iv*) Legyen π egy tetszőleges prímeleme L-nek. Ekkor $\sigma \in G[n]$-ből következik, hogy $\sigma(\pi)\pi^{-1} \equiv 1 \pmod{\mathcal{M}_L^n}$, azaz $\sigma(\pi)\pi^{-1} \in U_{n,L}$. Másrészt ha π_1 egy másik prímelem, akkor $\pi\pi_1^{-1}$ egység, ezért $\sigma(\pi)\pi^{-1} \equiv \sigma(\pi_1)\pi_1^{-1} \pmod{U_{n+1,L}}$. Tehát a

$$\begin{aligned} \varphi\colon G[n] &\longrightarrow U_{n,L}/U_{n+1,L} \\ \sigma &\longmapsto \sigma(\pi)\pi^{-1} \pmod{U_{n+1,L}} \end{aligned}$$

leképezés jóldefiniált. Továbbá ha π prím, akkor $\sigma(\pi)$ is az, ezért φ homomorfizmus:

$$\sigma_1\sigma_2(\pi)\pi^{-1} = \left(\sigma_1(\sigma_2(\pi))(\sigma_2(\pi))^{-1}\right)\left(\sigma_2(\pi)\pi^{-1}\right).$$

Másrészt φ magja

$$\mathrm{Ker}(\varphi) = \left\{\sigma \in G[n] : \sigma(\pi) \equiv \pi \pmod{\mathcal{M}_L^{n+1}} \text{ minden } \pi \text{ prímre}\right\} = G[n+1],$$

mert prímek szorzatainak hányadosaként minden egész elem előáll (a nulla kivételével). $\square$

Ezt az állítást a 5.1.2-es lemmával összevetve $G = \mathrm{Gal}(L/F)$ csoportelméleti tulajdonságairól kapunk információt:

5.2.2. Következmény.

(i) $G/G[0]$ *egy* $f(L/F)$*-rendű ciklikus csoport.*

(ii) $G[0]/G[1]$ *szintén ciklikus, és rendje osztja* $(p^{f(L/F)} - 1)$*-et.*

(iii) Ha $n \geq 1$*, akkor* $G[n]/G[n+1]$ *egy elemi Abel* p*-csoport, melynek rangja legfeljebb* $f(L/F)$*.*

(iv) G *feloldható.*

Ahhoz, hogy az elágazási részcsoportokat végtelen Galois-bővítésekre is értelmezni tudjuk, egy új filtrálást kell tekintenünk (vagyis ugyanezt a filtrálást egy másik számozással). A 5.2.1-es állítás (*iii*)-as pontjában láttuk, hogy $G[n]$ jól viselkedik a részcsoportokra történő megszorításkor. Viszont faktorcsoportok esetén nem ez a helyzet. Általában ha $H \lhd G$ egy normálosztó, akkor $(G/H)[n] \neq G[n]H/H$.

Próbáljuk meg illusztrálni a problémát! Tegyük fel, hogy van egy L/K Galois-bővítésünk egy E normális közbülső testtel, és a Galois-csoportok: $\mathrm{Gal}(L/K) = G$, $\mathrm{Gal}(L/E) = H$ illetve $\mathrm{Gal}(E/K) = G/H$. Azt a speciális esetet fogjuk tekintetni, amikor a testek $L = \mathbb{F}_p((t_L))$, $E = \mathbb{F}_p((t_E))$ és $K = \mathbb{F}_p((t_K))$. Legyen $\varphi \in G$! Ekkor

$$\varphi(t_L) = t_L + \sum_{i \geq i_L(\varphi)} c_i t_L^i$$

valamilyen $i_L(\varphi) \geq 1$ egész számra, melyre $c_{i_L(\varphi)} \neq 0$. Ez a szám határozza meg, hogy a φ automorfizmus melyik elágazási csoportban van benne: $\varphi \in G[i_L(\varphi) - 1]$, de $\varepsilon > 0$ esetén $\varphi \notin G[i_L(\varphi) - 1 + \varepsilon]$. Viszont a megszorított hatás E prímelemén lehet ettől különböző:

$$\varphi|_E(t_E) = t_E + \sum_{i \geq i_E(\varphi|_E)} d_i t_E^i.$$

Tegyük fel most, hogy L/E egy p-edfokú ciklikus szeparábilis bővítés! Ekkor t_E-t kifejezhetjük t_L-lel az alábbi módon:

$$t_E = \sum_{i=p}^{\infty} a_i t_L^i, \text{ ahol } a_i \in \mathbb{F}_p, \text{ és } a_p \neq 0. \tag{5.1}$$

Jobban megérthetjük $i_L(\varphi)$ és $i_E(\varphi|_E)$ kapcsolatát, ha összehasonlítjuk a $\varphi(t_E)$-re kapott kétféle kifejezést. Kezdjük először azzal a speciális esettel, amikor $\varphi = g$, a $H = \mathrm{Gal}(L/E)$ ciklikus csoport generátora. Ebben az esetben $i_E(g|_E) = i_E(\mathrm{id}_E) = \infty$.

5.2.2. Definíció. Legyen L/E egy Galois-bővítés egy $H = \langle g \rangle$ p-edrendű ciklikus Galois-csoporttal. Ekkor az $s(L/E) := i_L(g) - 1$ számot az L/E bővítés *elágazási töréspont*jának (ramification break) nevezzük.

Az elnevezés abból a tényből származik, hogy ez az a pont, ahol az elágazási filtrálás megtörik: $H[s(L/E)] = H$, viszont $H[s(L/E) + \varepsilon] = 1$ tetszőleges pozitív ε-ra. Ez egy fontos szám.

5.2.3. Lemma. *Legyen a_u az első nem nulla együttható az* (5.1)*-es kifejezésben, melyre $u \not\equiv 0 \pmod p$. Ekkor $u = s(L/E)(p-1) + p$.*

Bizonyítás. Először vegyük észre, hogy létezik ilyen u, hiszen egyébként t_E p-edik hatvány lenne L-ben, ami azt jelenti, hogy az L/E bővítés nem lenne szeparábilis. Mivel $g(t_E) = t_E$, ezért (5.1)-ből azt kapjuk, hogy

$$\sum_{i=p}^{\infty} a_i t_L^i = g\left(\sum_{i=p}^{\infty} a_i t_L^i\right) = \sum_{i=p}^{\infty} a_i \left(t_L + \sum_{j \geq i_L(g)} c_j t_L^j\right)^i.$$

Végezzük el a jobb oldalon az i-edik hatványra emelést, és vegyünk el mindkét oldalból $\sum_{i=p}^{\infty} a_i t_L^i$-t. Mivel a karakterisztika p, ezért

$$0 = a_p c_{i_L(g)} t_L^{p i_L(g)} + u a_u c_{i_L(g)} t_L^{u-1} t_L^{i_L(g)} + (\text{magasabb fokú tagok}).$$

Mivel $a_p c_{i_L(g)} \neq 0$ és $u a_u c_{i_L(g)} \neq 0$, ezért a két fenti tagnak ki kell ejtenie egymást, így fokaik megyeznek: $u = (i_L(g) - 1)(p-1) + p = s(L/E)(p-1) + p$. □

Használva ezt a kapcsolatot u és $s(L/E)$ között, most már meg tudjuk határozni $i_L(\varphi)$-t $i_E(\varphi|_E)$ és $s(L/E)$ segítségével. A jelölés egyszerűsítése végett legyen $s := s(L/E)$, $i_L := i_L(\varphi)$, illetve $i_E := i_E(\varphi|_E)$!

5.2.4. Lemma.

(i) Ha $i_E - 1 < s$, akkor $i_L = i_E$.

(ii) Ha $i_E - 1 \geq s$ és $i_L - 1 \neq s$, akkor $i_L - 1 = s + p(i_E - 1 - s)$.

Bizonyítás. Ahogy az előző lemmában, tekintsük $\varphi(t_E)$ kifejezését:

$$\begin{aligned}
\sum_{i=p}^{\infty} a_i t_L^i + \sum_{j\geq i_E} d_j \left(\sum_{i=p}^{\infty} a_i t_L^i\right)^j &= t_E + \sum_{j\geq i_E} d_j t_E^j \\
&= \varphi(t_E) \\
&= \varphi\left(\sum_{i=p}^{\infty} a_i t_L^i\right) \\
&= \sum_{i=p}^{\infty} a_i \left(t_L + \sum_{l\geq i_L} c_l t_L^l\right)^i .
\end{aligned}$$

Ismét eltüntetjük az egyező $\sum_{i=p}^{\infty} a_i t_L^i$ tagokat mindkét oldalról, és a maradékot összehasonlítjuk. A bal oldalon az első tag $d_{i_E} a_p t_L^{pi_E}$. A jobb oldalon két lehetséges tag jön számításba: $a_p c_{i_L} t_L^{pi_L}$ és $a_u t_L^{u-1} u c_{i_L} t_L^{i_L}$. Tehát vagy $pi_E = \min(pi_L, u-1+i_L)$ vagy $pi_L = u-1+i_L \leq pi_E$. Mivel az előző lemma szerint $u-1 = (p-1)(s+1)$, ezért négy esetet különböztetünk meg:
1. eset: $pi_L < u-1+i_L$. Ekkor $i_L - 1 < s$ és $i_E = i_L$. Ebben az estben $i_E - 1 < s$.
2. eset: $pi_L > u-1+i_L$. Ekkor $i_L - 1 > s$ és

$$pi_E = u-1+i_L = (p-1)(s+1)+i_L > p(s+1).$$

Ebből következik, hogy $i_L - 1 = s + p(i_E - 1 - s)$ és hogy $i_E - 1 > s$.
3. eset: $pi_L = u-1+i_L < pi_E$. Ekkor $i_L - 1 = s$ és $i_E \geq i_L$, tehát $i_E - 1 \geq s$.
4. eset: $pi_L = u-1+i_L = pi_E$. Ebben az esetben $i_E - 1 = i_L - 1 = s$.
A lemma állítása következik, mert az (i)-es feltevés csak az első esetben, a (ii)-es feltevés pedig csak a második esetben áll fenn. □

Megjegyzés: Ha $s = i_L - 1$ és a két tag, $a_p c_{i_L} t_L^{pi_L}$ és $a_u t_L^{u-1} u c_{i_L} t_L^{i_L}$ kiejti egymást (a fenti bizonyítás harmadik esete), akkor a következtetés valójában hamis, hiszen i_E nagyobb értéket vesz fel, mint ami a lemma állításában szerepel. Például, ha φ a generátora a $\mathrm{Gal}(L/E)$ ciklikus csoportnak, akkor $s(L/E) = i_L(\varphi)$ definíció szerint, ugyanakkor $\varphi|_E = 1$ miatt $i_E(\varphi|_E) = \infty$.

Az $i_L(\varphi)-1$ kifejezés megmondja, hogy φ melyik tagjában van a filtrálásnak. Tehát ha van egy E/K Galois-bővítésünk, akkor értelmezhetünk egy függvényt, mely megmondja, hogyan változik a filtrálás számozása, amikor áttérünk E/K-ról L/K-ra, ahol L egy p-edfokú teljesen elágazó bővítése E-nek:

$$h_{L/E}(x) := \begin{cases} x, \text{ ha } x \leq s(L/E) \\ s(L/E) + p(x - s(L/E)), \text{ ha } x > s(L/E). \end{cases}$$

A 5.2.4-es lemma épp azt állítja, hogy ha $G = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(L/E)$, $G/H = \mathrm{Gal}(E/K)$ és $|H| = p$, akkor

$$(G/H)[x] = G[h_{L/E}(x)]H/H.$$

Vegyük észre, hogy a $h_{L/E}$ függvény deriváltja épp az elágazási töréspontban nem folytonos. Ez is indokolja az elnevezést.

Ezt általánosíthatjuk lokális testek tetszőleges Galois-bővítésére. Először legyen $(L:E) = l$ prím!

$$h_{L/E}(x) := \begin{cases} x, \text{ ha } L/E \text{ elágazásmentes, egyébként} \\ lx, \text{ ha } (l,p)=1 \\ x, \text{ ha } x \leq s(L/E) \text{ és } l=p \\ s(L/E)+p(x-s(L/E)), \text{ ha } x > s(L/E) \text{ és } l=p. \end{cases}$$

Egy tetszőleges L/K Galois-bővítésre vegyünk egy normális közbülső testekből álló

$$L = E_m > E_{m-1} > \cdots > E_1 > E_0 = K$$

tornyot, melyre E_i/E_{i-1} prímfokú ciklikus bővítés, és legyen

$$h_{L/K} := h_{L/E_{m-1}} \circ h_{E_{m-1}/E_{m-2}} \circ \cdots \circ h_{E_1/K}!$$

Ezt megtehetjük, hiszen $\mathrm{Gal}(L/F)$ feloldható a 5.2.2-es következmény szerint. Ezt a

$$h_{L/F} : [-1,\infty) \to [-1,\infty)$$

függvényt nevezzük a bővítés *Hasse-Herbrand függvény*ének. Be lehet látni, hogy a definíció nem függ a közbülső testek választásától, szakaszonként lineáris és szigorúan monoton nő. Ez utóbbi két állítás triviális a definicióból, az elsőhöz viszont a Hasse-Herbrand függvénynek a normaleképezéssel való kapcsolatát kell megvizsgálni (lásd [14] Chapter III. Section 3). Továbbá

5.2.5. Tétel (Herbrand, [14]). *Legyenek $L \geq E \geq K$ lokális testek úgy, hogy mindegyik bővítés Galois, és $G := \mathrm{Gal}(L/K)$, illetve $H := \mathrm{Gal}(L/E)$! Ekkor*

$$(G/H)[h_{E/K}(x)] = G[h_{L/K}(x)]H/H.$$

Vegyük észre, hogy az állítás implicite tartalmazza azt a tényt, hogy $i_L(\varphi) - 1 = s(L/E)$ esetén – melyet kizártunk az 5.2.4-es lemmában – van olyan $\psi \in G$, melyre $\psi|_E = \varphi|_E$ és $i_L(\psi) \neq s(L/E)$ és így az előző lemma miatt $i_L(\psi) - 1 = h_{L/E}(i_E(\psi|_E) - 1)$. Például amikor φ a generátora a ciklikus bővítésnek, akkor $\psi = 1$ vehető.

Használva ezt a függvényt átszámozhatjuk az elágazási részcsoportokat úgy, hogy megmaradjanak hányadosra való áttéréskor:

5.2.3. Definíció. Legyen G az L/K bővítés Galois-csoportja! Ekkor a *felső számozású elágazási csoportok*at az alábbi módon értelmezzük:

$$G(x) := G[h_{L/K}(x)].$$

5.2.6. Állítás. *Legyen $H \lhd G$ normálosztó a G Galois-csoportban. Ekkor $(G/H)(x) = G(x)H/H$.*

Az alábbi következmény a definícióból közvetlenül levezethető:

5.2.7. Következmény. *A Hasse-Herbrand függvény baloldali deriváltja $|G(0) : G(x)|$, jobb oldali deriváltja pedig szintén $|G(0) : G(x)|$, ha $h_{L/K}(x)$ nem egész, és $|G[0] : G[h_{L/K}(x)+1]|$, ha $h_{L/K}(x)$ egész.*

Megjegyzés: A Hasse-Herbrand függvényt úgy is lehet definiálni, mint a

$$\varphi_{L/K}(x) := \int_0^x \frac{dt}{|G[0] : G[t]|}$$

függvény inverze.

5.3. Végtelen Galois-bővítések

Eddig véges testbővítésekkel foglalkoztunk. Most tekintsünk egy L/K végtelen Galois-bővítést, és írjuk fel L-et véges bővítések $L = \bigcup_{i\in I} K_i$ egyesítéseként. Ezt tetszőleges algebrai bővítés esetén megtehetjük. A $\mathrm{Gal}(L/K)$ Galois-csoportot egy pro-véges csoportnak definiáljuk: $\mathrm{Gal}(L/K) := \varprojlim \mathrm{Gal}(K_i/K)$. Az összekötő leképzések a természetes faktorleképezések. Ha úgy akarjuk értelmezni az elágazási részcsoportokat egy ilyen végtelen Galois-bővítésre, mint a véges részbővítések elágazási részcsoportjainak inverz limesze, akkor szükségünk van arra, hogy ezek az elágazási részcsoportok megmaradjanak a faktorleképezéseknél. Ezen a módon tehát csak felső számozású elágazási csoportokat tudunk értelmezni.

5.3.1. Definíció. Legyen L/K egy végtelen Galois-bővítése a K lokális testnek, és a Galois-csoport $G := \mathrm{Gal}(L/K)$. Ekkor egy $w \in [-1, \infty)$ valós számra a felső számozású elágazási részcsoportja G-nek

$$G(w) = \varprojlim \mathrm{Gal}(K_i/K)(w),$$

ahol $L = \bigcup_{i\in I} K_i$ a véges részbővítések egyesítése.

Megjegyzés: Ha L végtelen algebrai bővítése a K lokális testnek, akkor L-re kiterjeszthető K értékelése egy $v_L \colon L^* \to \mathbb{Q}$ homomorfizmussal, melyre $v_L\big|_K = v_K \colon K^* \to \mathbb{Z}$. Tehát ez az értékelés nem lesz feltétlenül diszkrét, és L nem is lesz teljes az indukált topológiával. Viszont az egészek gyűrűjét, és annak maximális idálját, továbbá a maradéktestet hasonlóképpen értelmezhetjük: $\mathcal{O}_L := \{x \in L : v_L(x) \geq 0\}$, $\mathcal{M}_L := \{x \in L : v_L(x) > 0\}$, és $k_L := \mathcal{O}_L/\mathcal{M}_L$. Továbbá L Hensel-féle test lesz – mely általánosítja a teljes, diszkréten értékelt test fogalmát: Ha $f(x), g_0(x), h_0(x) \in \mathcal{O}_L[x]$ olyan egész együtthatós polinomok, melyek főegyütthatója 1, és $f(x) \equiv g_0(x)h_0(x) \pmod{\mathcal{M}_L[x]}$, akkor léteznek olyan 1-főegyütthatós, egész együtthatós g, h polinomok, melyekre $f(x) = g(x)h(x)$, $g(x) \equiv g_0(x) \pmod{\mathcal{M}_L[x]}$ és $h(x) \equiv h_0(x) \pmod{\mathcal{M}_L[x]}$.

5.3.1. Állítás. *Ha $G_i(w)$-vel jelöljük $\mathrm{Gal}(K_i/K)(w)$ ősképét G-ben, akkor*

$$G(w) = \bigcap_{i\in I} G_i(w).$$

Bizonyítás. Mivel az inverz-limesz definíciójában a leképezések szürjektívek, ezért a

$$\varphi_i \colon G \to \mathrm{Gal}(K_i/K)$$

leképezések is szürjektívek, továbbá $\varphi_i(G(w)) = \mathrm{Gal}(K_i/K)(w)$. Tehát $G_i(w) = G(w)\mathrm{Ker}(\varphi_i)$, és így a 1.1.1-es állítás miatt

$$G(w) = \overline{G(w)} = \bigcap_{i\in I} G(w)\mathrm{Ker}(\varphi_i) = \bigcap_{i\in I} G_i(w),$$

hiszen $G(w)$ kompakt halmazok inverzlimesze, tehát kompakt, és mivel egy pro-véges csoport Hausdorff tér, ezért zárt is. □

5.3.2. Definíció. Az L/K bővítés *felső elágazási töréspont*jainak (upper ramification breaks) $B(L/K)$ halmaza azon x racionális számokból áll, melyekre van egy olyan véges M/K részbővítése L/K-nak, melyre

$$\mathrm{Gal}(M/K)(x + \varepsilon) \neq \mathrm{Gal}(M/K)(x)$$

tetszőleges $\varepsilon > 0$ esetén. Az L/K bővítés *vad automorfizmus*ai a $\mathrm{Gal}(L/K)(1)$-beli automorfizmusok.

Megjegyzés: Ez a definíció különbözik az *elágazási töréspontok* szokásos definíciójától: azon x-ek halmaza, melyekre $\mathrm{Gal}(L/K)(x+\varepsilon) \neq \mathrm{Gal}(L/K)(x)$ tetszőleges $\varepsilon > 0$-ra. Ezek épp a felső elágazási töréspontok, és csökkenő sorozataik limeszei [23].

Bizonyítás. Vegyük észre, hogy adott $\varepsilon > 0$-ra $\mathrm{Gal}(L/K)(x+\varepsilon) \neq \mathrm{Gal}(L/K)(x)$ ekvivalens azzal, hogy valamely K_i véges részbővítésre $\mathrm{Gal}(K_i/K)(x+\varepsilon) \neq \mathrm{Gal}(K_i/K)(x)$. □

5.3.3. Definíció. Egy L/F Galois-bővítést *mélyen elágazó*nak (deeply ramified) nevezünk, ha a felső elágazási töréspontjainak halmaza nem korlátos. A bővítés *aritmetikailag pro-véges* (arithmetically profinite), ha a $\mathrm{Gal}(L/F)(x)$ felső elágazási csoportok nyíltak $\mathrm{Gal}(L/F)$-ben.

Megjegyzés: A mélyen elágazó bővítéseket számos matematikus (többek között Tate és Iwasawa) munkája tette híressé. Coates és Greenberg [8] belátta, hogy ezek a bővítések jó általánosításai a $\mathbb{Z}_p$-bővítéseknek. Speciálisan Tate eredményeit [34] is ki lehet terjeszteni, és alkalmazni lehet Abel-féle varietások Kummer-elméletében.

5.3.2. Állítás. *Egy L/F Galois-bővítés pontosan akkor mélyen elágazó, ha tetszőleges x-re a $\mathrm{Gal}(L/F)(x)$ elágazási részcsoport nemtriviális.*

Bizonyítás. Ha $\mathrm{Gal}(L/F)(x)$ triviális valamilyen x-re, akkor x felső korlátja a töréspontok halmazának. Megfordítva tegyük fel, hogy van egy ilyen x korlát. Ekkor $\mathrm{Gal}(L/F)(y) = \mathrm{Gal}(L/F)(x)$ minden $y \geq x$-re. De minden N nyílt normálosztóra $\mathrm{Gal}(L/F)(y)N = N$ elég nagy y-ra, ami azt jelenti, hogy $\mathrm{Gal}(L/F)(x)N = N$ minden $N \lhd_o \mathrm{Gal}(L/F)$-re, tehát $\mathrm{Gal}(L/F)(x) = 1$. □

5.3.3. Következmény. *Egy aritmetikailag pro-véges bővítés mélyen elágazó.*

5.3.4. Állítás. *A következők ekvivalensek:*

(i) L/F aritmetikailag pro-véges;

(ii) L/F inerciarészteste véges fokú F felett és minden x-re a $h_{M/F}(x)$ sorozatnak van határértéke, ha M az L/F véges részbővítésin fut végig.

Bizonyítás. Jelöljük $G := \mathrm{Gal}(L/F)$-fel a Galois-csoportot. Először is vegyük észre, hogy L/F inerciateste pontosan akkor véges fokú F felett, ha $(G : G(0))$ véges (azaz $G(0)$ nyílt), hiszen $G(0) = G[0]$ fixteste épp az inerciaresztest az 5.2.1-es állítás miatt.
Egyik irány: (ii) $\Rightarrow$ (i). Elég belátni, hogy $G(x)$ nyílt $G(0)$-ban. Az 5.2.7-es következmény szerint $h_{M/F}(x)$ grafikonjának meredeksége mindig egész szám, mert valamilyen elágazási részcsoport indexe. Írjuk fel L-et L_i véges fokú közbülső testek felszálló uniójaként! Mivel $h_{L_i/F}(x)$-nek van határértéke, ezért tetszőleges $a > 0$-ra van olyan j egész, hogy h_{L_i/L_j} (bal vagy jobb oldali) deriváltja minden $x < h_{L_j/F}(a)$ és $i > j$ esetén 1. Tehát $h_{L_i/F}$ grafikonjának a alatti része nem változik. Tehát $h_{L_i/F}(x) = h_{L_j/F}(x)$ minden $i > j$-re és $x < a$-ra. Most ha $G_i(x)$-szel jelöljük $\mathrm{Gal}(L_i/F)(x)$ ősképét, akkor $G(x) = \bigcap G_i(x)$, és a 5.2.7-es következmény szerint $G_i(x)$ indexe $G(0)$-ban állandó (mégpedig $h_{L_j/F}$ bal oldali deriváltja x-ben). Tehát mivel $G(0)$ véges indexű, ezért $G(x)$ is, ami azt jelenti, hogy L/F aritmetikailag pro-véges.

Másik irány: $(i) \Rightarrow (ii)$. Ha $G(a)$ nyílt valamilyen a-ra, akkor valamilyen j egész számra $G_i(x) = G(x)$ minden $i > j$ és $x < a$ esetén. Ebből következik, hogy h_{L_i/L_j} deriváltja 1 minden $x < h_{L_j/F}(a)$-ra. Tehát $h_{L_i/F}(x) = h_{L_j/F}(x)$, ha $i > j$ és $x < a$, ezért $h_{L_i/F}(x)$-nek van határértéke. □

5.3.4. Definíció. Ilymódon értelmezhetjük egy L/F aritmetikailag pro-véges bővítés Hasse-Herbrand függvényét:

$$h_{L/F}(x) := \lim h_{M/F}(x),$$

ahol M a véges fokú közbülső testeken fut végig. Továbbá az *alsó számozású elágazási részcsoportok:*

$$\mathrm{Gal}(L/F)[x] := \mathrm{Gal}(L/F)(h_{L/F}^{-1}(x)).$$

5.3.5. Következmény. *Ha L/F aritmetikailag pro-véges, akkor a töréspontok diszkrét halmazt alkotnak.*

Bizonyítás. Tetszőleges $a > 0$-ra az a alatti töréspontok pontosan az L_j/F véges bővítés töréspontjai, hiszen $h_{L_i/F}$ grafikonja a alatt megegyezik $h_{L_j/F}$ grafikonjával. Tehát a $(0, a)$ intervallum csak véges sok töréspontot tartalmaz, azaz a töréspontok halmaza diszkrét. □

5.3.6. Következmény. *Ha L/F egy aritmetikailag pro-véges bővítés, akkor a p-hez relatív prím fokú részbővítések egyesítése véges fokú F felett, speciálisan* $\mathrm{Gal}(L/F)$ *virtuálisan pro-p csoport.*

Bizonyítás. Láttuk, hogy az F_0 inerciarésztest véges fokú F felett. Ha $|M : F_0|$ relatív prím p-hez, akkor $h_{M/F}(x) \geq h_{M/F_0}(x) = |M : F_0|x$, mert L/F_0 teljesen elágazó. Node $h_{M/F}(x)$ korlátos, tehát készen vagyunk. □

A következő lemma és állítás Camina tételének bizonyításában játszik fontos szerepet, mely szerint minden megszámlálható bázisú pro-p csoport beágyazható a Nottingham csoportba.

5.3.7. Lemma. *Legyen $L = \bigcup_{i \geq 1} \mathbb{F}_p((t_i))$ p-karakterisztikájú lokális testek egy tornya úgy, hogy mindegyik közbülső test p-edfokú teljesen elágazó bővítése az előzőnek. Ha az $s_i := s(\mathbb{F}_p((t_{i+1}))/\mathbb{F}_p((t_i)))$ elágazási töréspontok egy növekvő sorozatot alkotnak, akkor a felső elágazási töréspontok halmaza*

$$B(L/\mathbb{F}_p((t_1))) = \left\{s_1 + (s_2 - s_1)p^{-1} + \cdots + (s_i - s_{i-1})p^{-(i-1)} : i \geq 1\right\}.$$

Bizonyítás. Először belátjuk, hogy ezek töréspontok. Legyen $G_i := \mathrm{Gal}(\mathbb{F}_p((t_{i+1}))/\mathbb{F}_p((t_1)))$ és helyettesítsünk $x = s_1 + (s_2 - s_1)p^{-1} + \cdots + (s_i - s_{i-1})p^{-(i-1)}$-et a

$$\begin{aligned} G_i(x)G_{i-1}/G_{i-1} &= G_i[h_{\mathbb{F}_p((t_{i+1}))/\mathbb{F}_p((t_1))}(x)]G_{i-1}/G_{i-1} \\ &= (G_i/G_{i-1})[h_{\mathbb{F}_p((t_i))/\mathbb{F}_p((t_1))}(x)] \\ &= (G_i/G_{i-1})[s_i] \end{aligned}$$

egyenletbe! Mivel s_i az elágazási töréspontja $\mathbb{F}_p((t_{i+1}))/\mathbb{F}_p((t_1))$-nek, ezért $G_i(x)G_{i-1} = G_i$, de minden $\varepsilon > 0$-ra $G_i(x+\varepsilon)G_{i-1} = G_{i-1}$, azaz $x \in B(L/\mathbb{F}_p((t_1)))$. Visszafelé alkalmazva az érvelést láthatjuk, hogy más töréspont nincs. □

5.3.8. Állítás. *Legyen L mint az előző lemmában. Ekkor a következők ekvivalensek:*

(i) $L/\mathbb{F}_p((t_1))$ *aritmetikailag pro-véges;*

(ii) $L/\mathbb{F}_p((t_1))$ *mélyen elágazó;*

(iii) $s_1 + (s_2 - s_1)p^{-1} + \cdots + (s_i - s_{i-1})p^{-(i-1)} \to \infty$, *ha* $i \to \infty$.

Bizonyítás. Az előző lemma miatt (ii) és (iii) ekvivalenciája triviális, az 5.3.3-as következmény szerint pedig (i)-ből következik (ii). Továbbá

$$h_{\mathbb{F}_p((t_j))/\mathbb{F}_p((t_1))}(s_1 + (s_2 - s_1)p^{-1} + \cdots + (s_j - s_{j-1})p^{-(j-1)}) = s_j \le s_i$$

és $h_{\mathbb{F}_p((t_{i+1}))/\mathbb{F}_p((t_i))}(x) = x$, ha $x < s_i$. Tehát $h_{\mathbb{F}_p((t_i))/\mathbb{F}_p((t_1))}(x) = h_{\mathbb{F}_p((t_j))/\mathbb{F}_p((t_1))}(x)$ minden $x < s_1 + (s_2 - s_1)p^{-1} + \cdots + (s_j - s_{j-1})p^{-(j-1)}$ és $i \ge j$-re, azaz $h_{\mathbb{F}_p((t_i))/\mathbb{F}_p((t_1))}(x)$-nek van határértéke, ha $x < \sup B(L/\mathbb{F}_p((t_1)))$. □

A következő Fontaine-től és Wintenbergertől ([15] és [37]) származó konstrukció rávilágít az aritmetikailag pro-véges bővítések és a Nottingham csoport kapcsolatára. Ha $L \ge M_1 \ge M_2 \ge F$, ahol M_1 és M_2 véges bővítések, akkor az N_{M_1/M_2} normaleképezés ad egy M_1^*-ból M_2^*-ba menő homomorfizmust. Ekkor értelmezhetjük a multiplikatív csoportok inverz limeszét:

$$N(L/F)^* := \varprojlim M^*,$$

ahol M a véges részbővítéseken fut végig, az összekötő leképezések pedig a normaleképezések. Ha L/F aritmetikailag pro-véges, akkor az $N(L/F)^*$-ot nullával kiegészítve, a kapott halmazon megadhatunk egy összeadást is, amellyel $N(L/F) := N(L/F)^* \cup \{0\}$ test lesz:

5.3.5. Definíció. Legyen $a = (a_M)$ és $b = (b_M)$ $(a_M, b_M \in M^*)$ két normakompatibilis sorozat $N(L/F)^*$-ban! Ekkor a szorzást $N(L/F)^*$-on komponensenként definiáljuk: $a \cdot b = (a_M b_M)$. A két elem összege pedig legyen $(a_M) + (b_M) := (c_M)$, ahol $c_M := \lim_E N_{E/M}(a_E + b_E)$, és E az L/M bővítés véges fokú közbülső testein fut végig. Itt megengedjük a (0_M) normakompatibilis sorozatot is.

Az összeadás definíciója azon alapul, hogy egyre feljebb végezzük el a műveletet, és aztán levetítjük a kisebb résztestekre. Ez az egyenletes pro-p csoportokon definiált összeadásra emlékeztet, ahol

$$g + h := \lim_{n\to\infty} (g^{p^n} h^{p^n})^{p^{-n}},$$

ha g és h a G egyenletes pro-p csoport két eleme.

5.3.9. Tétel. *Legyen* L/F *egy aritmetikailag pro-véges bővítés!*

(1) *Ekkor az így definiált* $N(L/F) := N(L/F)^* \cup \{0\}$ *egy teljes, diszkréten értékelt* p*-karakterisztikájú test a* $v_N((a_M)) := v_K(a_K)$ *értékeléssel, ahol* K *egy olyan véges részbővítés, mely tartalmazza* L/F *inerciarésztestét.* $N(L/F)$ *maradékteste izomorf* L *maradéktestével, és* $t_N = (\pi_M)$ *egy prímelem, ha* (π_M) *egy prímekből álló normakompatibilis sorozat. Ilymódon az* $N(L/F)$ *test izomorf az* L *maradékteste feletti formális Laurent-sorok testével.*

(2) *Ha* L/F *még teljesen elágazó bővítés, melynek minden véges részbővítése* p*-hatvány fokú, akkor* L *minden* τ F*-automorfizmusához hozzárendelhetünk egy* σ *vad automorfizmusát a normák testének:* $\sigma((\pi_M)) := (\tau\pi_M)$. *A* $\tau \mapsto \sigma$ *leképezés a* $\mathrm{Gal}(L/F)$ *Galois csoport beágyazása* $N(L/F)$ *vad automorfizmusainak csoportjába.*

5.3.6. Definíció. Az így kapott testet nevezzük az L/F bővítéshez tartozó *normák testé*nek (field of norms).

A bizonyítás az alábbi két (technikai) lemmán múlik ([14] Chapter III):

5.3.10. Lemma. *Legyen L/F véges szeparábilis bővítés. Ekkor $\varepsilon \in \mathcal{O}_L$ esetén*

$$h_{L/F}\left(v_F(N_{L/F}(\varepsilon)-1)\right) \geq v_L(\varepsilon-1),$$

és ha $\alpha \in L$, $\beta \in F$ elemekre $v_L(\alpha-\beta)>0$, akkor

$$h_{L/F}\left(v_F(N_{L/F}(\alpha)-\beta)\right) \geq v_L(\alpha-\beta).$$

5.3.11. Lemma. *Legyen M'/M egy teljesen elágazó p-hatvány fokú bővítés! Ekkor*

$$v_M\left(N_{M'/M}(\alpha+\beta)-N_{M'/M}(\alpha)-N_{M'/M}(\beta)\right) \geq \frac{(p-1)q(M'/M)}{p}$$

$\alpha,\beta \in \mathcal{O}_{M'}$-re. Ha $\alpha \in \mathcal{O}_M$, akkor létezik olyan $\beta \in \mathcal{O}_{M'}$, melyre

$$v_M\left(N_{M'/M}(\beta)-\alpha)\right) \geq \frac{(p-1)q(M'/M)}{p},$$

ahol $q(M'/M) := \sup\{x \geq 0 : h_{M'/M}(x)=x\}$.

Az 5.3.9-*es tétel bizonyítása.* Az 5.3.4-es állítás és az 5.3.6-os következmény miatt az állítást elég belátni teljesen elágazó bővítésekre, melyeknek minden részbővítése p-hatvány fokú. Ekkor L-et felírhatjuk $L=\bigcup_{i=0}^{\infty} L_i$ alakban, ahol $L_{i-1} \geq_p L_i$, és $L_0=F$, továbbá ha (α_{L_i}) egy normakompatibilis sorozat, akkor – mivel a bővítések teljesen elágazóak – minden $i,j \in \mathbb{N}$-re $v_{L_i}(\alpha_{L_i})=v_{L_j}(\alpha_{L_j})$. Először belátjuk, hogy az összeadás jóldefiniált, azaz rögzített j-re az $N_{L_i/L_j}(\alpha_{L_i}+\beta_{L_i})$ sorozat konvergens. Először tegyük fel, hogy $\alpha_F,\beta_F \in \mathcal{O}_F$! Ekkor az 5.3.11-es lemma miatt ha $i \geq k$, akkor

$$N_{L_i/L_k}(\alpha_{L_i}+\beta_{L_i}) \equiv \alpha_{L_k}+\beta_{L_k} \pmod{\mathcal{M}_{L_k}^{a_k}}, \tag{5.2}$$

ahol $a_k=(p-1)q(L/L_k)/p \leq (p-1)q(L_i/L_k)/p$. Másrészt a Hasse-Herbrand függvény korlátossága miatt $a_k \to \infty$, ha $k \to \infty$, és így $i \geq k \geq j$ esetén az 5.3.10-es lemma miatt

$$v_{L_j}\left(N_{L_i/L_j}(\alpha_{L_i}+\beta_{L_i})-N_{L_k/L_j}(\alpha_{L_k}+\beta_{L_k})\right) \geq h_{L_k/L_j}^{-1}(a_k) \geq h_{L/L_j}^{-1}(a_k),$$

azaz az $N_{L_i/L_j}(\alpha_{L_i}+\beta_{L_i})$ sorozat Cauchy, tehát konvergens. Az általános esethez először konstruálunk egy prímekből álló normakompatibilis sorozatot. Legyen k egy olyan index, melyre $a_k>1$, és $\gamma_{L_k} \in L_k$ egy prímelem. Ekkor az 5.3.11-es lemma alapján tudunk egy olyan $\gamma_{L_i} \in L_i$ sorozatot konstruálni, melyre

$$v_{L_i}(N_{L_{i+1}/L_i}(\gamma_{L_{i+1}})-\gamma_{L_i}) \geq a_i.$$

Így indukcióval és alkalmazva (5.2)-t azt kapjuk, hogy

$$v_{L_i}(N_{L_j/L_i}(\gamma_{L_j})-\gamma_{L_i}) \geq a_i, \text{ ha } j \geq i \geq k.$$

Ezért az 5.3.10-es és az 5.3.11-es lemma miatt

$$v_{L_s}(N_{L_j/L_s}(\gamma_{L_j}) - N_{L_i/L_s}(\gamma_{L_i})) \geq h^{-1}_{L_i/L_s}(a_i) \geq h_{L/L_s}(a_i)$$

minden $j \geq i \geq s \geq k$-ra. Mivel $h^{-1}_{L/L_s}(a_i) \to \infty$, ha $i \to \infty$, tehát létezik a $\delta_{L_s} := \lim_{i\to\infty} N_{L_i/L_s}(\gamma_{L_i})$ határérték, és ha $j < k$-ra $\delta_{L_j} := N_{L_k/L_j}\delta_{L_k}$-t vesszük. akkor egy $(\delta_{L_i}) \in N(L/F)$ elemet kapunk, melyre $v_N((\delta_{L_i})) = 1$.

Most mivel egész elemekre már tudjuk, hogy az összeadást definiáló határérték létezik, ezért egy tetszőleges $(\alpha_{L_i}), (\beta_{L_i}) \in N(L/F)$ pár esetén leoszthatunk (δ_{L_i}) megfelelő, mondjuk $\min(v_N((\alpha_{L_i})), v_N((\beta_{L_i})))$-edik hatványával, és azt kapjuk, hogy az összeadás ezeken az elemeken is értelmes. A kommutativitás, az asszociativitás, és a disztributivitás nyilvánvaló, tehát $N(L/F)$ test, melynek v_N egy diszkrét értékelése. Továbbá mivel $1 = (1_{L_i})$, ezért $p = (\alpha_{L_i})$, ahol

$$\alpha_{L_i} = \lim_{j\to\infty} N_{L_j/L_i}(p) = \lim_{j\to\infty} p^{|L_j:L_i|} = 0,$$

tehát $\mathrm{char} N(L/F) = p$.

A teljességhez vegyünk egy $A^{(n)} = (\alpha^{(n)}_{L_i} \in N(L/F))$ Cauchy-sorozatot. Feltehetjük, hogy $v_N(A^{(n)}) \geq 0$. A Cauchy tulajdonság azt jelenti, hogy van olyan n_i, melyre

$$v_{L_i}(\alpha^{(n)}_{L_i} - \alpha^{(m)}_{L_i}) \geq a_i, \text{ ha } n, m \geq n_i.$$

Alkalmazva (5.2)-t azt kapjuk, hogy

$$v_{L_i}(N_{L_j/L_i}(\alpha^{(n_j)}_{L_j}) - \alpha^{(n_i)}_{L_i}) \geq a_i.$$

Az 5.3.10-es és az 5.3.11-es lemma miatt

$$v_{L_s}(N_{L_i/L_s}(\alpha^{(n_i)}_{L_i}) - N_{L_j/L_s}(\alpha^{(n_j)}_{L_j})) \geq h^{-1}_{L/L_s}(a_i) \to \infty,$$

ha $i \geq j \to \infty$. Így $\alpha'_{L_s} := \lim_{i\to\infty} N_{L_i/L_s}(\alpha^{(n_i)}_{L_i})$-t véve egy olyan $A' = (\alpha'_{L_i}) \in N(L/F)$ elemet kapunk, melyre $A' = \lim A^{(n)}$.

Mivel $v_N((\alpha_{L_i})) = v_F(\alpha_F)$, ezért $\mathcal{O}_{N(L/F)}/\mathcal{M}_{N(L/F)} \cong \mathcal{O}_F/\mathcal{M}_F \cong \mathcal{O}_L/\mathcal{M}_L$, hiszen L/F-ről feltettük, hogy teljesen elágazó.

Végezetül a

$$\begin{array}{ccc} \mathrm{Gal}(L/F) & \longrightarrow & \mathrm{Aut}N(L/F) \\ \tau & \longmapsto & \sigma \end{array}$$

homomorfizmus nyilván injektív. Node a (2)-es esetben $\mathrm{Gal}(L/F)$ egy pro-p csoport, és $\mathrm{Aut}N(L/F)$ pro-p része pedig épp a vad automorfizmusok csoportja. □

A definícióból közvetlenül következik az alábbi állítás:

5.3.12. Állítás.

(1) *Egy aritmetikailag pro-véges bővítés minden végtelen részbővítése is aritmetikailag pro-véges.*

(2) *Ha egy M/K végtelen Galois-bővítésnek van olyan L/K aritmetikailag pro-véges részbővítése, melyre $(M:L)<\infty$, akkor M/K is aritmetikailag pro-véges.*

Megjegyzés: Az aritmetikailag pro-véges bővítések fogalmát – komolyabb testelméleti eszközökkel – lehet általánosítani szeparábilis (nem feltétlenül Galois-) bővítésekre, és igaz marad a (2)-es állítás a következő formában is: Ha az L/F Galois-bővítés aritmetikailag pro-véges, akkor L tetszőleges véges szeparábilis M bővítésére M/K is aritmetikailag pro-véges.

5.3.7. Definíció. Ha L/F aritmetikailag pro-véges, és K egy Galois-bővítése L-nek, akkor $N(K,L/F)$ legyen az összes olyan $N(E/F)$ kompozíciója, ahol E/F végigfut K/F azon Galois részbővítésein, melyekre $(E:L)<\infty$. A W *normák teste* funktor egy L/F aritmetikailag pro-véges bővítéshez hozzárendeli $N(L/F)$-et, és L minden K Galois-bővítéséhez pedig $N(K,L/F)$-et, és $\mathrm{Gal}(K/L)\cong\mathrm{Gal}(N(K,L/F)/N(L/F))\leq\mathrm{Gal}(N(K/F)/N(L/F))$-et.

5.4. $\mathcal{N}$ aritmetikailag pro-véges részcsoportjai

Legyen L/F egy aritmetikailag pro-véges bővítés, melyre L maradékteste $k_L=\mathbb{F}_q$ véges test. Ekkor a normák teste vad automorfizmusainak csoportja épp a $\mathcal{N}(\mathbb{F}_q)$ Nottingham csoport. Tehát egy teljesen elágazó aritmetikailag pro-véges pro-p-bővítés Galois-csoportja a Nottingham csoportba ágyazódik be a „normák teste” funktor által. Érdekes tudni, hogy a $\mathrm{Gal}(L/F)(x)$ felső elágazási részcsoportok hová képződnek ennél a beágyazásnál. Az $\mathcal{N}_i$ részcsoportok analógok az alsó számozású elágazási részcsoportokhoz, ezért természetes a következő definíció:

5.4.1. Definíció. Ha $G\leq_c\mathcal{N}$ egy zárt részcsoport, akkor legyen $G_i:=G\cap\mathcal{N}_i$ és $G_y:=G_{\lceil y\rceil}$! Bevezetjük a következő függvényt:

$$\varphi_G(x):=\int_0^x\frac{dy}{|G:G_y|}.$$

Ekkor G-t a Nottingham csoport egy *aritmetikailag pro-véges részcsoport*jának nevezzük, ha, ha $\lim\limits_{x\to\infty}\varphi_G(x)=+\infty$. Ebben az esetben legyen $\psi_G(x)$ a $\varphi_G(x)$ függvény inverze, és $G(x):=G_{\psi_G(x)}$. A $\psi_G(x)$ függvény szakadási pontjait hívjuk a G részcsoport *felső töréspont*jainak.

5.4.1. Állítás. *Legyen L/F egy teljesen elágazó aritmetikailag pro-véges pro-p-bővítés, és jelöljük G-vel a $\mathrm{Gal}(L/F)$ Galois-csoport képét $\mathcal{N}$-ben. Ekkor minden x-re a $\mathrm{Gal}(L/F)(x)$ csoport képe $G(x)$.*

Bizonyítás. Írjuk fel először L-et véges Galois-bővítések $L=\bigcup_{i\geq1}L_i$ felszálló uniójaként! Elég belátni, hogy tetszőleges n egész számra a $\mathrm{Gal}(L/F)[n]$ alsó elágazási csoport G_n-re képződik, hiszen ekkor $\mathrm{Gal}(L/F)=\mathrm{Gal}(L/F)[0]$ miatt

$$h_{L/F}^{-1}(x)=\int_0^x\frac{dy}{|\mathrm{Gal}(L/F):\mathrm{Gal}(L/F)[y]|}=\int_0^x\frac{dy}{|G:G_y|}.$$

Ez pedig nyilvánvaló, mert $\sigma\in\mathrm{Gal}(L/F)[n]$ pontosan akkor áll fenn, ha elég nagy i-re $\sigma|_{L_i}\in\mathrm{Gal}(L_i/F)[n]$, azaz ha $\alpha_i\in\mathcal{O}_{L_i}$-re $v_{L_i}(\sigma\alpha_i-\alpha_i)\geq n+1$. Node ez pedig épp azt jelenti, hogy $v_N((\sigma\alpha_i)-(\alpha_i))=\lim\limits_{i\to\infty}v_F(N_{L_i/F}(\sigma\alpha_i-\alpha_i))=\lim\limits_{i\to\infty}v_L(\sigma\alpha_i-\alpha_i)\geq n+1$, azaz a σ-hoz tartozó τ benne van $\mathcal{N}_n$-ben. $\square$

5.4.2. Állítás. *Legyen G egy aritmetikailag pro-véges részcsoportja $\mathcal{N}$-nek! Ekkor G Hausdorff dimenziója* $\mathrm{hdim} G = 0$.

Bizonyítás. Tegyük fel az állítással ellentétben, hogy $\xi := \mathrm{hdim} G > 0$. Ekkor van egy olyan $0 < \varepsilon < \xi$ és egy $N \in \mathbb{Z}^+$, melyre minden $n \geq N$ egész szám esetén

$$\frac{\log |G : G_n|}{(n-1)\log p} = \frac{\log |G\mathcal{N}_n : \mathcal{N}_n|}{\log |\mathcal{N} : \mathcal{N}_n|} > \varepsilon.$$

Tehát

$$\begin{aligned}
\lim_{x\to\infty} \varphi_G(x) &= \lim_{x\to\infty} \int_0^x \frac{dy}{|G : G_y|} \\
&= \lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{|G : G_k|} \\
&= \sum_{k=1}^{\infty} p^{-\log |G:G_k|} \\
&\leq \sum_{k=1}^{N-1} p^{-\log |G:G_k|} + \sum_{k=N}^{\infty} p^{-(k-1)\varepsilon \log p} \\
&< \infty.
\end{aligned}$$

Ez pedig ellentmondás. □

Felvetődik a kérdés, hogy $\mathcal{N}$ mely aritmetikailag pro-véges részcsoportjai állnak elő a normák teste funktor képeként. Wintenberger belátta a következőt:

5.4.3. Tétel (Wintenberger, [36]). *Minden $G \leq \mathcal{N}$ kommutatív részcsoportra van olyan L/F aritmetikailag pro-véges bővítés, melyre $W(\mathrm{Gal}(L/F)) = G$.*

Megjegyzés: Speciálisan minden Abel-féle részcsoport aritmetikailag pro-véges, és 0 Hausdorff dimenziós.

5.4.4. Tétel (C. Leedham-Green, A. Weiss [6]). *Minden véges p-csoport beágyazható az $\mathcal{N}$ Nottingham csoportba.*

Bizonyítás. Az állítást elég belátni $\mathcal{N} = \mathcal{N}(\mathbb{F}_p)$-re, hiszen ha $q = p^f$, akkor $\mathcal{N}(\mathbb{F}_q) \leq \mathcal{N}(\mathbb{F}_p)$. Legyen H egy véges p-csoport! Ekkor E. Witt eredménye [38] [39] szerint létezik egy teljesen elágazó K bővítése $\mathbb{F}_p((t))$-nek, melyre $H \cong \mathrm{Gal}(K/\mathbb{F}_p((t)))$. Mivel a bővítés teljesen elágazó, ezért $K \cong \mathbb{F}_p((t))$. Tehát H izomorf $\mathrm{Aut}(\mathbb{F}_p((t))) \cong A(\mathbb{F}_p)$ egy részcsoportjával. És így $|A(\mathbb{F}_p) : \mathcal{N}(\mathbb{F}_p)| = p - 1$ miatt H izomorf $\mathcal{N}(\mathbb{F}_p)$ egy részcsoportjával. □

5.4.5. Következmény ([6]). *$\mathcal{N}$ nem lineáris semmilyen test felett sem.*

Bizonyítás. Ez az előző tételből következik, hiszen rögzített dimenzióban egy feloldható lineáris csoport feloldható hossza korlátos [35]. □

Az 5.4.4-as tételt szeretnénk általánosítani megszámlálható bázisú pro-p csoportokra. A megfelelő Galois-elméleti eredmény a rendelkezésre áll. Vegyünk ugyanis egy G megszámlálható bázisú pro-p csoportot. Ekkor feltehetjük, hogy $G = \varprojlim G_i$, ahol $(G_i)_{i\in\mathbb{N}}$ véges p-csoportok egy inverz rendszere, melyben a leképezések epimorfizmusok, és minden i-re a $G_{i+1} \to G_i$ epimorfizmusok magja p-elemű. Legyen $F := \mathbb{F}_p((t))$! Tegyük fel, hogy valamilyen i-re találunk egy K_i/F teljesen elágazó bővítést, melyre $G_i \cong \mathrm{Gal}(K_i/F)$. Ekkor Iwasawa [19] eredménye szerint a G_{i+1} csoportot előállíthatjuk egy teljesen elágazó K_{i+1}/F bővítés Galois-csoportjaként, ahol $F \leq K_i \leq K_{i+1}$, és a $\mathrm{Gal}(K_{i+1}/F) \to \mathrm{Gal}(K_i/F)$ megszorítás megegyezik a megadott $G_{i+1} \to G_i$ leképezéssel. Így egy $L = \bigcup K_i$ testet konstruálhatunk rekurzívan, melyre $\mathrm{Gal}(L/F) = \varprojlim \mathrm{Gal}(K_i/F) = G$. Ha $L \cong \mathbb{F}_p((t))$ lenne, akkor $G \leq \mathrm{Aut}(L)$ miatt G egy beágyazását kapnánk a Nottingham csoportba. De L általában nem lokális test, és nem is diszkrét az értékelése. Viszont ha el tudnánk érni, hogy L/F aritmetikailag pro-véges legyen, akkor G-t be tudnánk ágyazni a normák teste vad automorfizmusainak csoportjába, ami épp az $\mathcal{N}(\mathbb{F}_p)$ Nottingham csoport. Ez az ötlete Fesenko bizonyításának Camina tételére.

Jelöljük a megfelelő elágazási töréspontokat

$$s_i := s(K_{i+1}/K_i)\text{-vel!}$$

Ekkor az 5.3.8-as állítás fényében csak azt kell elérni, hogy ezen s_i számok elég gyorsan nőjenek. Szükségünk lesz a következő közismert állításra:

5.4.6. Állítás. *Minden p-edfokú L/K Galois-bővítése egy p-karakterisztikájú K testnek Artin-Schreier bővítés, azaz $K(\beta)$ alakba írható, ahol β az*

$$x^p - x - \alpha$$

irreducibilis polinom gyöke valamilyen $\alpha \in K$ esetén.

Bizonyítás. Legyen $\sigma \in \mathrm{Gal}(L/K)$ a bővítés Galois-csoportjának generátoreleme. Ekkor L az $\mathbb{F}_p\mathrm{Gal}(L/K)$ csoportalgebra feletti modulus természetes módon, és a csoportalgebrában $(\sigma-1)^p = \sigma^p - 1 = 0$. Másrészt $\gamma \in L$ esetén $\gamma \in K$ pontosan akkor, ha $(\sigma-1)\gamma = 0$. Tehát van olyan $\gamma \in L$, melyre $(\sigma-1)\gamma \neq 0$, de $(\sigma-1)^2\gamma = 0$, azaz $0 \neq \delta = (\sigma-1)\gamma \in K$. Ekkor a $\beta := \gamma/\delta \in L$ elemre $\sigma\beta = \beta + 1$. Ebből látszik, hogy β minimálpolinomja invariánsan marad, ha az x változó helyére $x+1$-et helyettesítünk. Könnyű ellenőrizni, hogy ekkor a minimálpolinom a kívánt alakú. $\square$

Tehát ha K_i már megvan, akkor $K_{i+1} = K_i(\beta)$ alakú, ahol $\beta^p - \beta = \alpha \in K_i$. Most tegyük fel, hogy $c \in F$, és $E = K_i(\beta_1)$, ahol $\beta_1^p - \beta_1 = \alpha + c$. Ekkor minden $\tau \in \mathrm{Gal}(K_{i+1}/F)$-hez hozzárendelhetjük E/F-nek egy τ' automorfizmusát, melyre $\tau|_{K_i} = \tau'|_{K_i}$ és

$$\tau\beta - \beta = \tau'\beta_1 - \beta_1 =\in K_i,$$

hiszen ha σ-val jelöljük a $\mathrm{Gal}(E/K_i)$ generátorát, akkor $\sigma \in \mathrm{Z}(\mathrm{Gal}(K_{i+1}/F))$ centrumelem (ugyanis p-csoportban p-edrendű normálosztót generál), ezért

$$\sigma(\tau\beta - \beta) = \tau\sigma\beta - \sigma\beta = \tau(\beta+1) - (\beta+1) = \tau\beta - \beta,$$

azaz $\tau\beta - \beta \in K_i$. A kapott τ' valóban automorfizmusa E-nek F felett, mert

$$\begin{aligned}
\tau'(\beta_1^p - \beta_1) &= (\tau'\beta_1)^p - \tau'\beta_1 \\
&= (\beta_1 + \tau\beta - \beta)^p - (\beta_1 + \tau\beta - \beta) \\
&= \beta_1^p - \beta_1 + (\tau\beta)^p - \tau\beta - (\beta^p - \beta) \\
&= \alpha + c + \tau|_{K_i}\alpha - \alpha = \tau'|_{K_i}\alpha + c \\
&= \tau'(\alpha + c).
\end{aligned}$$

Tehát kommutatív az alábbi diagram,

$$\begin{tikzcd}
\mathrm{Gal}(E/F) \arrow[rr, "\simeq"] \arrow[dr] & & \mathrm{Gal}(K_{i+1}/F) \arrow[dl] \\
& \mathrm{Gal}(K_i/F) &
\end{tikzcd}$$

azaz K_{i+1}-et $E = K_i(\beta_1)$-re cserélve ugyanannak a beágyazási problémának a megoldását kapjuk. Így annyi szabadságunk van, hogy α-hoz hozzáadhatunk egy $c \in \mathbb{F}_p((t))$ alaptestbeli elemet. Látni fogjuk, hogy ilymódon el is érhető, hogy az elágazási töréspontok tetszőlegesen nagyok legyenek. Jelöljük t_i-vel K_i prímelemét, $\mathcal{O}_i$-vel az egészeinek a gyűrűjét, és v_i-vel az értékelését, melyre $v_i(t_i) = 1$!

5.4.7. Lemma. *Tegyük fel, hogy $K_{i+1} = K_i(\beta_1)$, ahol β_1 a $\beta_1^p - \beta_1 = \alpha_1 \in K_i$ egyenlet megoldása. Ekkor ha $v_i(\alpha_1) < 0$ és nem osztható p-vel, akkor a K_{i+1}/K_i bővítés teljesen elágazó, továbbá elágazási töréspontja $s_i = -v_i(\alpha_1)$.*

Bizonyítás. Mivel $\beta_1^p - \beta_1 = \alpha_1$, ezért $v_i(\beta_1) = -n/p$, ha kiterjesztjük az értékelést, és $v_i(\alpha_1) = n$. Mivel n és p relatív prímek, ezért a bővítés teljesen elágazó. Továbbá léteznek olyan $b, d \in \mathbb{Z}$ egész számok, melyekre $bp - dn = 1$. Vegyük $t_{i+1} := \beta_1^d t_i^b$-t! Ekkor $v_i(t_{i+1}) = 1/p$ és $K_{i+1} = \mathbb{F}_p((t_{i+1}))$. Feltehetjük, hogy $\mathrm{Gal}(K_{i+1}/K_i) = \langle\sigma\rangle$, ahol $\sigma\beta_1 = \beta_1 + 1$, így

$$\begin{aligned}
\sigma t_{i+1} &= \sigma(\beta_1^d t_i^b) \\
&= (\beta_1 + 1)^d t_i^b \\
&= t_{i+1} + d t_{i+1}/\beta_1 + \cdots + t_{i+1}/\beta_1^d.
\end{aligned}$$

Most $v_i(t_{i+1}/\beta_1^a) = v_i(t_{i+1}) + an/p = (an+1)/p$ mindegyik szóbanforgó a-ra. Mivel $d \not\equiv 0 \pmod p$, ezért $v_i(\sigma t_{i+1} - t_{i+1}) = (n+1)/p$, ami épp azt jelenti, hogy $s_i = n$. □

Ha azt szeretnénk, hogy s_i minél nagyobb legyen, akkor úgy tűnhet, hogy c-t csak meg kell választani olyannak, aminek minél nagyobb abszolútértékű negatív értékelése van. Azonban ha $v_i(c) < v_i(\alpha)$, akkor $v_i(\alpha_1) = v_i(\alpha + c) = v_i(c)$, ami pedig osztható K_i/F fokával, hiszen a bővítés teljesen elágazó. Speciálisan $v_i(\alpha_1) \equiv 0 \pmod p$, és így az előző lemma nem alkalmazható. Tehát ennél ügyesebbnek kell lennünk. Legyen $\wp(x) := x^p - x$! Ekkor az 5.4.7-es lemma bizonyításából látszik, hogy a $K(\beta)$ bővítésben ha $\wp(\gamma) \in K$ valamilyen $\gamma \in K(\beta) \setminus K$-ra, akkor $\gamma = k\beta + \delta$ alakú, ahol $k \in \mathbb{F}_p$, illetve $\delta \in K$, hiszen ez esetben $\sigma\gamma - \gamma \in \mathbb{F}_p$. Így az ($F \hookrightarrow K_i$ beágyazás által indukált)

$$F/\wp(F) \to K_i/\wp(K_i)$$

homomorfizmus magja véges dimenziós $\mathbb{F}_p$ fölött, és ezért az

$$F/\wp(F) \to K_i/(\wp(K_i) + t_i^{-k}\mathcal{O}_i)$$

leképezés sem a 0 leképezés. Tehát találhatunk egy olyan $c \in F$-et, amely nincs $\wp(K_i)+t_i^{-k}\mathcal{O}_i$-ben. Egy ilyen c elem felírható az alábbi összeg alakban:

5.4.8. Lemma. *Tegyük fel, hogy $c \in F$, de $c \notin \wp(K_i)+t_i^{-k}\mathcal{O}_i$! Ekkor létezik olyan $x, z \in K_i$, melyre*

$$c = \wp(z) + x, \text{ és } p \nmid v_i(x) < -k.$$

Bizonyítás. Mivel $v_i(c)$ osztható p-vel, ezért

$$c = c_{-pn}t_i^{-pn} + c_{-pn+1}t_i^{-pn+1} + \cdots = \wp(c_{-pn}t_i^{-n}) + y$$

valamely $v_i(y) > v_i(c)$-re. Ezt folytathatjuk, amíg $v_i(y)$ negatív és osztható p-vel. Tehát $c = \wp(z) + x$ olyan $x, z \in K_i$ elemekkel, melyekre $v_i(x) \geq 0$, vagy $v_i(x)$ negatív és relatív prím p-hez. Node $c \notin \wp(K_i) + t_i^{-k}\mathcal{O}_i$, tehát a második eset áll fenn, és $p \nmid v_i(x) < -k$. □

Tegyük fel most, hogy elértük a $K_{i+1} = K_i(\beta)$ szintet, ahol $\beta^p - \beta = \alpha \in K_i$. Legyen $k \geq -v_i(\alpha)$ egy nagy pozitív egész, válasszunk egy $c \in F \setminus \big(\wp(K_i) + t_i^{-k}\mathcal{O}_i\big)$ elemet, és legyen β_1 a $\beta_1^p - \beta_1 = \alpha + c$ egyenlet megoldása! Legyen továbbá x, z mint az előző lemmában, és $\beta_2 := \beta_1 - z$! Ekkor $\beta_2^p - \beta_2 = \alpha + x$, ahol $v_i(\alpha + x) = v_i(x) < -k$, és $K_i(\beta_2) = K_i(\beta_1)$. Az 5.4.7-es lemma szerint

$$s_i = s(K_i(\beta_1)/K_i) = s(K_i(\beta_2)/K_i) = -v_i(\alpha + x) > k.$$

Tehát K_{i+1}-et $K_i(\beta_1)$-gyel helyettesítve elérhetjük, hogy $s_i = s(K_{i+1}/K_i)$ tetszőlegesen nagy legyen. Speciálisan konstruálhatunk egy olyan (K_i) testbővítéssorozatot, melyre

$$s_1 + (s_2 - s_1)p^{-1} + \cdots + (s_i - s_{i-1})p^{-(i-1)}$$

szigorúan monoton nőve tart végtelenhez. A 5.3.8-as lemma alkalmazásával azt kapjuk, hogy

5.4.9. Tétel. *Ha G egy megszámlálható bázisú pro-p csoport, akkor $\mathbb{F}_p((t))$-nek van olyan L aritmetikailag pro-véges bővítése, melyre $G \cong \mathrm{Gal}(L/\mathbb{F}_p((t)))$.*

Ennek következménye a fő eredmény ebben a fejezetben:

5.4.10. Tétel (Camina, [6]). *Minden megszámlálható bázisú pro-p csoport izomorf az $\mathcal{N}(\mathbb{F}_p)$ Nottingham csoport egy részcsoportjával.*

Fesenko bizonyítása. Alkalmazzuk a W funktort az aritmetikailag pro-véges L/F bővítésre. Az 5.3.9-es tétel szerint ez egy $G \hookrightarrow \mathcal{N}(\mathbb{F}_p)$ beágyazást ad. □

Megjegyzés: Camina eredeti bizonyítása szintén Galois-elméleti jellegű volt, de nem használta a normák teste funktort. Valójában mindkét konstrukció olyan részcsoportokat ad, melyek benne vannak a Nottingham csoport torziójának lezártjában.

5.5. p-edrendű elemek

Az előző fejezetben láttuk, hogy minden véges p-csoport beágyazható a Nottingham csoportba, de az a bizonyítás nem explicit: p^2 rendű elemre nem is ismert explicit példa. Viszont Klopsch [24] osztályozta a p-edrendű elemeket konjugált osztály erejéig. Az ő második bizonyításának módszerét követem. Vegyük észre először, hogy a Nottingham csoportban egy torzióelem mélysége mindig relatív prím p-hez a 2.3.1-es lemma miatt.

5.5.1. Lemma. *Legyen $(t)f, (t)g \in \mathcal{N}(\mathbb{F}_q)$ két p-edrendű elem a Nottingham csoportban, melyre*

$$\begin{aligned}(t)f &= t\left(1+\sum_{j=k}^{\infty} f_j t^j\right), \quad f_k \neq 0\\ (t)g &= t\left(1+\sum_{j=n}^{\infty} g_j t^j\right), \quad g_n \neq 0.\end{aligned}$$

Ekkor f és g pontosan akkor konjugáltak, ha $n = k$ és $f_k = g_n$.

Bizonyítás. Az egyik irány triviális: ha f és g konjugáltak, akkor persze $k = n$, és $f_k = g_n$. A másik irányhoz legyen

$$\begin{aligned}(t)f &:= t\left(1+\sum_{j=k}^{\infty} f_j t^j\right),\\ (t)g &:= t\left(1+\sum_{j=k}^{\infty} g_j t^j\right), \quad f_k = g_k \neq 0\end{aligned}$$

két p-edrendű elem, $H_1 := \langle f\rangle$, illetve $H_2 := \langle g\rangle$, továbbá $K_i := \mathrm{Fix}(H_i) \leq \mathbb{F}_q((t))$ a fixtestek ($i = 1, 2$)! Ekkor a $\mathbb{F}_q((t))/K_i$ bővítések Galois bővítések, melyek Galois-csoportja $\mathrm{Gal}(\mathbb{F}_q((t))/K_i) = H_i$. Tehát ahhoz, hogy az f és a g elemek konjugáltak, elég belátni, hogy van olyan $\sigma \in \mathcal{N}(\mathbb{F}_q)$, melyre $K_1\sigma = K_2$, mert ez épp azt jelenti, hogy $\sigma^{-1}H_1\sigma = H_2$. Az 5.4.6-os állítás miatt a $\mathbb{F}_q((t))/K_i$ bővítés egy $x^p - x - \alpha_i$ alakú polinom gyökével való bővítés, ahol $\alpha_i \in K_i$. Továbbá feltehetjük, hogy $p \nmid v_{K_i}(\alpha_i) < 0$, mert α_i-t megváltoztatva tetszőleges $\wp(K_i)$-beli elemmel ugyanazt a bővítést kapjuk, és minden pozitív értékelésű elem benne van $\wp(K_i)$-ben, továbbá minden negatív, p-vel osztható mélységű elemmel van p-vel nem osztható mélységű, modulo $\wp(K_i)$ kongruens elem. Ekkor a definíció és az 5.4.7-es lemma szerint az $\mathbb{F}_q((t))/K_1$ és az $\mathbb{F}_q((t))/K_2$ bővítés elágazási töréspontja megegyezik, azaz:

$$-v_{K_1}(\alpha_1) = s(\mathbb{F}_q((t))/K_1) = D(f) = k = D(g) = s(\mathbb{F}_q((t))/K_2) = -v_{K_2}(\alpha_2).$$

Most legyen $\beta_i \in \mathbb{F}_q((t))$ az $x^p - x = \alpha_i$ egyenlet (egyik) gyöke ($i = 1, 2$)! Ekkor

$$v_{\mathbb{F}_q((t))}(\beta_i) = v_{\mathbb{F}_q((t))}(\alpha_i)/p = p v_{K_i}(\alpha_i)/p = -k.$$

Tehát ha $\beta_1 = \sum_{l=-k}^{\infty} a_l t^l$, és $\beta_2 = \sum_{l=-k}^{\infty} b_l t^l$ a két hatványsor alak, akkor

$$c_1 + \sum_{l=-k}^{\infty} a_l t^l = \beta_1 f = \sum_{l=-k}^{\infty} a_l t^l \left(1 + \sum_{j=k}^{\infty} f_j t^j\right)^l, \text{ illetve}$$

$$c_2 + \sum_{l=-k}^{\infty} b_l t^l = \beta_2 g = \sum_{l=-k}^{\infty} b_l t^l \left(1 + \sum_{j=k}^{\infty} g_j t^j\right)^l, \text{ ahol}$$

$0 \neq c_1, c_2 \in \mathbb{F}_p \leq \mathbb{F}_q$. Végezzük el az l-edik hatványra emeléseket (ahol kell, ott reciprokot is vegyünk), vonjuk ki mindkét egyenlet mindkét oldalából az egyező összeadandókat, és hasonlítsuk össze a konstans tagokat! Ekkor azt kapjuk, hogy $c_1 = -a_{-k} k f_k$, illetve $c_2 = -b_{-k} k g_k$. Mivel $p \nmid k$ és $f_k = g_k$, ezért azt kapjuk, hogy $\frac{a_{-k}}{b_{-k}} \in \mathbb{F}_p$, és így β_2-t lecserélve egy egészszám-szorosára elérhetjük, hogy $a_{-k} = b_{-k}$ legyen. Vegyük észre, hogy a $-k$ értékelésű elemeken a k-adik gyökvonás elvégezhető (és $\mathbb{F}_q$-beli k-adik egységgyök szorzótól eltekintve egyértelmű), tehát van olyan gyök, melyre $(\beta_i/a_{-k})^{-1/k} \in t(1 + t\mathbb{F}_q[[t]])$. Továbbá mivel $t(1 + t\mathbb{F}_q[[t]])$-n tranzitívan hat a Nottingham csoport, ezért van olyan $\sigma \in \mathcal{N}$, melyre $(\beta_1/a_{-k})^{-1/k}\sigma = (\beta_2/a_{-k})^{-1/k}$, és így $\beta_1\sigma = \beta_2$, sőt $\alpha_1\sigma = \alpha_2$. Ebből viszont következik, hogy $K_1\sigma = K_2$, mert csak azt kell ellenőrizni, hogy K_1 valamelyik prímeleme K_2 valamelyik prímelemébe megy σ-nál. Ezen prímelemeknek megfelel például α_1 illetve α_2 valamelyik $-1/k$-adik hatványa, hiszen $p \nmid k$ és $v_{K_i}(\alpha_i) = -k$ $(i = 1, 2)$ miatt a k-adik gyökvonás elvégezhető ezeken az elemeken. □

Most már osztályozni tudjuk a p-edrendű elemeket:

5.5.2. Tétel. *A Nottingham csoport p-edrendű elemeinek konjugált osztályai reprezentálhatók a*

$$(t)F(n, \lambda) := t \sqrt[n]{\frac{1}{1 - \lambda t^n}}$$

alakú elemekkel, ahol $p \nmid n \in \mathbb{Z}^+$ és $\lambda \in \mathbb{F}_q$.

Bizonyítás. Könnyű ellenőrizni, hogy ezek valóban p-edrendű elemek, továbbá, hogy

$$(t)F(n, \lambda) = t(1 + n\lambda t^n + \text{magasabb fokú tagok}),$$

ezért a lemma miatt készen vagyunk. □

5.5.3. Következmény. *Minden p-edrendű elem stabilizál egy egydimenziós részalgebrát* Lie$(\mathcal{N})$*-ben.*

Bizonyítás. Az állítást elég belátni az $F(n, \lambda)$ alakú elemekre. A 3.4.7-es példa szerint viszont $F(n, \lambda)$ stabilizálja $\langle e_n \rangle$-et. □

5.6. További számelméleti kapcsolatok

Camina munkájának egy következménye, hogy minden végesen generált pro-p csoport előállítható egy aritmetikailag pro-véges bővítés Galois-csoportjaként, ha a karakterisztika p. Továbbá Sen eredménye a következő:

5.6.1. Tétel (Sen, [30]). *Egy 0-karakterisztikájú lokális test olyan teljesen elágazó bővítése, melynek Galois-csoportja p-adikus analitikus, mindig aritmetikailag pro-véges.*

Sokáig ez volt az egyetlen eredmény 0 karakterisztikában. Megoldatlan volt, hogy létezik-e olyan aritmetikailag pro-véges, vagy akár csak mélyen elágazó bővítés, mely nem p-adikus analitikus, illetve nincs is végtelen p-adikus analitikus faktora (ami elegendő volna ahhoz, hogy a bővítés mélyen elágazó legyen). Fesenko [12] adott egy példát nem p-adikus analitikus aritmetikailag pro-véges bővítésre, bár ennek a példának vannak p-adikus analitikus faktorai.

Mivel – ahogy Coates és Greenberg [8] leírta – a mélyen elágazó bővítéseknek szép Kummer-elmélete van, ezért felvetődött az alábbi kérdés:

5.6.2. Probléma (Coates és Greenberg). *Van-e olyan teljesen és mélyen elágazó L/F bővítés, melyre F egy véges bővítése $\mathbb{Q}_p$-nek, és $\mathrm{Gal}(L/F)$-nek nincsenek végtelen p-adikus analitikus faktorai?*

Fesenko [13] belátta, hogy a 3.1.4-es példában értelmezett $\mathfrak{A}_q \leq \mathcal{N}$ részcsoport $q = p^r$ esetén (is) öröklődően épp végtelen, továbbá

5.6.3. Tétel (Fesenko, [13]). *Legyen $q = p^r > p$, és F egy legalább q-adfokú véges elágazásmentes bővítése $\mathbb{Q}_p$-nek. Ekkor van olyan L/F teljesen elágazó aritmetikailag pro-véges – speciálisan mélyen elágazó – Galois bővítés, melynek Galois-csoportja $\mathfrak{A}_q$, és tetszőleges $F \leq M \leq K \leq L$ közbülső testekre $\mathrm{Gal}(K/M)$ nem p-adikus analitikus, ha $(M : F) < \infty$ és K/M egy végtelen Galois-bővítés.*

Megjegyzés: Mivel $\mathfrak{A}_q \leq \mathcal{N}$ Hausdorff dimenziója $\mathrm{hdim}\mathfrak{A}_q = 1/q > 0$, ezért az 5.4.2-es állítás szerint $W(\mathrm{Gal}(L/F)) \neq \mathfrak{A}_q$, viszont $W(\mathrm{Gal}(L/F)) \cong \mathfrak{A}_q$, azaz ez a csoport a normák teste funktor által egy másik, vele izomorf csoportra képződik.

Irodalomjegyzék

[1] J. L. Abercrombie, Subgroups and subrings of profinite rings, *Math. Proc. Cambr. Phil. Soc.* **116** (1994), 209–222.

[2] M. Abért, Group laws and free subgroups in topological groups, *Bull. London Math. Soc.*, preprint

[3] Y. Barnea and B. Klopsch, Index Subgroups of the Nottingham Group, *Adv. Math.* **180** (2003), no. 1, 187–221.

[4] Y. Barnea and M. Larsen, Random generation in simple algebraic groups over local fields, *J. Algebra* **271** (2004), no. 1, 1–10.

[5] Y. Barnea and A. Shalev, Hausdorff dimension, pro-p groups and Kac-Moody algebras, *Trans Amer. Math. Soc.* **349** (1997), 5073–5091.

[6] R. Camina, Subgroups of the Nottingham group, *J. Algebra* **196** (1997) 101–113.

[7] R. Camina, The Notthingam Group, in: *New Horizons in Pro-p Groups*, in: Progr. Math., vol. 184, Birkhäuser Boston, Cambridge, MA, 2000, 205–221.

[8] J. Coates and R. Greenberg, Kummer theory for abelian varieties over local fields, *Invent. Math.* **124** (1996), 129–174.

[9] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199–205.

[10] J. D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic Pro-p Groups*, 2nd edition, in: Cambridge Stud. Adv. Math. 61, Cambridge Univ. Press, Cambridge, 1999.

[11] M. Ershov, New just-infinite pro-p groups of finite width and subgroups of the Nottingham group, *J. Algebra* **275** (2004) 419–449.

[12] I. Fesenko, On deeply ramified extensions, *J. London Math. Soc.* **57**(2) (1998), 325–335.

[13] I. Fesenko, On just infinite pro-p-groups and arithmetically profinite extensions of local fields, *J. Reine Angew. Math.* **517** (1999) 61–80.

[14] I. Fesenko and S. Vostokov, *Local Fields and Their Extensions*, A.M.S., Providence, R.I., 1993.

[15] J.-M. Fontaine and J.-P. Wintenberger, Le "corps des normes" de certaines extensions algébriques de corps locaux, *C. R. Acad. Sci. Paris Sér. A-B* **288** (1979), no. 6, A367–A370.

[16] P. Hegedűs, The Nottingham Group for $p = 2$, *J. Algebra* **246** (2001), 55–69.

[17] P. Hegedűs, Topics from Group Theory, Ph.D. thesis, University of Cambridge, 2001.

[18] K. Iwasawa, *Local Class Field Theory*, Oxford Mathematical Monographs O.U.P., 1986.

[19] K. Iwasawa, On solvable extensions of algebraic number fields, *Ann. Math.* **58** (1953), 548–572.

[20] S. A. Jennings, Substitution groups of formal power series under substitution, *Canad. J. Math.* **6** (1954), 325–340.

[21] D. L. Johnson, The group of formal power series under substitution, *J. Austral. Math. Soc.* **45** (1988), 296–302.

[22] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Ded.* **36** (1990), 67–87.

[23] Y. Kawada, On the ramification theory of infinite algebraic extensions, *Ann. Math.* **58** (1953), 24–47.

[24] B. Klopsch, Automorphisms of the Nottingham group, *J. Algebra* **223** (2000), 37–56.

[25] B. Klopsch, Normal subgroups in substitution groups of the formal power series, *J. Algebra* **228** (2000), 91–106.

[26] M. W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Ded.* **56** (1995), 103–113.

[27] A. Mann, Positively finitely generated groups, *Forum Math.* **8** (1996), 429–459.

[28] S. Saks, *Theory of the Integral*, Dover, 1964.

[29] M. P. F. du Sautoy and I. Fesenko, Where the Wild Things Are: Ramification Groups and the Nottingham Group, in: *New Horizons in Pro-p Groups*, in: Progr. Math., vol. 184, Birkhäuser Boston, Cambridge, MA, 2000, 287–328.

[30] Sh. Sen, Ramification in p-adic Lie extensions, *Invent. Math.* **17** (1972), 44–50.

[31] A. Shalev, Asymptotic group theory, *Notices Amer. Math. Soc.* **48** (2001), 383–389.

[32] A. Shalev, Lie Methods in the Theory of pro-p Groups, in: *New Horizons in Pro-p Groups*, in: Progr. Math., vol. 184, Birkhäuser Boston, Cambridge, MA, 2000, 1–54.

[33] B. Szegedy, Almost all finitely generated subgroups of the Nottingham group are free, *Bull. London Math. Soc.* **37** (2005), no. 1, 75–79.

[34] J. T. Tate, p-divisible groups, 1967 *Proc. Conf. Local Fields* (Driebergen, 1966), 158–183.

[35] B. A. F. Wehrfritz, *Infinite Linear Groups*, Springer Verlag, 1973.

[36] J.-P. Wintenberger, Extensions abéliennes et groupes d'automorphismes des corps locaux, *C. R. Acad. Sci. série A*, **290** (1980), 201–203.

[37] J.-P. Wintenberger, Le corps des normes de certaines extensions infinies de corps locaux; applications, *Ann. Sci. École Norm. Sup. (4)* **16** (1983), no. 1, 59–89.

[38] E. Witt, Der Existenzsatz für abelsche Funktionenkörper, *J. für Mathematik* **173** (1935), 43–51.

[39] E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^k, *J. für Mathematik* **174** (1936), 237–245.

[40] I. O. York, The group of formal power series under substitution, Ph.D. thesis, Nottingham University, 1990.