Eötvös Loránd Tudományegyetem

Természettudományi Kar

Algebra és Számelmélet

Tanszék

Osztálytestelmélet

Témavezető:
dr. Zábrádi Gergely
egyetemi docens

Szerző:
Kiss Zsombor
matematikus MSc

Budapest, 2024

Tartalomjegyzék

1. fejezet

Bevezetés

A számelmélet egyik legnagyobb feladata $\mathbb{Q}$ Galois-bővítéseinek megértése. Ezen testek leírása teljes általánosságban egy jelenleg elérhetetlen cél. Azonban ha csak $\mathbb{Q}$ Abel-bővítéseire koncentrálunk, akkor a híres Kronecker-Weber tétel ad kielégítő választ: $\mathbb{Q}$ Abel-bővítései pontosan a körosztási testek résztestei.

Az osztálytestelmélet fő célja egy általános K számtest Abel-bővítéseinek leírása K belső tulajdonságainak segítségeivel, így általánosítva a Kronecker-Weber tételt. Valóban, később látni fogjuk, hogy az osztálytest elmélet tételeinek egyszerű következménye a $K = \mathbb{Q}$ esetben. Kicsit pontosabban, ezek a tételek szolgáltatni fognak nekünk egy homomorfizmust, az Artin leképzést, aminek segítségével össze tudunk kötni három, első ránézésre teljesen különböző dolgot: K ideálstruktúráját, a számtestek közti norma leképzést, K Abel-bővítéseit és azok Galois-csoportját.

Dolgozatom első fejezetében Kummer-elméletről fogok írni némi motivációként az osztálytestelmélet előtt, hiszen már itt is megfigyelhető lesz egy bizonyos kapcsolat egy test belső struktúrája és annak bővítései között.

Az ezután következő fejezetekben ismertetni fogom az osztálytestelmélet főbb tételeit és azok különböző megfogalmazásait, bizonyítások nélkül. Valamint bemutatom, hogyan lehet ezeket a tételeket használni, néhány érdekes következményen keresztül.

A végső fejezetekben bevezetem az absztrakt osztálytestelméletet, aminek segítségével bizonyítani fogjuk a lokális reciprocitástételt. A bizonyításban nagyrészt Neukirch[1] könyvét fogom követni.

Mivel az osztálytestelmélet nagyban épít az alapvető algebrai számelmélet eredményeire, ezért ezeket adottnak fogom venni. A szükséges tudás elsajátítható [1] első

két fejezetéből, [2]-ből, vagy lényegében bármely bevezető jellegű algebrai számelmélet könyvből. Továbbá feltételezem, hogy az olvasó ismeri a Krull-topológiát végtelen Galois-csoportokon és a Galois-elmélet fő tételének általánosítását végtelen bővítésekre,[3] valamint, hogy egy kicsit általánosabban, ismeri a provéges csoportok definícióját. Kohomológiai ismeretek azonban *nem* szükségesek, a hosszú egzakt sorozatok és néhány következményük (a kígyó-lemma) kivételével.

A dolgozatomban, a tömörségre törekedve, több bizonyítást is csak elég vázlatosan írtam le, azonban minden kihagyott lépés igazolható maximum egy-két mondattal.

2. fejezet

Kummer-elmélet

Egy K test véges Abel-bővítéseit, vagy általánosabban n exponensű Abel-bővítéseit, jelentősen egyszerűbb karakterizálni, ha K tartalmazza az n-edik egységgyököket és $n \nmid char(K)$. Ekkor a következő tételt kapjuk:

1. Tétel. *Legyen L egy n exponensű (nem feltétlenül véges) Abel-bővítése K-nak. Ekkor $\Delta = (L^\times)^n \cap K^\times$ mellett $L = K(\sqrt[n]{\Delta})$. Továbbá ha L ciklikus, akkor létezik olyan $a \in K$ elem, hogy $L = K(\sqrt[n]{a})$.*

Bizonyítás. Ha $\alpha^n \in \Delta$ akkor létezik olyan $\beta \in L$, hogy $\beta^n = \alpha^n$, vagyis egy egységgyök faktorral térnek el, így $\alpha \in L$, tehát $K(\sqrt[n]{\Delta}) \subseteq L$. A másik tartalmazást elég belátni L ciklikus résztesteire, hiszen ezek generálják azt. Legyen M egy d-edfokú ciklikus bővítés, σ által generált Galois-csoporttal és ζ egy d-edik egységgyök. Mivel $N_{M|K}(\zeta) = 1$, ezért a Hilbert 90-es tétel[2] miatt létezik olyan $\alpha \in M$, hogy $\zeta = \alpha^{\sigma-1}$. Ezt az n-edikre emelve látjuk, hogy σ fixen hagyja α^n-t. Ez lesz a választásunk a tételben szereplő a-ra, hiszen α generálni fogja M-et, mert $\alpha^{\sigma^i} = \zeta^i \cdot \alpha \neq \alpha$. □

Továbbá bizonyítható a következő tétel, ami leírja K n-exponensű Abel-bővítéseinek Galois-csoportjait K multiplikatív csoportjának függvényében:

2. Tétel. *A $\Delta \to K(\sqrt[n]{\Delta})$ és az $L \to (L^\times)^n \cap K^\times$ leképzések egymás inverzei, és K n exponensű Abel-bővítéseit megfeleltetik $K^\times$ azon részcsoportjaival, amik tartalmazzák $(K^\times)^n$-t, és $\Delta/(K^\times)^n$ izomorf lesz $Hom(G(L \mid K, \mu_n))$-el a következő módon: minden $a \in \Delta$ definiál egy $G(L \mid K) \to \mu_n$ leképzést a $\sqrt[n]{a}^{\sigma-1}$ képlettel. (Végtelen bővítésnél Hom csak a folytonos leképzéseket jelöli.)*

Bizonyítás. A bizonyításban a Pontyagin-dualitást fogjuk alkalmazni,[4] amit véges csoportok esetén triviális igazolni, így az itteni bizonyítás a véges bővítések esetében teljes lesz a Pontryagin-dualitás teljes ereje nélkül is.

Legyen G egy lokálisan kompakt, Hausdorff Abel-csoport és jelölje $\hat{G} = Hom(G, S^1)$ a folytonos csoporthomomorfizmusok csoportját a pontonkénti szorzás műveletével, ahol S^1-et $\mathbb{C}^\times$ egység normájú elemeinek részcsoportjaként fogjuk fel a szokásos topológiával ellátva. $\hat{G}$-én a következő bázis adja a topológiát: $S_{K,U} = \{\phi \in \hat{G} \mid \phi(K) \subset U\}$ ahol U nyílt S^1-ben és K kompakt G-ben. Be lehet látni, hogy ekkor $\hat{G}$ maga is lokálisan kompakt és Hausdorff Abel-csoport lesz, ekkor a dualizálást alkalmazhatjuk kétszer is, és kapunk egy természetes injekciót $G \rightarrowtail \hat{\hat{G}} : a \to \chi_a \mid \chi_a(\phi) = \phi(a)$. A Pontryagin-dualitás azt mondja ki, hogy ez egy izomorfizmus és így a természetesség miatt a $\hat{}$ funktor kategóriák egy ekvivalenciáját adja meg a lokálisan kompakt Hausdorff Abel-csoportok kategóriája és annak a $\hat{}$ képeként előálló kategória között.

Amennyiben G véges és diszkrét, akkor már a $\hat{}$ is izomorfizmust ad, hiszen ez pont G karaktereinek csoportja lesz a diszkrét topológiával, ami izomorf G-vel a végesen generált Abel-csoportok alaptétele miatt. Továbbá ha G egy n-exponensű csoport akkor $\hat{G} = Hom(G, \mu_n)$, maga is n-exponensű lesz.

Tehát, visszatérve a bizonyításhoz, legyen $\Delta(L) = (L^\times)^n \cap K^\times$ és $L(\Delta) = K(\sqrt[n]{\Delta})$, azt már láttuk, hogy $L(\Delta(L)) = L$, tehát azt kell megmutatnunk, hogy $\Delta' := \Delta(L(\Delta)) = \Delta$. Az egyértelmű, hogy $\Delta \subset \Delta'$. Most definiálunk egy homomorfizmust $\psi : \Delta' \to Hom(G(L \mid K, \mu_n)) : a \to \sqrt[n]{a}^{\sigma-1}$ ami $\sqrt[n]{a}$ megválasztásától független. $\ker\psi = K^n$, hiszen $\sqrt[n]{a}^{\sigma-1} = 1$ minden automorfizmusra, akkor és csak akkor ha $\sqrt[n]{a}$ benne van a Galois-csoport fixtestébe, azaz K-ba, és így $a \in K^n$. A szürjektívitás bebizonyításához legyen $\chi \in Hom(G, \mu_n)$ tetszőleges. Mivel χ folytonos, ezért $\ker\chi$ zárt és egy normálosztó, hiszen G Abel-csoport, vagyis ha T $\ker\chi$ fixteste, akkor $G(T \mid K) \cong G/\ker\chi$, ami így egy $d \mid n$ fokú ciklikus bővítés. Az előző tételhez hasonlóan generálja σ ezt a csoportot és legyen $\zeta = \chi(\sigma)$ egy primitív d-edik egységgyök. A Hilbert 90-es tétel miatt létezik egy $\alpha \in T$ amire $\zeta = \alpha^{\sigma-1}$ és az is igaz, hogy $(\alpha^n)^\sigma = (\zeta \cdot \alpha)^n = \alpha^n$, tehát $\alpha^n \in \Delta'$ és $\chi(\sigma) = \alpha^{\sigma-1}$.

Azaz most van egy kommutatív diagramunk:

$$\begin{array}{ccc} \Delta/K^n & \hookrightarrow & Hom(G/H, \mu_n) \\ \downarrow & & \downarrow \\ \Delta'/K^n & \xrightarrow{\cong} & Hom(G, \mu_n) \end{array}$$

ahol $H = \{\sigma \in G \mid \psi_a(\sigma) = 1 \forall a \in \Delta\}$ a leképzések pedig az inklúziók, ψ és annak megszorítása. Először belátjuk, hogy $H = 1$. Valóban, ha $\sigma \in H$, akkor az fixen hagyja $\sqrt[n]{\Delta}$-át és így az általa generált testet, L-t is, azaz $\sigma = 1$. Tehát már csak azt kell megmutatnunk, hogy $\psi \mid_\Delta$ szürjektív mert akkor azt kapjuk a kommutatív diagramunkból, hogy az inklúzió egy izomorfizmus, és $\Delta = \Delta'$. A Pontryagin dualitás miatt ez következne abból, ha $\hat{\psi} : G/H \to Hom(\Delta/K^n, \mu_n)$ injektív lenne, de hiszen ez injektív, mert H pont a $\hat{\psi} : G \to Hom(\Delta/K^n, \mu_n)$ duális leképzés magja.

□

Például $\mathbb{Q}$ maximális 2 exponensű bővítése $\mathbb{Q}(i, \sqrt{2}, ..\sqrt{p}...)$ és Galois-csoportja izomorf lesz a prímek és i felett vett C_2 direkt szorzattal. Általánosabban ha $K \supset \mu_n$ egy számtest, akkor annak multiplikatív csoportját megérthetjük a Minkowski-egységtétel, az ideálok egyértelmű faktorizációjának és az ideálosztály-csoport segítségével és több esetben is le tudjuk írni a maximális n exponensű bővítést.

Felmerül a kérdés, hogy mi történik akkor, ha $char(K) = p \mid n$. Ekkor úgynevezett Artin-Schreier-elmélet ad részleges választ: az $a \to a^n$ művelet helyett az $a \to a^p - a$ operátort tekintjük L additív csoportja felett és a Kummer-elmélettel teljesen analóg módon így bizonyíthatók hasonló állítások a p exponensű Abel-bővítésekre.

Kicsit általánosabban legyen G egy k test abszolút Galois-csoportja a Krull-topológiával ellátva, és $\bar{k}$ a maximális szeparábilis bővítés. Továbbá legyen G_K a K testet fixen hagyó automorfizmusok csoportja. Ekkor $\bar{k}$ additív és multiplikatív csoportjai G modulusok (azaz $\mathbb{Z}G$ modulusok) lesznek, és igaz lesz rájuk, hogy előállnak a G_K-ák által rögzített részmodulusok uniójaként, ahol K véges bővítés. Ezt általánosítva egy A modulusról azt mondjuk, hogy folytonos G modulus, ha G modulus és $A = \bigcup_{K \text{véges}} A_K$ ahol A_K a G_K által rögzített részmodulus. A folytonos modulusokat multiplikatívan fogom írni és $\sigma \in G$ hatását a^σ-ával fogom jelölni.

Észrevehetjük, hogy az $a \to a^n$ operátorról azt használtuk, hogy szürjektív G endomorfizmus $A = \bar{k}^\times$-n, hogy a magja egy n elemű ciklikus csoport és azt, hogy

a Hilbert 90-es tétel igaz. Kicsit pontosítva legyen $\rho : A \to A$ egy szürjektív G modul homomorfizmus (azaz $\mathbb{Z}G$ modul homomorfizmus,) melynek kernelje, μ_ρ egy n rendű ciklikus csoport és legyen K egy olyan test amire $\mu_\rho \subset A_K$. Ekkor minden $\Delta \subset A_K$-ra $K(\rho^{-1}(\Delta)) \mid K$ egy n exponensű Abel-bővítés lesz, ahol egy $\Delta \subset A$ által generált testet úgy definiáljuk, hogy a Δ-át rögzítő elemek és G_K által generált csoport lezártja által rögzített test. Valóban, könnyen igazolható, hogy tetszőleges $\alpha \in \rho^{-1}(a)$-ra $\sigma \to \alpha^{\sigma-1}$ egy az α-ától független injektív homomorfizmust definiál $G(K(\rho^{-1}(a)) \mid K)$-ból μ_ρ-ba, ami így n exponensű, ciklikus, és mivel $K(\rho^{-1}(\Delta))$ előáll ilyen testek kompozitumaként, ezért az is egy n exponensű Abel-bővítés lesz.

A Hilbert 90-es tétel megfelelőjének megfogalmazásához szükségünk van a norma definíciójára általános folytonos G-modulusokra.

1. Definíció. Leqyen $L \mid K$ egy véges bővítés, ekkor $N_{L:K} : A_L \to A_K$-át a következő képlettel definiáljuk: $N_{L:K}(a) = \prod_{\sigma \in G(L|K)} a^\sigma$. Továbbá definiáljuk a következő csoportot: $H^{-1}(G(L \mid K), A_L) =_{N_{L|K}} A_L / I_G A_L$, ahol $N_{L|K} A_L$ az egység normájú elemek, $I_G A_L$ pedig az $a^{\sigma-1}$ alakú elemek által generált részcsoport.

Így a Hilbert 90-es tételt a következő axiómával tudjuk helyettesíteni tetszőleges ρ leképzésre:

Axióma $H^{-1}(G(L \mid K), A_L) = 1$ minden ciklikus bővítésre.

Ezt az $a^\rho = a^p - a$ leképzés esetében a normál bázis tétel[5] segítségével lehet visszavezetni egy egyszerű mátrixokról szóló állításra. Így alkalmazhatók rá az előző tételek általánosításai.

3. Tétel. *Legyen L egy n exponensű (nem feltétlenül véges) Abel-bővítése K-nak. Ekkor $\Delta = (A_L)^\rho \cap A_K$ mellett $L = K(\rho^{-1}(\Delta)$. Továbbá ha L ciklikus, akkor létezik olyan $a \in A_K$ elem, hogy $L = K(\rho^{-1}(a))$.*

4. Tétel. *A $\Delta \to K(\rho^{-1}(\Delta)$ és az $L \to (A_L)^\rho \cap A_K$ leképzések egymás inverzei, és K n exponensű Abel-bővítéseit megfeleltetik A_K azon részcsoportjaival, amik tartalmazzák A_K^ρ-t, és Δ / A_K^ρ izomorf lesz $Hom(G(L \mid K, \mu_\rho))$-el a következő módon: minden $a \in \Delta$ definiál egy $G(L \mid K) \to \mu_\rho$ leképzést a $(\rho^{-1}(a))^{\sigma-1}$ képlettel. (Végtelen bővítésnél Hom csak a folytonos leképzéseket jelöli.)*

3. fejezet

Az osztálytestelmélet tételei, klasszikus megfogalmazás

3.1. Állítások

A következőkben egy számtest K prímjei alatt, annak ekvivalens értékeléseinek ekvivalencia osztályait értjük, vagyis a véges prímeket amik $\mathcal{O}_K$ prímideáljainak felelnek meg és a végtelen prímeket, amik $K \to \mathbb{C}$ beágyazások konjugált párjainak felelnek meg. Egy prím valós ha ez a beágyazás csak $\mathbb{R}$-be megy, tehát a konjugált pár csak egy beágyazásra vonatkozik.

Most legyen $K \subset L$ számtestek egy bővítése, és legyen $\mathfrak{p}$ K egy véges prímje ami nem ágazik el. Ekkor ha adott egy $\mathcal{P}$ prím $\mathfrak{p}$ felett, akkor $\mathcal{P}$ felbontási részcsoportja $D_{\mathcal{P}}$ izomorf lesz a megfelelő hányadostestek Galois csoportjával, speciálisan ciklikus csoport lesz melynek a generáló elemét, a Frobenius automorfizmust vissza tudjuk húzni $D_{\mathcal{P}}$-be. Továbbá az is látható, hogy a $\mathfrak{p}$ feletti többi prímre visszahúzott elem a $\mathcal{P}$-hez tartozó konjugáltjai lesznek, így minden $\mathfrak{p}$-hez hozzá tudjuk rendelni $Gal(L|K)$ egy konjugált osztályát. Ezt az osztályt, vagy az ábeli esetben az egyetlen elemét $\mathfrak{p}$ Artin szimbólumának hívjuk és $(\mathfrak{p}, L|K)$-val jelöljük.

Az Artin leképzés fontosságát a következő tétel sugallja:

5. Tétel. *Minden K számtestre létezik egy L számtest ami K legnagyobb Abel bővítése melyben egyetlen véges prím sem ágazik el és K egyetlen valós beágyazása sem terjed ki L komplex beágyazásává. Erre a bővítésre igaz, hogy az Artin leképzés egy izomorfizmust ad K ideálosztály-csoportja és a bővítés Galois csoportja közt. Ezt a testet hívjuk K Hilbert osztálytestének.*

Ebből kiindulva azt mondjuk, hogy egy végtelen prím elágazik, ha valós és van komplex kiterjesztése L-re. Tehát ha megtaláljuk egy számtest Hilbert osztálytestét akkor megtaláltuk az összes elágazásmentes Abel bővítését is.

Felmerül a kérdés, hogy ezt hogy lehet általánosítani nem elágazásmentes Abel bővítésekre is. Az Artin leképzés nyilván nem tud izomorfizmust adni, hiszen az elágazó prímeken nincs is definiálva. Erre az úgynevezett Artin reciprocitástétel ad választ amit Emil Artin, osztrák matematikus sejtette meg először és észrevette, hogy az összes addig ismert reciprocitástörvényt, azaz a kvadratikus reciprocitástétel magasabb kitevőre való általánosításait, le tudta vezetni ebből az egy állításból. Innen ered a tétel neve. Mattuck elmondása szerint[6] ez a sejtés annyira meglepő volt, hogy amikor Artin megemlítette más matematikusoknak, például Hasse-nek, csak kinevették.

A fenti tétel $\mathbb{Q}$ esetében nem mond túl sokat, hiszen Minkowski egy tétele alapján tudjuk, hogy $\mathbb{Q}$-nak nincsenek elágazásmentes bővítései és az ideálosztály-csoportja is triviális. Viszont ebben az esetben a Kronecker-Weber tétel alapján az Abel-bővítések a körosztási testek résztestei és az n-edik körosztási test Galois-csoportja izomorf $(\mathbb{Z}/n\mathbb{Z})^\times$-vel. Weber sejtése volt, hogy minden számtesthez tartoznak hasonló, nevezetes Abel-bővítések, amik tartalmazzák az összes többi Abel-bővítést, továbbá észrevette, hogy az ideálosztály-csoport és $(\mathbb{Z}/n\mathbb{Z})^\times$ tekinthetők ugyanannak a fogalomnak különböző eseteiként. Valamint ez a definíció a fenti problémánkat is megfogja oldani az elágazó prímekkel!

Tekintsük tehát azokat a prímideálokat $\mathcal{O}_K$ -ban amik relatív prímek bizonyos előírt prímekhez. Továbbá a végtelen prímek miatt érdemes bevezetni az úgy nevezett modulusokat amik a prímek formális szorzatai, amiben a véges prímek nem negatív a végtelen valós prímek pedig nulla vagy egy, a komplexek pedig mindig nulla kitevővel szerepelnek. Ekkor minden modulus felírható $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ alakban a véges és végtelen osztói szorzataként.

2. Definíció. Jelölje $I^{\mathfrak{m}}$ a törtideálok azon halmazát, melyeket az $\mathfrak{m}_0$-t nem osztó prímek generálnak, $K^{\mathfrak{m}}$ pedig K azon elemeit melyek relatív prímek $\mathfrak{m}$ véges osztóihoz. Továbbá legyen $K_{\mathfrak{m},1}$ azon $a \in K$-k halmaza melyekre $ord_{\mathfrak{p}}(a-1)$ nagyobb vagy egyenlő mint $\mathfrak{p}$ kitevője $\mathfrak{m}$-ben annak minden véges osztójára és a képe > 0 minden $\mathfrak{m}$-et osztó valós prím alatt.

Könnyen belátható a kínai maradéktétel segítségével, hogy az osztálycsoport

$C \cong I^{\mathfrak{m}}/K^{\mathfrak{m}}$, tehát ha az L-ben elágazó prímek osztják a modulust akkor így az Artin szimbólum nem definiáltsága ezeken a prímeken már nem jelent problémát. A fenti tétel általánosításához viszont a következő csoportra lesz szükségünk.

3. Definíció. Legyen $i : K \to I$ az a leképzés ami az elemeket a megfelelő főideálokhoz küldi, ekkor $C_{\mathfrak{m}} = I^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$ az $\mathfrak{m}$-hez tartozó sugárosztálycsoport.

Adott K esetén a sugárosztálycsoport meghatározásában nagyon hasznos a következő tétel:

6. Tétel.

$$1 \to U/U_{\mathfrak{m},1} \to K^{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to C \to 1$$

egy egzakt sorozat, ahol U az $\mathcal{O}_K$ egységeit, $U_{\mathfrak{m},1}$ pedig azok megfelelő részhalmazát jelölik. Továbbá

$$K^{\mathfrak{m}}/K_{\mathfrak{m},1} \cong \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \{\pm 1\} \times (\mathcal{O}/\mathfrak{m}_0)^*.$$

Bizonyítás. Alkalmazzuk a kernel-cokernel lemmát a $K_{\mathfrak{m},1} \xrightarrow{f} K^{\mathfrak{m}} \xrightarrow{g} I^{\mathfrak{m}}$ sorozatra! Mivel $\ker f = 1, \ker g \circ f = U_{\mathfrak{m},1}, \ker g = U, \operatorname{coker} f = K^{\mathfrak{m}}/K_{\mathfrak{m},1}, \operatorname{coker} g \circ f = C_{\mathfrak{m}}$ és $\operatorname{coker} g = I^{\mathfrak{m}}/K^{\mathfrak{m}} \cong C$, ezért azt kapjuk, hogy

$$1 \to U_{\mathfrak{m},1} \to U \to K^{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to C \to 1$$

egzakt.

A $K^{\mathfrak{m}} \to \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \{\pm 1\} \times (\mathcal{O}/\mathfrak{m}_0)^*$ leképzés pedig szürjektív a megközelítési tétel miatt és magja $K_{\mathfrak{m},1}$. □

Az osztálytestelmélet egyik fő tétele arról szól, hogy a különböző Artin szimbólumú prímek hogy oszlanak el aszimptotikusan. Mivel ezt az aszimptotikusságot algebrailag nem tudjuk értelmezni ezért szükségünk lesz a következő analitikus definícióra:

4. Definíció. Legyen K egy számtest. Azt mondjuk, hogy egy prímeket tartalmazó T halmaznak δ sűrűsége van ha

$$\sum_{\mathfrak{p} \in T} 1/N(\mathfrak{p})^s \sim \delta log(1/(s-1))$$

ahol $s \to 1$ jobbról és N az ideál normája.

Most már készen állunk arra, hogy kimondjuk az osztálytestelmélet főbb tételeit:

7. Tétel. ***Reciprocitástétel*** *Legyen L egy Abel-bővítése K-nak, ekkor létezik egy olyan modulus $\mathfrak{m}$ amelyben az L-ben elágazó prímek szerepelnek nem nulla kitevővel és az Artin leképzés egy izomorfizmust ad:*

$$I_K^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) \cdot N(I_L^{\mathfrak{m}}) \cong G(L|K).$$

$I_K^{\mathfrak{m}}$ egy részcsoportjáról azt mondjuk, hogy kongruencia csoport modulo $\mathfrak{m}$ ha tartalmazza $i(K_{\mathfrak{m},1})$-et.

8. Tétel. ***Létezéstétel*** *Minden H kongruencia csoportra létezik egy L véges Abel bővítése K-nak és egy modulus, aminek osztói az L-ben elágazó prímek és melyre $H = i(K_{\mathfrak{m},1}) \cdot N(I_L^{\mathfrak{m}})$, speciálisan minden modulusra létezik egy sugárosztálytest, melynek Galois csoportjába az Artin leképzés egy izomorfizmust ad $C_{\mathfrak{m}}$-ből.*

$K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ fenti karakterizációjából és az egzakt sorozat természetességéből látszik, hogy léteznie kell egy minimális modulusnak, melyen átfaktorizálódik az Artin leképzés és az egzakt sorozatban lévő leképzés kompozíciója, ezt a modulust a bővítés konduktorának hívjuk.

A reciprocitástétel és a létezéstételektől valamelyest különálló harmadik főtétel Dirichlet egyik tételét általánosítja, mely azt mondja ki, hogy a prímek "egyenletesen oszlanak el a különböző kongruenciaosztályokba." Valóban a másik két tételt be lehet bizonyítani majdnem teljesen algebraian, de következő tétel bizonyításában nagy szerepet játszik az analízis:

9. Tétel. ***Chebotarev-sűrűségtétel*** *Legyen $L|K$ számtestek egy Galois bővítése (nem feltétlenül ábeli) és legyen C $Gal(L|K)$ egy konjugált osztálya, ekkor a prímek sűrűsége melyekre $(\mathfrak{p}, L|K) = C$, $|C|/|Gal(L|K)|$ lesz.*

Ebből ki lehet hozni, hogy egy számtest akkor és csak akkor tartalmazza a másikat, ha a benne felbomló prímek halmazát tartalmazza a másikban felbomló prímek halmaza esetlég véges kivételekkel. Ez már önmagában is egy nagyon erős technika annak bizonyítására, hogy különböző számtestek egymást tartalmazzák, viszont ezen felül még azt is ki lehet hozni ebből, hogy K egy Abel bővítése akkor és csak akkor része az $\mathfrak{m}$-hez tartozó sugárosztálytestnek, ha konduktora osztja $\mathfrak{m}$-et. Ennek következménye egyrészt az, hogy a sugártesteket egyértelműen meghatározzák a modulusok, és az alábbi tétel, aminek bizonyítása gyakorlatilag ugyan az mint a lokális megfelelőjének, így ezt kihagyjuk.

10. Tétel. *Egy $\mathfrak{m}$ modulushoz tartozó $L_\mathfrak{m}$ sugártest résztestei és $C_\mathfrak{m}$ részcsoportjai közt a norma leképzés egy tartalmazás megfordító bijekció.*

3.2. Néhány alkalmazás

Most megnézzük, hogy ezeket a tételeket hogy lehet alkalmazni néhány érdekes következményen keresztül.

11. Tétel. ***Kronecker-Weber*** *$\mathbb{Q}$ minden véges Abel-bővítését tartalmazza valamely körosztási test.*

Bizonyítás. Jelölje ∞ a racionális számok egyetlen beágyazását $\mathbb{C}$-be. Elég bebizonyítanunk, hogy minden $4 \mid n$, vagy $2 \nmid n$ természetes számra az $\mathfrak{m} = n\infty$ konduktor sugárosztályteste egy körosztási test, hiszen bármely adott konduktor oszt egy ilyet. Ez a feltétel azért szükséges, mert ekkor $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$-ben pontosan az $\mathfrak{m}$-et osztó prímek ágaznak el. Most leírjuk az Artin leképzést $I^\mathfrak{m}$-en, ami az n-t nem osztó racionális prímek által generált szabad csoport. Legyen $p \nmid n$, ekkor a $(p, \mathbb{Q}(\zeta_n) \mid \mathbb{Q}) \in G(\mathbb{Q}(\zeta_n) \mid \mathbb{Q}) : \zeta_n \to \zeta_n^p$ automorfizmus eleget tesz az Artin leképzés definíciójának. Valóban, legyen $\mathfrak{p}$ egy prím p felett, ekkor, mivel ζ_n^i egy egész bázisa $\mathcal{O}$-nak, ezért

$$(p, \mathbb{Q}(\zeta_n) \mid \mathbb{Q})(\Sigma c_i \zeta_n^i) = \Sigma c_i \zeta_n^{p \cdot i} \equiv (\Sigma c_i \zeta_n^i)^p \pmod{\mathcal{O}/\mathfrak{p}}.$$

Tehát az Artin leképzés egy szürjektív homomorfizmus $G(\mathbb{Q}(\zeta_n) \mid \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$-be, aminek magja pont $K_{\mathfrak{m},1}$ vagyis $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$ az $\mathfrak{m}$-hez tartozó sugárosztálytest. □

Fontos megjegyezni, hogy az osztálytestelmélet tételeinek bizonyítása nem épít a Kronecker-Weber-tételre, így ez nem körkörös érvelés.

Ha $p \in \mathbb{Z}$ egy páratlan prím, akkor $\mathbb{Q}(\zeta_p)$ Galois-csoportja egy $p-1$ rendű ciklikus csoport lesz és így lesz egy egyedi 2 indexű részcsoportja, vagyis $\mathbb{Q}(\zeta_p)$-nek pontosan egy 2 fokú részbővítése van. Ugyan ezt a résztestet elemibb módszerekkel is meglehet határozni, a következő állítás a konduktorok használatát demonstrálja:

12. Tétel. *Leqyen $p^* = \pm p$ úgy megválasztva, hogy $p* \equiv 1$ modulo 4, ekkor $\mathbb{Q}(\zeta_p)$ kvadratikus részteste $\mathbb{Q}(\sqrt{p^*})$.*

Bizonyítás. Mivel $\mathbb{Q}(\zeta_p)$ konduktora $p\infty$, ezért az egyetlen véges prím ami elágazhat résztesteiben, az a p, de $\mathbb{Q}(\sqrt{d})$ diszkriminánsa d vagy $4d$ attól függően, hogy $d \equiv 1$

(mod 4)-e vagy nem, amit mindig osztani fog egy p-től különböző prím, kivéve ha $d = p^*$. □

Mint ahogy a fejezet elején említettem, Artin megmutatta, hogy a reciprocitástételből hogyan következnek az addig ismert reciprocitástételek. Ezt legkönnyebben a Hilbert szimbólum bevezetésével lehet látni, de ehhez szükségünk lenne némi lokális osztálytestelméletre. Viszont a kvadratikus reciprocitást le lehet vezetni a Hilbert szimbólum nélkül is amit most bemutatok.

13. Tétel. ***Kvadratikus reciprocitás****[7] Legyenek p és q páratlan pozitív prímek, ekkor*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Bizonyítás. Legyen $p^* = (-1)^{\frac{p-1}{2}} \equiv 1$ modulo 4. Az állítás ekvivalens a

$$\left(\frac{p}{q}\right) = \left(\frac{p*}{q}\right)$$

egyenlettel, és mivel $(\mathbb{Z}/p\mathbb{Z})^\times$ ciklikus csoport, ezért egyetlen 2 indexű részcsoportja van, tehát csak egy homomorfizmus létezik belőle a kételemű csoportba, tehát elég belátni, hogy a $q \to \left(\frac{p*}{q}\right)$ leképzés egy homomorfizmust definiál $(\mathbb{Z}/p\mathbb{Z})^\times$-én. A fentiekben láttuk, hogy $\mathbb{Q}(\sqrt{p^*})$ konduktora osztja $p\infty$-t tehát Az Artin leképzés egy homomorfizmust definiál $(\mathbb{Z}/p\mathbb{Z})^\times$-én. Továbbá legyen $\mathfrak{q}$ egy q feletti prím, ekkor

$$(q, \mathbb{Q}(\sqrt{p^*}) \mid \mathbb{Q})\sqrt{p^*} \equiv \sqrt{p^*}^{N(\mathfrak{q})} \equiv \left(\frac{p*}{q}\right)\sqrt{p^*} \pmod{\mathfrak{q}}.$$

No de $\sqrt{p^*}$ konjugáltja csak $\pm\sqrt{p^*}$ lehet és $1 \neq -1 \pmod q$, szóval az egyenlet $\mathbb{Q}(\sqrt{p^*})$-ban is fennáll, vagyis $\left(\frac{p*}{q}\right)$ valóban művelettartó. □

A következő példa egy jóval bonyolultabb kérdés, aminek legtöbb részesetét szintén azonnal meg tudjuk oldani az osztálytestelmélet segítségével. Fermat egyik tétele alapján egy prím akkor és csak akkor írható fel két egész szám négyzeteként, ha $p \equiv 1 \pmod 4$. Észrevehetjük, hogy $a^2 + b^2$ pont $a + b \cdot i$ normája a $\mathbb{Q}(i)$ testben, így felmerül a kérdés, hogy mi történik más kvadratikus testekben, vagy egy kicsit általánosabban: mely prímekre oldható meg a $p = a^2 + n \cdot b^2$ egyenlet?

Ha n négyzetmentes és $\not\equiv -1 \pmod 4$, azaz amikor $\mathbb{Q}(\sqrt{-n})$ egészeinek gyűrűje $\mathbb{Z}[\sqrt{n}]$, akkor az, hogy p felbomlik-e vagy sem, csak $\left(\frac{n}{p}\right)$-tól, tehát n kongruenciaosztályától függ modulo p. Ha emellett $\mathbb{Z}[\sqrt{-n}]$ főideálgyűrű, akkor ez pontosan azt

jelenti, hogy létezik egy p normájú elem. Tehát az egyenlet megoldhatósága csak $\left(\frac{n}{p}\right)$-tól függ. Amennyiben $\mathbb{Z}[\sqrt{-n}]$ nem főideálgyűrű, a Hilbert-osztálytest létezését kihasználva tudjuk bizonyítani a következőt:

14. Tétel. *Legyen n négyzetmentes és $\not\equiv 1 \pmod 4$ és $h(n)$ jelölje $\mathbb{Q}(\sqrt{-n})$ ideálosztály-csoportjának számosságát. Ebben az esetben létezik egy $h(n)$ fokú $f(x)$ polinom, $\mathbb{Q}(\sqrt{-n})$ Hilbert-osztálytestének minimálpolinoma, úgy hogy a $p = a^2+n\cdot b^2$ egyenlet akkor és csak akkor oldható meg, ha $\left(\frac{n}{p}\right) = 1$ és $f(x) \pmod p$ lineáris faktorokra bomlik.[7]*

Bizonyítás. Először is vegyük észre, hogy egy tetszőleges K számtestben egy prímideál akkor és csak akkor főideál ha K Hilbert-testében teljesen felbomlik, hiszen ezek ekvivalensek azzal, hogy a Hilbert-testhez tartozó Artin leképzés magjában van a prímideál. A mi esetünkben $p = a^2 + n \cdot b^2$ akkor és csak akkor ha felbomlik két főideál szorzatára $\mathbb{Q}(\sqrt{-n})$-ban, $(p) = \pi \cdot \bar{\pi}$, ami akkor és csak akkor történik meg ha $\left(\frac{n}{p}\right) = 1$ és $(\pi, H \mid \mathbb{Q}(\sqrt{-n})) = 1$, ahol H a $\mathbb{Q}(\sqrt{-n})$ Hilbert-teste, ami ekvivalens azzal, hogy $\left(\frac{n}{p}\right) = 1$ és H minimálpolinomja lineáris faktorokra bomlik $\mathbb{Z}[\sqrt{-n}]/\pi\mathbb{Z}[\sqrt{-n}] \cong \mathbb{Z}/p\mathbb{Z}$ felett. □

Amennyiben $\mathbb{Z}[\sqrt{-n}]$ nem a teljes egészek gyűrűje, akkor is igazolható egy kongruencia csoport, és a megfelelő Abel bővítés segítségével egy hasonló tétel.

4. fejezet

Az osztálytestelmélet tételei, modern megfogalmazás

4.1. Lokális osztálytestelmélet

Az osztálytestelmélet nem csak számtestekre alkalmazható, hanem lokális testekre, azaz $\mathbb{Q}_p$ vagy $\mathbb{F}_p(t)$ véges bővítéseire is. Ebben az esetben a reciprocitás és a létezéstétel valamivel egyszerűbb és egységesebb formát öltenek: itt nem kell külön modulusokat rögzíteni minden alkalommal amikor használni akarjuk a tételeket, hanem létezik egyetlen egy Artin leképzés a maximális Abel-bővítés Galois-csoportjába, melynek megszorítása véges elágazásmentes bővítésekre megadja a globális Artin leképzés egy megfelelőjét.

Pontosabban legyen K egy lokális test és legyen $L \mid K$ egy véges elágazásmentes bővítés. Először is, egy lokális test egészeinek gyűrűjében csak egy prímideál van és ez is főideál, ezért nem is remélhetjük, hogy az Artin leképzés egy izomorfizmust adna az ideálosztály-csoport és a Galois-csoport közt, mert az előbbi mindig triviális. Ezért a homomorfizmust $K^\times$-n definiáljuk a következőképpen: mivel egy elágazásmentes bővítés lényegében a hányadostest bővítése, azaz mindig Galois, ciklikus csoporttal, ami kanonikusan izomorf valamely véges test feletti bővítés Galois-csoportjával, ezért vissza tudjuk húzni annak generátorát, a Frobenius automorfizmust, amit $Frob_{L|K}$-val fogunk jelölni. Most definiáljuk, hogy bármely π prímelemre legyen $\phi_{L|K}(\pi) = Frob_{L|K}$, tehát minden egység elemre az identitás, mert azok mind felírhatók különböző prímek hányadosaiként, így valóban egy homomorfizmust definiáltunk egész $K^\times$-n.

15. Tétel. ***Lokális reciprocitástétel*** *Minden K lokális testre létezik egy $\phi_K : K^\times \to G(K^{ab} \mid K)$, ami minden L véges elágazásmentes bővítésre megszorítva $\phi_{L|K}$-ával egyenlő. Továbbá $\phi_{L|K}$ átfaktorizálódik $N_{L|K}(L^\times)$-en és így meghatároz egy*

$$K^\times / N_{L|K}(L^\times) \cong G(L \mid K)$$

izomorfizmust.

Igazolható a következő állítás:

16. Tétel. *Minden véges $L \mid K$ Abel-bővítésre $N_{L|K}(L^\times)$ egy véges indexű nyílt részcsoportja $K^\times$-nak.*

Bizonyítás. $N_{L|K} : L \to K$ folytonos, hiszen az automorfizmusok és a szorzás is az, így $N_{L|K}(U_L)$ egy zárt halmaz lesz hiszen a kompakt U_L csoport képe. Továbbá a valuáció lehetséges értékeit megvizsgálva azt kapjuk, hogy $N_{L|K}(U_L) = N_{L|K}(L) \cap U_K$, tehát

$$U_K / N_{L|K}(U_L) \cong U_K / N_{L|K}(L) \cap U_K \cong U_K N_{L|K}(L) / N_{L|K}(L) \leq K^\times / N_{L|K}(L),$$

ami véges a reciprocitástétel miatt, vagyis $N_{L|K}(U_L)$ egyben nyílt részhalmaza is az U_K nyílt részcsoportnak, és így $K^\times$-nak is. (Itt azt használtuk, hogy egy véges indexű részcsoport egy topológiai csoportban akkor és csak akkor nyílt, ha zárt is.) Szóval $N_{L|K}(L)$ tartalmaz egy nyílt részcsoportot és így maga is nyílt. □

Az állítás megfordítottja is igaz, de sokkal nehezebb igazolni.

17. Tétel. ***Lokális létezéstétel*** *Minden $H \subset K^\times$ véges indexű nyílt részcsoporthoz létezik olyan $L \mid K$ véges Abel-bővítés, hogy $N_{L|K}(L^\times) = H$.*

Vegyük észre, hogy ez feltétel hasonlít a globális verziónak azon feltételéhez, ahol megköveteljük, hogy a kongruencia csoportok tartalmazzák $i(K_{\mathfrak{m},1})$-et valamely modulusra. Később látni fogjuk, hogy ez nem véletlen, hanem bizonyos értelemben itt is valamilyen topológia rejlik a háttérben.

Ezen felül az is igaz, hogy az Abel-bővítések normái egyértelműen meghatározzák őket.

18. Tétel. *A norma leképzés egy tartalmazás megfordító bijekciót ad K véges Abel-bővítései, és véges indexű multiplikatív részcsoportjai közt.*

Bizonyítás. Az előző két tétel alapján elég belátni, hogy $L \subset L' \iff N(L) \supset N(L')$. Ha $L \subset L'$, akkor az $N_{L'|K} = N_{L|K} \circ N_{L'|L}$ egyenlet miatt megkapjuk az egyik implikációt, melynek egy speciális esete: $N(LL') \subset N(L) \cap N(L')$. Most a reciprocitástételt használva bebizonyítjuk, hogy itt egyenlőség áll fenn. Legyen $x \in N(L) \cap N(L')$, ez azt jelenti, hogy $\phi_K(x)$ megszorítva L-re és L'-re is az identitás, tehát a két test kompozitumán is csak az identitás lehet, vagyis $x \in N(LL')$.

Most tegyük fel, hogy $N(L) \supset N(L')$, ekkor $N(LL') = N(L')$, tehát

$$|L' : K| = |K^\times / N(L')| = |K^\times / N(LL')| = |L' : K|,$$

azaz $LL' = L'$ és $L \subset L'$. □

Felmerülhet a kérdés, hogy a reciprocitástételben szereplő homomorfizmus egyedi-e, és a válasz igen.

19. Tétel. *Ha létezik olyan ϕ_K homomorfizmus, mint a reciprocitástételben, akkor az egyértelműen meghatározott.*

Bizonyítás. Az ötlet az, hogy a prímelemek generálják a $K^\times$ csoportot, így ha ϕ_K és ϕ'_K két homomorfizmus, ami rendelkezik a reciprocitástételben említett tulajdonságokkal, akkor elég megmutatni, hogy $\phi_K(\pi) = \phi'_K(\pi)$ minden prímre.

Először is szükségünk lesz egy kicsit jobban megérteni, hogy $G(K^{ab} \mid K)$ hogy néz ki. Vegyük észre, hogy ϕ_K injektív, hiszen ha egy automorfizmus minden véges résztestre megszorítva az identitás, akkor az egész testen az identitás. ϕ_K viszont nem lesz szürjektív, de ha minden véges Abel-bővítésre a $K^\times/N(L)$ csoportok felett vesszük az inverz limeszt ezek felett, akkor az már izomorf lesz $G(K^{ab} \mid K)$-val és az is látszik, hogy ez nem más mint $K^\times$ telítése a norma-topológiában, azaz abban a topológiában, amiben az $N(L)$ részcsoportok adnak egy egységelem körüli bázist.

Mivel $K^\times = U_K \times \pi^{\mathbb{Z}}$ és a norma-topológia bázisát fel tudjuk írni $\pi^{n\mathbb{Z}} \cdot (1 + \mathfrak{m}^m)$ alakban ezért elég meghatározni U_K telítését abban a topológiában amiben $(1+\mathfrak{m}^m)$ ad egy bázist és $\mathbb{Z}$ telítését, ha a bázist az $n\mathbb{Z}$ csoportok adják. Tehát $\hat{K^\times} = U_K \times \pi^{\hat{\mathbb{Z}}}$.

A végtelen Galois-elmélet alaptételét alkalmazva szét tudjuk szedni K-át π és U_K fixtesteire, azaz $K = K_\pi \cdot K_{U_K}$, vagy ha ϕ_K helyett ϕ'_K-át használjuk, akkor $K = K'_\pi \cdot K'_{U_K}$. Legyen $K_{\pi,n}$ a $\pi^{\mathbb{Z}}(1 + \mathfrak{m}^n)$ csoporthoz tartozó test, ekkor könnyen látható, hogy $K_\pi = \bigcup_n K_{\pi,n} = K'_\pi$, és nyilván $\phi_K(\pi)$ és $\phi_K(\pi)'$ is triviálisan hat ezen a testen, tehát ha be tudjuk bizonyítani, hogy K_{U_K} a legnagyobb elágazásmentes

bővítés akkor, készen vagyunk, mert ekkor $K_{U_K} = K'_{U_K}$ és $\phi_K(\pi) = \phi_K(\pi)'$ itt is hiszen tudjuk, hogy mindkettő $Frob_{L|K}$-ként hat minden véges elágazásmentes testen.

Minden egységelem felírható két prím hányadosaként és mivel bármely két prím ugyan úgy hat minden elágazásmentes bővítésen, ezért $K_{un} \subset K_{U_K}$ Másrészt ha $L \subset K_{U_K}$ véges, akkor $N(L^\times) = \pi^{n\mathbb{Z}}U_K$ valamely n-re, de ekkor $G(L \mid K) \cong K^\times/N(L^\times) \cong \mathbb{Z}/n\mathbb{Z}$, azaz $n = |L : K|$ és így L elágazásmentes, azaz valóban $K_{un} = K_{U_K}$. □

Meg kell jegyeznem, hogy a reciprocitás és létezéstétel is igaz abban az esetben, amikor $K = \mathbb{R}$, viszont ez nem a tételek bizonyításából következik, hanem majdhogynem triviális, hiszen $\mathbb{R}$ egyetlen algebrai bővítése $\mathbb{C}$, ami egyben a maximális Abel-bővítés is, és normája $\mathbb{R}^+$ a pozitív valós számok multiplikatív csoportja, így $\mathbb{R}^\times/\mathbb{R}^+ \cong \mathbb{Z}/2\mathbb{Z} \cong G(\mathbb{C} \mid \mathbb{R})$. Továbbá az is látható, hogy nem létezik más véges indexű (nyílt) részcsoport, hiszen ha $(\mathbb{R}^\times)^m \subset H$, akkor $\mathbb{R}^+ \subset H$, mert pozitív számoknak tudjuk m-edik gyökét vonni.

4.2. Globális osztálytestelmélet

A fő tételek klasszikus megfogalmazásából és az Artin leképzés néhány alapvető tulajdonságából látszik, hogy $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}} \cong G(K^{ab} \mid K)$, azonban kiderül, hogy ha a lokális-globális elvet akarjuk használni a globális tételek bizonyításában, akkor célratörőbb egy másik csoportot vizsgálni, melynek hányadosaként előáll $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}}$. Ez lesz az úgy nevezett idéle-osztálycsoport.

Az idéle elnevezés az ideális elem, id. ele. rövidítéséből jön és egy K számtest idéle-csoportját a következőképpen definiáljuk:

5. Definíció. Legyen K egy globális számtest, v egy prímje, K_v a v-hez tartozó valuáció melletti teljessé tettje, $\mathcal{O}_v$ az egészek gyűrűje K_v-ben és U_v az egységek csoportja. ekkor K idéle-csoportja

$$\mathbb{I}_K = \{(a_v) \in \prod_v K_v^\times \mid a_v \in U_v \text{véges sok kivétellel.}\}$$

Ezt a csoportot az úgynevezett megszorított szorzattopológiával látjuk el, vagyis azzal a topológiával melyet a $\{\prod_v V_v \mid V_v$ nyílt $K_v^\times$-ban és véges sok kivétellel $= U_v\}$ bázis generál.

Látszik, hogy ez egy topológiai csoport és, hogy létezik egy szürjektív folytonos homomorfizmus $id : \mathbb{I}_K \to I_K$,

$$(a_v) \to \prod_{v \text{ véges}} p_v^{ord_v(a_v)},$$

ahol I_K-át a diszkrét topológiával látjuk el.

Intuitívan, ez azért jó nekünk, mert valamilyen topológiát akarunk értelmezni I_K-n, de mivel ez egy direkt összeg megszámlálhatóan sok $\mathbb{Z}$ felett ezért maga is megszámlálható, így túl sok értelmes topológiát nem tudunk rárakni a diszkrét topológián kívül, ami nem ad túl sok információt, ezért az ideálokat "kibővítjük" az egységelemekkel és a végtelen prímekkel, így bizonyos értelemben meg tudjuk örökölni a K_v-ékből. Valóban, láthatjuk, hogy minden olyan S halmazra, ami véges sok véges prímet tartalmaz a végtelen prímek mellett, az

$$U(S, \epsilon) = \{(a_v) \mid \|a_v - 1\|_v < \epsilon \forall v \in S, a_v \in U_v \forall v \notin S\}$$

halmazok 1 egy bázisát adják és itt már kezd látszani a hasonlóság $K_{\mathfrak{m},1}$-el.

6. Definíció. Most definiáljuk a főideálok idéle megfelelőit egy $i : K^\times \to \mathbb{I}_K$ homomorfizmussal: $i(a) = (a, a, a, ...)$ Az idéle-osztálycsoport a

$$\mathbf{C}_K := \mathbb{I}_K / i(K)$$

faktorcsoport a hányados topológiával.

Míg $\mathbb{I}_K$-n a topológia elég mesterségesnek tűnhet, $\mathbf{C}_K$-n már közel sem triviális a helyzet. Például I_K-ból $\mathfrak{p}_v$-ét bizonyos prímelemek megválasztása után vissza tudjuk húzni $\mathbb{I}_K$-be az $(1, 1, ...\pi_v, 1, ...)$ idéle formájában, tehát lényegében csak I_K és $\prod_v U_v$ direkt szorzata. C_K-ból $\mathbf{C}_K$-ba viszont ezt nem tudjuk megcsinálni, például ha $K = \mathbb{Q}(\sqrt{-5})$, akkor $C_K \cong \mathbb{Z}/2\mathbb{Z}$ a 2 feletti ideál által generálva, viszont az $(1, 1 + \sqrt{-5}, 1, 1, ...)$ által generált csoport nem $\mathbb{Z}/2\mathbb{Z}$ lesz $\mathbf{C}_K$-ban.

Azt már láttuk, hogy C_K hogy áll elő $\mathbb{I}_K$ hányadosaként, és most valami hasonlót szeretnénk belátni $C_\mathfrak{m}$-ről is.

7. Definíció. Legyen

$$W_\mathfrak{m}(\mathfrak{p}) = \begin{cases} \mathbb{R}^+ & \mathfrak{p} \text{ valós}, \\ U_\mathfrak{p}^{(\mathfrak{m}(\mathfrak{p}))} & \mathfrak{p} \text{ véges} \end{cases}$$

és legyen

$$\mathbb{I}_{\mathfrak{m}} = \mathbb{I} \cap (\prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) \times \prod_{\mathfrak{p}\not|\mathfrak{m}} K_{\mathfrak{p}}^{\times})$$

valamint

$$W_{\mathfrak{m}} = \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) \times \prod_{\mathfrak{p}\not|\mathfrak{m}\text{végtelen}} K_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p}\not|\mathfrak{m}\text{véges}} U_{\mathfrak{p}}$$

A fenti definíció raison d'etre-ja a következő:

20. Tétel. *Az id leképzés $\mathbb{I}_{\mathfrak{m}}$-re megszorítva egy izomorfizmust ad*

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \cdot W_{\mathfrak{m}} \cong C_{\mathfrak{m}}.$$

Hasonlóan az inklúzió is egy izomorfizmust indukál

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong \mathbb{I}/K^{\times}.$$

Bizonyítás. Egyértelműen $K_{\mathfrak{m},1} \subset \ker id$ és $W_{\mathfrak{m}} \subset \ker id$ tehát $K_{\mathfrak{m},1} \cdot W_{\mathfrak{m}} \subset \ker id$. A másik irányban, ha egy adott (a_v) idelére és $b \in K_{\mathfrak{m},1}$-re $id((a_v)) = id(b)$, akkor $id(b^{-1}(a_v)) = 1$, azaz $b^{-1}(a_v) \in W_{\mathfrak{m}}$.

A következő állítás belátásához bármilyen $(a_v) \in \mathbb{I}$-hez találnunk kell egy $b \in K^{\times}$-t, amire $b^{-1}(a_v) \in \mathbb{I}_{\mathfrak{m}}$. Ezt az approximációs tétel segítségével megtehetjük úgy, hogy a véges sok $v \mid \mathfrak{m}$ helyen b-t megfelelően közel választjuk a_v-hez, így az indukált leképzés szürjektív és mivel $\mathbb{I}_{\mathfrak{m}} \cap K = K_{\mathfrak{m},1}$, ezért egy izomorfizmus is. □

A $\mathbf{C}_K$-n definiált topológia fontosságát mutatja, hogy bármely $\psi : C_{\mathfrak{m}} \to G$ egyértelműen terjeszthető ki egy folytonos leképzésre.

21. Tétel. *Legyen G egy véges csoport a diszkrét topológiával. Bármely $\psi : C_{\mathfrak{m}} \to G$ csoporthomomorfizmus egyértelműen meghatárot egy $\phi : \mathbb{I} \to G$ folytonos homomorfizmust, amire $\phi(K^{\times}) = 1$ és $\phi((a_v)) = \psi(id(a_v))$ minden olyan idélére, amire ami $(a_v) \in \mathbb{I}^S(\mathfrak{m}) = \{(a_v) \mid v \mid \mathfrak{m} \implies a_v = 1\}$ és minden folytonos leképzés, amire $\phi(K^{\times}) = 1$, előállítható egy ilyen ψ-ből.*

Bizonyítás. Tekintsük a következő diagramot:

$$\mathbb{I} \longrightarrow \mathbb{I}/K \xleftarrow{\cong} \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \longrightarrow \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \cdot W_{\mathfrak{m}} \xrightarrow{\cong} C_{\mathfrak{m}} \xrightarrow{\psi} G$$

Egyértelmű, hogy ψ-t vissza tudjuk húzni egy homomorfizmusra, aminek a magja tartalmazni fogja a $W_{\mathfrak{m}}$ nyílt halmazt, és mivel a mag egy részcsoport ezért nyílt lesz, azaz ϕ folytonos.

Az egyértelműséghez elég bebizonyítani, hogy $K^\times \cdot \mathbb{I}^S(\mathfrak{m})$ sűrű. Ehhez elég lenne találnunk egy olyan K-beli elemet, ami tetszőlegesen közel lehet hozni egy adott idéléhez az $\mathfrak{m}$-et osztó koordinátákban, no de ezt meg tudjuk tenni az approximációs tétel használatával.

Az utolsó állításhoz pedig tekintsük újra a fenti diagramot. Ha ϕ folytonos, akkor magja nyílt, mert G diszkrét, azaz tartalmaznia kell $W_\mathfrak{m}$-et valamilyen $\mathfrak{m}$-re. Így az $\mathbb{I}_\mathfrak{m} \rightarrowtail \mathbb{I}$ inklúzióból kapott izomorfizmus segítségével kapunk egy homomorfizmust $\mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1} \cdot W_\mathfrak{m}$-en, ami nem más mint $C_\mathfrak{m}$.

□

A $K^\times$ csoport megfelelője a globális esetben $\mathbf{C}_K$ lesz, ezért az idéléken is definiálnunk kell egy normát.

8. Definíció. Legyen $L \mid K$ egy véges bővítés és v egy prímje K-nak, w pedig L egy prímje. Ekkor az $N_{L|K} : \mathbb{I}_L \to \mathbb{I}_L$ leképzést a következőképpen definiáljuk. Ha $(a_w) \in \mathbb{I}_L$, akkor $(N_{L|K}(a))_v = \prod_{w|v} N_{L_w|K_v}(a_w)$. Látszik, hogy az $N_{L|K}(a) = \prod_{w|v} N_{L_w|K_v}(a)$ identitás miatt ez $i(L^\times)$-re megszorítva lényegében a megszokott norma, és hogy így a $\mathbf{C}_L \to \mathbf{C}_K$ faktorcsoportokon is kapunk egy $N_{L|K}$ leképzést.

Az Artin leképzés definiálásához vegyük észre, hogy a lokális osztálytestelmélet minden $w \mid v$-re szolgáltat egy $\phi_v : K_v^\times \to G(L_w \mid K_v) \cong D_w \subset G(L \mid K)$ homomorfizmust, ami független lesz w-től mert minden különböző w-re a leképzés eleget tesz az lokális Artin leképzést definiáló feltételeknek és láttuk, hogy ez egyértelműen meghatározza a függvényt.

22. Tétel. *Létezik egy egyértelműen meghatározott folytonos $\phi_K : \mathbb{I}_K \to G(K^{ab} \mid K)$ ami minden L véges Abel-bővítésre kommutatívvá teszi a következő diagramot:*

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & G(L_w \mid K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{a \to \phi_K(a)|_L} & G(L \mid K) \end{array}$$

Bizonyítás. Legyen $a = (a_v)$ egy tetszőleges idéle. Már láttuk, hogy lokális testek egy $L_w \mid K_v$ bővítése akkor és csak akkor elágazásmentes, ha $\phi_v(U_K)$ rögzíti és mivel csak véges sok v ágazik el és véges sok a_v nem egységelem, ezért $\phi_v(a_v)$ véges sok kivétellel triviális lesz L_w-re megszorítva. Azaz tudjuk értelmezni a $\phi_{L|K}(a) := \Pi_v \phi_v(a_v)$ szorzatot $G(L \mid K)$-ban, amiről látszik hogy csak ez lehet $\phi_K(a) \mid_L$ értéke.

Ha L' egy másik Abel-bővítése K-nak, akkor $\phi_{L|K} \mid_{L\cap L'} = \phi_{L'|K} \mid_{L\cap L'}$, hiszen ez igaz a $\phi_v \mid_{L_w}$- ékre, tehát a $\phi_{L|K}$-ák a maximális Abel-bővítésen is meghatároznak egy $\phi_K(a)$ automorfizmust. Ahhoz, hogy belássuk, hogy ϕ_K folytonos, tekintsük azt az egységelem körüli bázist, amit a $\{\sigma \mid \sigma \mid_L = 1\}$ halmazok alkotnak az összes véges L Abel-bővítésre. Elég megmutatni, hogy ezeknek az inverz képei nyíltak $\mathbb{I}_K$-ban. No de egy adott L-re csak véges sok v ágaik el, tehát a $V = \Pi_{v \text{ nem ágazik el}} U_v \times \Pi_{v \text{ elágazik}} \ker \phi_v \mid_{L_w}$ az egységelem egy nyílt környezete lesz a magban, ami így nyílt. □

23. Tétel. ***Globális reciprocitástétel*** *A ϕ_K homomorfizmus átfaktorizálódik $\mathbf{C}_K$-n és minden $L \mid K$ véges Abel-bővítésre egy izomorfizmust definiál:*

$$\phi_{L|K} : \mathbf{C}_K / N_{L|K}(\mathbf{C}_L) \to G(L \mid K)$$

24. Tétel. ***Globális létezéstétel*** *Minden $H \subset \mathbf{C}_K$ véges indexű nyílt részcsoportra létezik egy $L \mid K$ véges Abel-bővítés, melyre $H = N_{L|K}(\mathbf{C}_L)$.*

Mint ahogy azt elvárnánk ezek a tételek erősebbek, mint a klasszikus megfogalmazásuk.

25. Tétel. *A globális reciprocitás- és létezéstételekből következnek a klasszikus reciprocitás- és létezéstételek.*

Bizonyítás. Kezdjük a reciprocitástétellel. Legyen $L \mid K$ egy véges Abel-bővítés. Mivel ϕ_K folytonos és $\phi_K(K^\times) = 1$, ezért létezik egy $\mathfrak{m}$ és $\psi : C_\mathfrak{m} \to G(L \mid K)$, amire $a \in \mathbb{I}^{S(\mathfrak{m})} \implies \phi_K(a) = \psi(id(a))$ és ϕ_K magja tartalmazza $W_\mathfrak{m}$-et, tehát az összes L-ben elágazó prím eleme $S(\mathfrak{m})$-nek, mert ezeknél a bővítéseknél L_w-t nem hagyhatja rögzítve az összes egységelem. A $\phi_{L|K}(a) := \Pi_v \phi_v(a_v)$ képletből látszik, hogy ψ nem más, mint a klasszikus Artin leképzés $I_\mathfrak{m}$-en, ami így szürjektív és ahhoz, hogy bebizonyítsuk, hogy a magja $K_{\mathfrak{m},1} N_{L|K} I_L$, elég belátni, hogy a következő diagram kommutatív:

$$\begin{array}{ccc} \mathbb{I}_L & \longrightarrow & I_L \\ \downarrow N & & \downarrow N \\ \mathbb{I}_K & \longrightarrow & I_K \end{array}$$

Valóban, legyen egy $a = (1, 1, 1 ... \pi_w, 1, 1 ...)$, ekkor $id \circ N(a) = \mathfrak{p}_v^{f_w} = N \circ id(a)$ és ezek az elemek generálják a csoportot, tehát készen vagyunk.

Most a létezéstétel igazolásához legyen $K_{\mathfrak{m},1} \subset H \subset I_\mathfrak{m}$ egy kongruenciacsoport. Mivel $C_\mathfrak{m} \cong \mathbb{I}_\mathfrak{m} / K_{\mathfrak{m},1} \cdot W_\mathfrak{m}$, ezért H megfeleltethető $\mathbf{C}_K$ egy nyílt, véges indexű

részcsoportjával. Tehát létezik egy véges Abel-bővítés, amire $H = N_{L|K}\mathbf{C}_L$, azaz $H = K_{\mathfrak{m},1} \cdot N_{L|K}\mathbb{I}_L$, ($\mathbb{I}_K^{\mathfrak{m}}$-ben,) és így szintén a fenti kommutatív diagram miatt $H = K_{\mathfrak{m},1} \cdot N_{L|K}I_L$ □

5. fejezet

Az absztrakt osztálytestelmélet

5.1. Osztálytestelmélet provéges csoportokon

Most megkezdem a reciprocitástételek vázlatos bizonyítását.

A bizonyítás különlegessége, hogy nagyon kevés információt használunk a testekről magukról, majdnemhogy teljesen csoportelméleti bizonyításról beszélhetünk. Hogy ez tisztábban látszódjon, általános provéges csoportokra fogjuk bebizonyítani az úgynevezett reciprocitástételt, egyetlen egy axiómára építve, amihez viszont már nem elég ez az információ. Később be fogjuk látni ezt az axiómát a lokális esetben, azonban ez a globális esetben is igaz, így a két tétel bizonyítása az axióma igazolása után ugyanaz.

Nagyon érdekes, hogy egy provéges csoportból "ki lehet nyerni" testbővítéseket még akkor is ha za nem egy Galois-csoport, a következőképpen. Legyen G egy provéges csoport. Ha ez egy Galois-csoport lenne, akkor a zárt részcsoportjai a résztesteknek felelnének meg tehát indexeljük G zárt részcsoportjait "testekkel", így G_K-át felfoghatjuk úgy mint a "K testet" rögzítő automorfizmusok csoportját. Hasonlóan definíció szerint azt mondjuk ezekről a testekről, hogy $K \subset L$ akkor és csak akkor ha $G_L \subset G_K$, egy test Galois ha G_K normális részcsoport, k-ával jelöljük azt a testet amire $G_k = G$, hasonlóan $G_{\bar{k}} = \{1\}$, és G-re $G(\bar{k} \mid k)$-ként gondolunk. Egy $L \mid K$ bővítés foka $[G_K : G_L]$ és Galois-csoportja G_K/G_L ha a bővítés Galois. Továbbá a testek kompozitumjait és metszeteit is tudjuk értelmezni a megfelelő csoportok metszetei és szorzataihoz tartozó indexekként. Hasonlóan értelmezhetők az automorfizmusok megszorításai és a testek automorfizmusok alatti képei is.

Ezen felül a provéges csoportunk mellé társítanunk kell egy A folytonos modulust

is, mint a Kummer-elméletben, ha azt akarjuk, hogy az általános tétel speciális esetében $K^\times$ vagy $\mathbf{C}_\mathbb{Q}$-ról tudjunk kimondani valamit. Valóban, ha a kedves olvasót nem érdekli az általános eset, akkor a fentiek alapján nyugodtan felteheti, hogy A csupán "$\bar{K}^\times$ vagy $\bigcup_{K|\mathbb{Q}\text{véges}} \mathbf{C}_K$" rövidítése és G a megfelelő abszolút Galois-csoport. Itt $\bigcup_{K|\mathbb{Q}\text{véges}} \mathbf{C}_K$- ben $\mathbf{C}_K$-át megfeleltetjük az

$$i : \mathbb{I}_K \to \mathbb{I}_L : (a_v) \to i(a)_w = a_v \text{ minden } w \mid v \text{ esetén}$$

homomorfizmus által indukált $\mathbf{C}_K \to \mathbf{C}_L$ leképzés képével (amiről be lehet látni, hogy injektív) és G hatását koordinátákként értelmezzük.

Továbbá H^{-1} mellé definiáljuk a

$$H^0(G(L \mid K), A_L) = A_K / N_{L|K} A_L$$

csoportot, melynek segítségével meg tudjuk fogalmazni azt a bizonyos, a Kummer-elméletbelihez hasonló axiómát:

Osztálytest axióma Minden véges ciklikus bővítésre $H^{-1}(G(L \mid K), A_L) = 1$ és $\#H^0(G(L \mid K), A_L) = [L : K]$.

Az elmélet kidolgozásához a provéges G csoport és a folytonos G-modulus mellet még szükségünk lesz egy szürjektív, folytonos $d : G \to \widehat{\mathbb{Z}}$ homomorfizmusra, amire intuitívan gondolhatunk úgy, hogy ez írja a le az elágazás jelenségét; és egy $v : A_k \to \widehat{\mathbb{Z}}$ homomorfizmusra, mely rendelkezik néhány technikai tulajdonsággal. A v leképzésre egy valuációként fogunk gondolni és ki fog derülni, hogy az információból, amit ez a két homomorfizmus szolgáltat, fel lehet építeni egy elméletet amiben a lokális testek estével hasonlóan tudunk használni olyan fogalmakat, mint prím, egység, elágazásmentes bővítés és egyebek, még akkor is ha a konkrét alkalmazásban (például a globális esetben) nagyon furcsa módon jelennek meg ezek a fogalmak.

A definicót motiváló példák a lokális estből jönnek: v a szokásos valuáció, d pedig az automotfizmusok megszorítása a maximális elágazásmentes bővítésre, melynek Galois-csoportja kanonikusan izomorf $\widehat{\mathbb{Z}}$-el. A globális esetben nincs túl sok választásunk d-re, hiszen minden Abel-bővítés benne van a körosztási testek uniójában, melynek Galois-csoportja

$$\widehat{\mathbb{Z}}^\times \cong \prod_p \mathbb{Z}_p^\times \cong \prod_p \mu_{\mathbb{Q}_p} \times \mathbb{Z}_p \cong (\prod_p \mu_{\mathbb{Q}_p}) \times \widehat{\mathbb{Z}},$$

tehát magától adódó, hogy vegyük a torziós csoport által rögzített T testet, melynek Galois csoportja így izomorf lesz $\widehat{\mathbb{Z}}$-vel; v pedig d és a $\phi_{\mathbb{Q}}$ artin leképzés kompozíciójaként fog előállni (amiről ugye tudni fogjuk, hogy létezik, amint bebizonyítjuk a lokális reciprocitás- és létezéstételt.) Lásd az 5.1-es táblázatot egy összegzésért.

Absztrakt	**Lokális**	**Globális**
G provéges csoport	$G(\bar{K} \mid K)$, ahol K lokális test	$G(\bar{\mathbb{Q}} \mid \mathbb{Q})$
A folytonos G-modulus	$\bar{K}^\times$	$\bigcup_{K\mid\mathbb{Q}\text{véges}} \mathbf{C}_K$
$d : G \to \widehat{\mathbb{Z}}$	$\sigma \to \sigma\mid_{\tilde{K}}$	$\sigma \to \sigma\mid_T$
$v : A_k \to \widehat{\mathbb{Z}}$	a szokásos valuáció	d komponálva a $\phi_{\mathbb{Q}}$-val

5.1. táblázat. Az absztrakt osztálytestelmélet objektumai

Visszatérve arra, hogy hogyan lehet az elágazással kapcsolatos fogalmakat értelmezni általános esetben, legyen I a d leképzés magja. Az I fix testére gondolhatunk úgy, mint $\tilde{k}$-ára, azaz k maximális elágazásmentes bővítésére, amire $G(\tilde{k} \mid k) \cong \widehat{\mathbb{Z}}$. Hasonlóan tudjuk értelmezni egy tetszőleges K test maximális elágazásmentes bővítését is. Legyen $I_K \subset G_K$ a d megszorításának magja, ekkor I_K rögzített testét $\tilde{K}$-ával jelöljük. Látszik, hogy $I_K = G_K \cap I = G_{K\tilde{k}}$, vagyis $\tilde{K} = K\tilde{k}$.

Legyen $f_K = [\widehat{\mathbb{Z}} : d(G_K)]$ és $e_K = [I : I_K]$, vagy egy kicsit általánosabban $f_{L|K} = [d(G_K) : d(G_L)]$ és $e_{L|K} = [I_K : I_L]$. Az egyből látszik, hogy a lokális esetben f megegyezik a régi definícióval és az, hogy ez e-re is így van, az a következő állításból következik.

26. Tétel. *Minden $L \mid K$ bővítésre $[L : K] = e_{L|K} \cdot f_{L|K}$.*

Bizonyítás. Ha $K \subset L \subset M$, véges bővítések tornya, akkor a definíciókból látszik, hogy $e_{M|K} = e_{M|L}e_{L|K}$ és $f_{M|K} = f_{M|L}f_{L|K}$, tehát az állításunkban feltehetjük, hogy $L \mid K$ Galois. Most a diagram kommutativitása miatt

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I_L & \longrightarrow & G_L & \xrightarrow{d} & d(G_L) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & I_K & \longrightarrow & G_K & \xrightarrow{d} & d(G_L) & \longrightarrow & 1 \end{array}$$

kapunk egy egzakt sorozatot a faktorcsoportokon:

$$1 \to I_K/I_L \to G(L \mid K) \to d(G_K)/d(G_L) \to 1,$$

ahol a rendeket nézve leolvashatjuk a képletet. □

Egy $L \mid K$ bővítésről azt mondjuk, hogy elágazásmentes ha $e_{L|K} = 1$ és hogy teljesen elágazó ha $f_{L|K} = 1$. Észrevehetjük, hogy ha f_K véges, akkor G_K-án is létezik egy $d_K = \frac{1}{f_K} d : G_K \to \widehat{\mathbb{Z}}$ szürjektív homomorfizmus, ami egy izomorfizmust indukál $G(\tilde{K} \mid K)$-val. Emiatt tudjuk értelmezni φ_K-át, a K test Frobenius automorfizmusát, (azaz az 1-nek megfelelő automorfizmust) melynek megszorítását L-re $\varphi_{L|K}$-val jelöljük.

Most készen állunk arra, hogy bevezessem a v-re vonatkozó feltételeket:

1. Legyen v képe Z olyan, hogy $\mathbb{Z} \subset Z$ és $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$. Ez gyakorlatilag azt jelenti, hogy $Z = \mathbb{Z}$ a lokális esetben, vagy $Z = \widehat{\mathbb{Z}}$ a globálisban.

2. $v(N_{K|k} A_K) = f_K Z$ minden $K \mid k$ véges bővítésre.

A v a d-hez hasonlóan minden véges bővítésre definiál egy szürjektív $v_K = \frac{1}{f_K} v \circ N_{K|k} : A_K \to Z$ homomorfizmust, melynek segítségével általános folytonos modulusokon is tudjuk értelmezni A_K prímjeit és egységeit: azt mondjuk, hogy π_K egy prím, ha $v(\pi_K) = 1$ és az egységek U_K csoportja v_K magja. (Vegyük észre, hogy milyen megfoghatatlanok $\mathbf{C}_K$ prímjei ebben az értelemben.)

5.2. Az általános reciprocitástétel

Ahelyett, hogy az Artin leképzés általánosítását definiálnánk, kiderül, hogy célratörőbb, ha az inverzével dolgozunk. Tehát most az a célunk, hogy definiáljunk egy $r_{L|K} : G(L \mid K) \to A_K / N_{L|K} A_L$ leképzést, amiről belátjuk, hogy véges Abel-bővítések esetén egy izomorfizmus. Az ötlet az az, hogy L automorfizmusait valahogy visszahúzzuk $\tilde{L}$ automorfizmusaira és ott definiáljuk a leképzést. Evégett legyen

$$Frob(\tilde{L} \mid K) = \{\sigma \in G(\tilde{L} \mid K) \mid d_K(\sigma) \text{egy pozitív egész.}\}$$

Erre a félcsoportra intuitívan gondolhatunk úgy, mint a Frobenius automorfizmus véges hatványaira szorozva $G(L \mid K)$ "elágazásos" automorfizmusaival. Valóban a $G(\tilde{L} \mid \tilde{K}) \cong G(L \mid L \cap \tilde{K})$ izomorfizmus kulcsfontosságú lesz.

27. Tétel. *Ha $L \mid K$ egy véges bővítés akkor $Frob(\tilde{L} \mid K)$ elemeinek megszorítása L-re egy szürjektív leképzést ad.*

Bizonyítás. Legyen $\sigma \in G(L|K)$ egy tetszőleges automorfizmus, ezt vissza kell húznunk $Frob(\tilde{L} \mid K)$-ba. Hiszen $\tilde{K} \subset \tilde{L}$, ezért a $d_K : G(\tilde{K} \mid K) \to \widehat{\mathbb{Z}}$ homomorfizmus átfaktorizálódik $G(\tilde{L} \mid K)$-n és így tudunk választani egy $\varphi \in G(L \mid K)$ automorfizmust, amire $d_K(\varphi) = 1$. Mivel $L \cap \tilde{K}$ egy véges elágazásmentes bővítés, ezért ciklikus és Galois csoportját φ megszorítása generálja, tehát létezik egy n, amire $\sigma_{L\cap\tilde{K}} = \varphi^n_{L\cap\tilde{K}}$. Most legyen $\tau = \sigma\varphi^{-n}$ egy $G(L \mid L \cap \tilde{K})$-beli automorfizmus. Ezt a $G(\tilde{L} \mid \tilde{K}) \cong G(L \mid L \cap \tilde{K})$ izomorfizmus segítségével kiterjesztjük egy $G(\tilde{L} \mid \tilde{K})$-beli automorfizmussá, (amit szintén τ-val jelölök). Tehát $\tau\varphi^n \in Frob(\tilde{L} \mid K)$ és $\tau\varphi^n \mid_L = \sigma$. □

Szükségünk lesz a következő technikai állításra:

28. Tétel. *Jelöljük Σ-ával egy adott $\sigma \in Frob(\tilde{L} \mid K)$ elem rögzített testét. (Ez után is ezt a jelölést fogjuk alkalmazni.) Ekkor Σ egy véges bővítése K-nak, $f_{\Sigma|K} = d_K(\sigma)$, $\tilde{\Sigma} = \tilde{L}$ és $\varphi_\Sigma = \sigma$.*

Bizonyítás. Először is $f_{\Sigma|K} = |\Sigma \cap \tilde{K} : K|$, azaz a legnagyobb elágazásmentes részbővítésének a foka, node φ_K-nak pont a $d_K(\sigma)$-adik hatványa lesz a legkisebb, ami rögzíti $\Sigma \cap \tilde{K}$-át, vagyis $f_{\Sigma|K} = d_K(\sigma)$.

Mivel már tudjuk, hogy $f_{\Sigma|K}$, véges ezért elég megmutatni, hogy $e_{\Sigma|K}$ is véges, ahhoz hogy a bővítés végességét igazoljuk. Valóban, $e_{\Sigma|K} = \#G(\Sigma \mid \Sigma \cap \tilde{K})$, de mivel $\tilde{\Sigma} = \Sigma\tilde{K} \subset \tilde{L}$, ezért $\#G(\Sigma \mid \Sigma \cap \tilde{K}) \leq \#G(\tilde{L} \mid \tilde{K})$, amiről tudjuk, hogy véges.

A megszorítás által adott $G(\tilde{L} \mid \Sigma) \to G(\tilde{\Sigma} \mid \Sigma)$ leképzés szürjektív és injektivitását elég belátni a $G(\tilde{L} \mid \Sigma)/G(\tilde{L} \mid \Sigma)^n \to G(\tilde{\Sigma} \mid \Sigma)/G(\tilde{\Sigma} \mid \Sigma)^n$ faktorcsoportokon, mert $G(\tilde{\Sigma} \mid \Sigma) \cong \widehat{\mathbb{Z}}$. A végtelen galois-elmélet tételéből tudjuk, hogy $G(\tilde{L} \mid \Sigma) = <\bar{\sigma}>$, node $\{1, \sigma, ...\sigma^{n-1}\}$ véges és így diszkrét, tehát a faktorcsoportnak maximum n eleme lehet, és így a leképzésnek izomorfizmusnak kell lennie, azaz $G(\tilde{L} \mid \Sigma) = G(\tilde{\Sigma} \mid \Sigma)$ és $\tilde{\Sigma} = \tilde{L}$.

Végül $d_\Sigma(\sigma) = f^{-1}_{\Sigma|K} d_K(\sigma) = 1$, tehát $\sigma = \varphi_\Sigma$.

□

Vegyük észre, hogy eddig nem is használtuk az osztálytest axiómát és még egy ideig nem is lesz szükségünk a teljes erejére, csak egy következményére.

29. Tétel. *Az osztálytest axiómából következik, hogy minden véges, elágazásmentes $L \mid K$ bővítésre $\#H^0(G(L \mid K), U_L) = \#H^{-1}(G(L \mid K) = 1$.*

Bizonyítás. Kezdjük a $\#H^{-1}(G(L \mid K) = 1$ egyenlőséggel! Legyen $u \in U_L$ olyan, hogy $N_{L|K} = 1$. Ekkor az axióma miatt létezik egy $a \in A_L$, amire $u = a^{\sigma-1}$, ahol σ generálja a bővítés Galois-csoportját. Mivel $v(A_L) = v(A_K)$, ezért létezik egy $\alpha \in A_K$, amire $v(\alpha) = v(a)$, tehát $a = v \cdot \alpha$ valamilyen $v \in U_L$-re és így $u = a^{\sigma-1} = v^{\sigma-1}$.

Most a második egyenlőséghez tekintsük a $A_K \xrightarrow{v_K} \mathbb{Z}/n\mathbb{Z}$ leképzést, ami átfaktorizálódik $A_K/N_{L|K}A_L$-en, mert $v_K(N_{L|K}(a)) = n \cdot v_L(a)$ és ennek magja $U_K/N_{L|K}U_L$, mert $N_{L|K}U_L = N_{L|K}A_L \cap U_K$. Vagyis kapunk egy egzakt sorozatot:

$$1 \to U_K/N_{L|K}U_L \to A_K/N_{L|K}A_L \to \mathbb{Z}/n\mathbb{Z} \to 1.$$

No de itt az utolsó két csoport elemszáma n, így $U_K/N_{L|K}U_L = 1$. □

30. Tétel. *Az*

$$r_{\tilde{L}|K}(\tilde{\sigma}) = N_{\Sigma|K}(\pi_\Sigma) \pmod{N_{\tilde{L}|K}A_{\tilde{L}}}$$

képlet a prímelem megválasztásától független, és így egy függvényt definiál $Frob(\tilde{L} \mid K)$-n. Itt a végtelen bővítés normája $N_{\tilde{L}|K}A_{\tilde{L}} = \bigcap_{M|K \text{véges részbővítés}} N_{M|K}A_M$.

Bizonyítás. Legyen π'_Σ egy másik prím Σ-ban, ekkor $\pi'_\Sigma = u\pi_\Sigma$ valamely $u \in U_\Sigma$ egységelemre és $N_{\Sigma|K}(\pi'_\Sigma) = N_{\Sigma|K}(u) \cdot N_{\Sigma|K}(\pi_\Sigma)$, tehát elég belátnunk, hogy $N_{\Sigma|K}u \in N_{M|K}A_M$ minden $K \subset M \subset \tilde{L}$ véges bővítésre. Nyilván feltehetjük hogy M tartalmazza Σ-át. Ekkor $M \mid \Sigma$ egy elágazásmentes bővítés lesz, mert $M \subset \tilde{L} = \tilde{\Sigma}$, tehát $u = N_{M|\Sigma}a$ valamilyen $a \in A_M$-re, vagyis $N_{\Sigma|K}u = N_{\Sigma|K} \circ N_{M|\Sigma}a = N_{M|K}a$.

□

Míg általában, ha definiálunk egy függvényt ami homomorfizmus, akkor arról ez többnyire egyértelmű szokott lenni, viszont érdekes, hogy itt közel sem ez a helyzet.

31. Tétel. *$r_{\tilde{L}|K}$ multiplikatív.*

Az állítás bebizonyításához szükségünk lesz két lemmára.

32. Tétel. *Legyen $\sigma, \varphi \in Frob(\tilde{L} \mid K)$ úgy, hogy $d_K(\varphi) = 1$ és $d_K(\sigma) = n$. ekkor minden $a \in A_\Sigma$-ra*

$$N_{\Sigma|K}a = N_{\tilde{L}|\tilde{K}} \circ \varphi_n a = \varphi_n \circ N_{\tilde{L} \mod \tilde{K}}a,$$

ahol $\varphi_n := 1 + \varphi + ...\varphi^{n-1}$.

Bizonyítás. Legyen $\Sigma_0 = \Sigma \cap \tilde{K}$, ekkor $N_{\Sigma|K} = N_{\Sigma_0|K} \circ N_{\Sigma|\Sigma_0}$. Mivel Σ_0 nem más mint Σ legnagyobb elágazásmentes részbővítése, ezért a ciklikus Galois-csoportját φ generálja, és így $N_{\Sigma_0|K} = \varphi_n$. Továbbá $G(\Sigma \mid \Sigma_0) \cong G(\tilde{\Sigma} \mid \tilde{K}) = G(\tilde{L} \mid \tilde{K})$, vagyis $N_{\Sigma|\Sigma_0} = N_{\tilde{L}|\tilde{K}}$, és az állítás egyik fele meg is van. A második pedig onnan következik, hogy $G(\tilde{L} \mid \tilde{K})$ normálosztó $G(\tilde{L} \mid K)$-ban. □

33. Tétel. *Legyen $\varphi \in Frob(\tilde{L} \mid K)$ olyan, hogy $d_K(\varphi) = 1$. Ekkor minden $u \in U_{\tilde{L}}$-re, ha*

$$u = \Pi_{\tau \in G(\tilde{L}|\tilde{K}} u_\tau^{\tau-1},$$

ahol $u_\tau \in U_{\tilde{L}}$, akkor $N_{\tilde{L}|\tilde{K}} u \in N_{\tilde{L}|K} U_{\tilde{L}}$.

Bizonyítás. Meg kell mutatnunk, hogy $N_{\tilde{L}|\tilde{K}} u \in N_{M|K} U_M$ minden $M \in \tilde{L}$ véges részbővítésre. Feltehetjük, hogy M Galois és tartalmazza u, u_τ és L-et. Jelöljük n-el $|M : K|$-át, és σ-ával φ^n-et. Ekkor σ rögzíti M-et, mert annak Galois csoportjában bármely automorfizmus n-edik hatványa az identitás. Ha továbbá definiáljuk a $\Sigma_n = \sigma^n$ fixtestét, akkor tekinthetjük a véges bővítések tornyát:

$$\begin{array}{c} \Sigma_n \\ | \\ \Sigma \\ | \\ M \\ | \\ L \\ | \\ K \end{array}$$

Az axiómát felhasználva tudunk választani olyan $u', u'_\tau \in U_{\Sigma_n}$ elemeket, amelyekre $u = u'^{\sigma_n}$, tehát $u'^{\varphi-1} = x \cdot \Pi_{\tau \in G(\tilde{L}|\tilde{K}} u'^{\tau-1}_\tau$ egy olyan $x \in U_{\Sigma_n}$-re, amire $x^{\sigma_n} = 1$. Szintén az axióma miatt választhatunk egy $y' \in U_{\Sigma_n}$-et, amire $x = y'^{\sigma-1} = y'^{\varphi^n-1}$. Ha ennek az egyenletnek vesszük a normáját, és kihasználjuk a $\varphi^n - 1 = \varphi_n \circ (\varphi - 1)$ egyenlőséget, azt kapjuk, hogy

$$N_{\tilde{L}|\tilde{K}} u'^{\varphi-1} = N_{\tilde{L}|\tilde{K}} (y'^{\varphi_n})^{\varphi-1}.$$

Azaz a két érték egy olyan $z \in U_{\tilde{K}}$ elemmel különbözik, amit φ fixen hagy, tehát

valójában $u \in U_K$. Végül alkalmazzuk az előző állítást a $y := y'^{\sigma_n}$ jelölés mellett!

$$N_{\tilde{L}|\tilde{K}} u = N_{\tilde{L}|\tilde{K}} u'^{\sigma_n} = N_{\tilde{L}|\tilde{K}} (y'^{\varphi_n})^{\sigma_n} \cdot z^{\sigma_n} = N_{\tilde{L}|\tilde{K}} y^{\varphi_n} \cdot z^n =$$

$$= N_{\Sigma|K}(y) N_{M|K}(z) \in N_{M|K} U_M.$$

□

Bizonyítás. 31. tétel bizonyítása. Tegyük fel, hogy $Frob(\tilde{L} \mid K)$-ban $\sigma_1 = \sigma_2\sigma_3$ és vezessük be a következő jelöléseket: $n_i = d_K(\sigma_i)$, Σ_i a σ_i által rögzített test és π_i ennek egy prím eleme. Ha $\varphi \in G(\tilde{L} \mid K)$ olyan, hogy $d_K(\varphi) = 1$, akkor legyen $\tau_i := \sigma_i^{-1} \cdot \varphi^{n_i} \in G(\tilde{L} \mid \tilde{K})$. A $\sigma_1 = \sigma_2\sigma_3$ egyenlőséget kihasználva:

$$\tau_1 = \sigma_3^{-1}\sigma_2^{-1}\varphi^{n_2+n_3} = \sigma_3^{-1}\varphi^{n_3} \cdot (\varphi^{-n_3}\sigma_2\varphi^{n_3})^{-1}\varphi^{n_2}.$$

Ha $\sigma_4 := \varphi^{-n_3}\sigma_2\varphi^{n_3}$, akkor $n_4 = n_2$, $\Sigma_4 = \Sigma_2^{\varphi^{n_3}}$ és $\pi_4 := \pi_2^{\varphi^{n_3}}$ egy prímelem lesz, amire $N_{\Sigma_2|K}\pi_2 = N_{\Sigma_4|K}\pi_4$ és így a fenti egyenlet azt mondja, hogy $\tau_1 = \tau_3\tau_4$.

A tétel bebizonyításához azt kell belátnunk, hogy $N_{\Sigma_1|K}\pi_1 \equiv N_{\Sigma_3|K}\pi_3 \cdot N_{\Sigma_4|K}\pi_4 \pmod{N}$. Legyen $u := \pi_1^{\varphi^{n_1}}\pi_3^{\varphi^{-n_3}}\pi_4^{\varphi^{n_4}}$, ekkor, mivel $u \in U_{\tilde{L}}$, az előző két lemmát alkalmazva elég lenne megmutatnunk, hogy $u^{\varphi-1} = \Pi u_\tau^{\tau-1}$. A $\pi_3 = u_3\pi_1, \pi_4 = u_4\pi_1$ és $\pi_1^{\tau_3-1} = u_1$ jelöléseket és a $(\tau_3 - 1) \cdot (\tau_4 - 1) = \tau_3\tau_4 - 1 + 1 - \tau_3 + 1 - \tau_4 = \tau_1 - 1 + 1 - \tau_3 + 1 - \tau_4$ azonosságot alkalmazva azt kapjuk, hogy

$$u^{\varphi-1} = u_3^{\tau_3-1}u_4^{\tau_4}u_1^{\tau_4-1}.$$

□

34. Tétel. *Legyen $L \mid K$ egy (nem feltétlen Abel) véges Galois-bővítés és $\sigma \in G(L \mid K)$, ekkor ha $\tilde{\sigma} \in Frob(\tilde{L} \mid K)$ σ bármely őse, akkor $r_{\tilde{L}|K}(\tilde{\sigma}) \pmod{N_{L|K}A_L}$ értéke $\tilde{\sigma}$ megválasztásától független lesz és így kapunk egy szürjektív*

$$r_{L|K} : G(L \mid K) \to A_K/N_{L|K}A_L$$

homomorfizmust.

Bizonyítás. Legyen $\tilde{\sigma}$ és $\tilde{\sigma'}$ két őse σ-nak. Ha $d_K(\tilde{\sigma}) = d_K(\tilde{\sigma'})$ akkor $\tilde{\sigma} = \tilde{\sigma'}$ és készen vagyunk. Tegyük fel most, hogy $d_K(\tilde{\sigma'}) > d_K(\tilde{\sigma})$. Ekkor $\tilde{\sigma'} = \tau\tilde{\sigma}$ valamely $\tau \in Frob(\tilde{L} \mid K)$-ra, tehát a multiplikativitást kihasználva elég bebizonyítani, hogy

$N_{\Sigma|K}\pi_\Sigma \in N_{L_K}A_L$, ahol Σ a τ fixteste. No de $\tau\mid_L = 1$, tehát $L \subset \Sigma$ és így készen vagyunk. □

Az osztálytest axióma teljes erejét még mindig nem használtuk, sőt, az elágazásmentes bővítések esetében még az izomorfizmus is kijön abból a bizonyos következményből.

35. Tétel. *Ha $L \mid K$ egy elágazásmentes véges bővítés, akkor $r_{L|K}$ egy izomorfizmus és*

$$r_{L|K}(\varphi_{L|K}) = \pi_K \pmod{N_{L|K}A_L}.$$

Bizonyítás. Mivel $L \mid K$ elágazásmentes, így $\tilde{L} = \tilde{K}$ és $\varphi_K \in Frob(\tilde{L} \mid K)$ az L-re megszorítva pont $\varphi_{L|K}$. No de φ_K rögzített teste K, tehát valóban $r_{L|K}(\varphi_{L|K}) = \pi_K \pmod{N_{L|K}A_L}$. Tekintsük most a függvények kompozícióját:

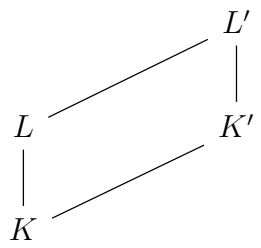
$$G(L \mid K) \to A_K/N_{L|K}A_L \xrightarrow{v_K} Z/n \cdot Z \cong \mathbb{Z}/n\mathbb{Z},$$

ahol $n = |L : K|$. Itt v_K a $v_K \circ N_{L|K}A_L \subset f_{L|K}Z = nZ$ tulajdonság miatt faktorizálódik át $N_{L|K}A_L$-en. v_K nyílván szürjektív és injektív is, hiszen ha $v_K(a) = n \cdot z \in n \cdot Z$, akkor létezik egy $\alpha \in A_K$, amire $v_K(\alpha) = z$, tehát $v_K(\alpha^n) = v_K(N_{L_K}\alpha) = n \cdot z$, no de a és α^n csak egy U_K-beli egységgel, tehát egy U_L-beli egység normájával különböznek, tehát $a \in N_{L|K}A_L$. Az, hogy $r_{L|K}$ egy izomorfizmus, most onnan következik, hogy a csoport generátorát $\mathbb{Z}/n\mathbb{Z}$ generátorába viszi.

□

Az általános esetben viszont tényleg szükségünk lesz az osztálytest axiómára, valamint $r_{L|K}$ egy funktoriális tulajdonságára.

36. Tétel. *Legyenek*



véges bővítések. Ekkor kapunk egy kommutatív diagramot:

$$\begin{array}{ccc} G(L' \mid K') & \xrightarrow{r_{L'|K'}} & A'_K/N_{L'|K'}A_{L'} \\ \downarrow & & \downarrow{\scriptstyle N_{K'|K}} \\ G(L \mid K) & \xrightarrow{r_{L|K}} & A_K/N_{L|K}A_L \end{array}$$

Bizonyítás. Ha $\tilde{\sigma} \in Frob(L' \mid K')$ olyan, hogy $\tilde{\sigma} \mid_{L'} = \sigma$, akkor egyben $(\tilde{\sigma} \mid_{\tilde{L}}) \mid_L = \sigma_L$, tehát $\tilde{\sigma'} := \tilde{\sigma} \mid_{\tilde{L}}$ egy őse lesz σ_L-nek $Frob(\tilde{L} \mid K)$-ban. Szokás szerint jelöljük Σ-ával $\tilde{\sigma}$ fixtestét és legyen π_Σ ennek egy prímje. Ekkor $\tilde{\sigma'}$ fixteste $\Sigma' := \Sigma \cap \tilde{L}$ és ennek $N_{\Sigma|\Sigma'}\pi_\Sigma$ egy prímje lesz. Az állítás így könnyen következik a

$$N_{K'|K} \circ N_{\Sigma|K'} = N_{\Sigma|K} = N_{\Sigma'|K} \circ N_{\Sigma|\Sigma'}$$

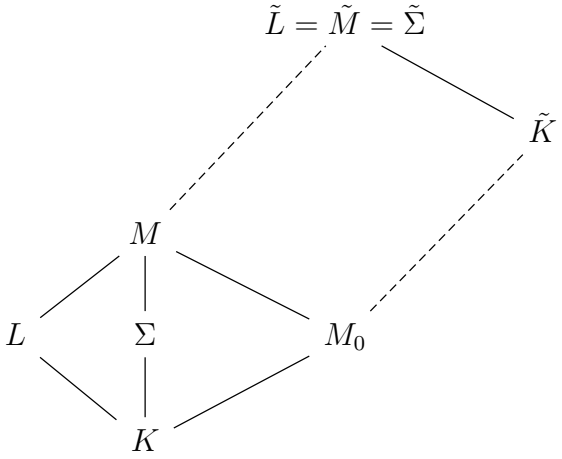
egyenlőségből. □

37. Tétel. *Minden $L \mid K$ véges Galois-bővítésre*

$$r_{L|K} : G(L \mid K)^{ab} \to A_K/N_{L|K}A_L$$

egy izomorfizmus. (Itt tetszőleges csoportra $G^{ab} = G/[G,G]$.)

Bizonyítás. Első lépés: $L \mid K$ teljesen elágazó ciklikus. Mivel $L \cap \tilde{K} = K$ és $\tilde{L} = L\tilde{K}$, ezért $G(\tilde{L} \mid K) = G(L \mid K) \times G(\tilde{K} \mid K)$. Jelöljük $= G(L \mid K)$ egy generátorát σ-val, ezt az izomorfizmus miatt egy $\tilde{L}$ feletti automorfizmusként is felfoghatjuk. (Hasonlóan φ_K-val.) Legyen $\tilde{\sigma} = (\sigma, \varphi_K)$ és Σ ennek egy fixteste. Ekkor Σ teljesen elágazásos, $n = |L : K|$-ad rendű bővítés, melynek Galois csoportja $< \sigma >$ megszorítása és $\tilde{L} = \tilde{\Sigma}$. Most legyen $M \mid K$ egy véges bővítés, ami tartalmazza L-et és Σ-át és legyen M_0 a maximális elágazásmentes részbővítése.



Vegyük észre, hogy $G(M \mid M_0) \cong G(\tilde{M} \mid \tilde{K}) = G(\tilde{L} \mid \tilde{K})$, tehát ciklikus és Galois csoportja szintén $< \sigma >$ megszorítása M-re. Speciálisan $N_{M|M_0} \mid_L = N_{L|K}$ és $N_{M|M_0} \mid_\Sigma = N_{\Sigma|K}$. Tegyük fel, hogy $r_{L|K}(\sigma^k) = 1$. Meg kell mutatnunk, hogy $n \mid k$ az injektivitás belátásához. $\tilde{\sigma}$-át választva σ őseként, ez azt mondja, hogy $N_{M|M_0}\pi_\Sigma^k = 1 \pmod{N_{L|K}A_L}$. Mivel $M \mid L$ elágazásmentes, ezért v_M értéke megegyezik π_Σ és π_L-en, tehát létezik egy $u \in U_M$, amire $\pi_\Sigma^k = u\pi_L^k$. Ebből következik, hogy $N_{M|M_0}\pi_\Sigma^k = N_{M|M_0}u \cdot N_{M|M_0}\pi_L^k = N_{M|M_0}u = 1 \pmod{N_{L|K}A_L}$, vagyis létezik egy $v \in U_L$-amire $N_{M|M_0}u = N_{M|M_0}v$, azaz $N_{M|M_0}uv^{-1} = 1$ Mivel $M \mid M_0$ ciklikus, ezért használhatjuk az axiómát, hogy találjunk egy $a \in U_M$-et, amire $uv^{-1} = a^{\sigma-1}$. Most legyen $x = \pi_L^k v a^{\tilde{\sigma}-1}$, ekkor $x \in A_{M_0}$, hiszen

$$(\pi_L^k v)^{\sigma-1} = (\pi_L^k v)^{\tilde{\sigma}-1} = (\pi_\Sigma^k u^{-1} v)^{\tilde{\sigma}-1} = (a^{1-\sigma})^{\tilde{\sigma}-1} = (a^{1-\tilde{\sigma}})^{\sigma-1},$$

és $n \cdot v_{M_0}(x) = v_M(x) = k$, azaz $n \mid k$ és az injektivitást beláttuk. A szürjektivitás pedig a csoportok elemszámából következik.

Második lépés: $L \mid K$ ciklikus. Ha $M \mid K$ egy Galois-részbővítése $L \mid K$-nak akkor kapunk egy kommutatív egzakt diagramot amit többször fogunk használni a bizonyításban.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G(L \mid M) & \longrightarrow & G(L \mid K) & \longrightarrow & G(M \mid K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle r_{L|M}} & & \downarrow{\scriptstyle r_{L|K}} & & \downarrow{\scriptstyle r_{M|K}} & & \\ & & A_M/N_{L|M}A_L & \xrightarrow{N_{M|K}} & A_K/N_{L|K}A_L & \longrightarrow & A_K/N_{M|M}A_M & \longrightarrow & 1 \end{array}$$

Az $M = L \cap \tilde{K}$ választás mellett az alsó sort kibővíthetjük bal oldalt egy egyessel és úgy is egzakt fog maradni a csoportok elemszámai miatt. No de a bal és jobb oldali nyílról már tudjuk, hogy izomorfizmusok, tehát a középső is az.

Harmadik lépés: $L \mid K$ Abel-bővítés. Indukciót alkalmazunk a bővítés rendjén. Ha $L \mid K$ ciklikus, akkor készen vagyunk, ha nem, akkor a ciklikus részbővítései szigorúan kisebbek lesznek és ezek generálják $L \mid K$-át tehát a szürjektivitást meg is kaptuk. Most válasszuk M-nek egy ciklikus részbővítést. A diagramban az indukciós feltevés miatt mindkét oldali homomorfizmus izomorfizmus, és így azt kapjuk, hogy $\ker r_{L|K} \subset G(L \mid M)$ minden ciklikus részbővítésre, tehát $\ker r_{L|K} = 1$.

Negyedik lépés: $L \mid K$ tetszőleges. Megint indukciót alkalmazunk a bővítés rendjén. Ha $G' \neq G, 1$, akkor legyen $M = L^{ab} \neq L, 1$ és a diagramot kergetve megkapjuk, hogy $r_{L|K}$ szürjektív és, hogy $\ker r_{L|K} \subset G(L \mid K)'$, tehát az injektivitást is.

Ha $G' = G$, akkor legyen M egy p-Sylow csoport fixtestje, ami nem mindig lesz Galois, de ettől még a diagram bal felét tudjuk használni. Mivel minden p-csoport feloldható, ezért M szigorúan kisebb, mint L és azt kapjuk, hogy $r_{L|M}$ szürjektív. Ha $G' = G$, akkor $G^{ab} = 1$, azaz elég megmutatnunk, hogy $r_{L|K}$ szürjektív. Ehhez pedig nyilván elég megmutatni, hogy N_{M_K} szürjektíven képez $A_K/N_{L|K}A_L$ p-Sylow részcsoportjára tetszőleges p esetén.Valóban, az $i : A_K \to A_M$ inklúzió ad nekünk egy $i : A_K/N_{L|K}A_L \to A_M/N_{L|M}A_L$ leképzést, amire $N_{M|K} \circ i = |M : K|$. Mivel $(|M : K|, 1) = 1$, ezért ez szürjektíven viszi $A_K/N_{L|K}A_L$ p-Sylow részcsoportját önmagába, tehát $N_{M|K}$-nak is annak kell lennie.

□

Egy érdekes következmény, hogy $N(L) = N(L^{ab})$, ami nagy nehézséget okoz az osztálytestelmélet tetszőleges bővítésekre való kiterjesztésében, ami a mai napig megoldatlan.

6. fejezet

A lokális reciprocitástétel bizonyítása

Ebben a fejezetben belátjuk az osztálytest axiómát és ezzel igazoljuk a lokális reciprocitás tételt.

Először is, vegyük észre, hogy az osztálytest axióma első fele a Hilbert 90-es tétel, így elég megállapítanunk $\#H^0$ értékét ciklikus bővítésekre. Ahelyett, hogy ezt direkt igazolnánk, inkább a $h = \frac{\#H^0}{\#H^{-1}}$, úgy nevezett Herbrand-hányadost határozzuk meg.

Most tekintsük ezt a hányadost egy tetszőleges ciklikus G csoport és hozzátartozó A modulus esetében.

38. Tétel. *Ha* $1 \to A \to B \to C \to 1$ *egy* G*-modulusokból álló egzakt sorozat, akkor*

$$h(B) = h(A)h(C).$$

Továbbá ha A *elemszáma véges, akkor* $h(A) = 1$.

Bizonyítás. Legyen σ egy generátora G-nek, ekkor $N \circ (\sigma - 1) = (\sigma - 1) \circ N = 0$, tehát tekinthetjük az

$$\ldots \xrightarrow{N} A \xrightarrow{\sigma-1} A \xrightarrow{N} A \xrightarrow{\sigma-1} \ldots$$

lánckomplexust, melynek homológiacsoportjai pont $H^0(A)$ és $H^{-1}(A)$ lesznek felváltva. Továbbá az is igaz, hogy egy $f : A \to B$ G-homomorfizmus egy láncleképzést ad a megfelelő komplexusok közt, hiszen f felcserélhető lesz a normával és a $\sigma - 1$ leképzéssel is, tehát az egzakt sorozatunkból nem csak három komplexust kapunk, hanem lánckomplexusok egy egzakt sorozatát.

$$\begin{array}{ccccccccc}
... & \longrightarrow & 1 & \longrightarrow & 1 & \longrightarrow & 1 & \longrightarrow & ... \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
... & \longrightarrow & A & \xrightarrow{N} & A & \xrightarrow{\sigma-1} & A & \longrightarrow & ... \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
... & \longrightarrow & B & \xrightarrow{N} & B & \xrightarrow{\sigma-1} & B & \longrightarrow & ... \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
... & \longrightarrow & C & \xrightarrow{N} & C & \xrightarrow{\sigma-1} & C & \longrightarrow & ... \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
... & \longrightarrow & 1 & \longrightarrow & 1 & \longrightarrow & 1 & \longrightarrow & ...
\end{array}$$

Mivel a homológia csoportok periódikusan váltakoznak, ezért ennek a sorozatnak a hosszú egzakt sorozata is periódikus lesz. Ha ezt a sorozatot magába fordítjuk, akkor a következő egzakt (nem kommutatív!) kört kapjuk:

$$\begin{array}{ccccc}
H^0(A) & \xrightarrow{f_1} & H^0(B) & \xrightarrow{f_2} & H^0(C) \\
\uparrow{\scriptstyle f_6} & & & & \downarrow{\scriptstyle f_3} \\
H^{-1}(C) & \xleftarrow{f_5} & H^{-1}(B) & \xleftarrow{f_4} & H^{-1}(A)
\end{array}$$

Határozzuk meg a homológiacsoportok számosságait!

$$\begin{array}{ll}
\#H^0(A) = \#Imf_6 \cdot \#Imf_1 & \#H^{-1}(A) = \#Imf_3 \cdot \#Imf_4 \\
\#H^0(B) = \#Imf_1 \cdot \#Imf_2 & \#H^{-1}(B) = \#Imf_4 \cdot \#Imf_5 \\
\#H^0(C) = \#Imf_2 \cdot \#Imf_3 & \#H^{-1}(C) = \#Imf_5 \cdot \#Imf_6
\end{array}$$

Innen megkapjuk, hogy $h(B) = h(A)h(C)$.

Ha A véges, akkor pedig az

$$1 \to Ker(N) \to A \to Im(N) \to 1$$

és

$$1 \to Ker(\sigma - 1) \to A \to Im(\sigma - 1) \to 1$$

sorozatokból $\#A$ értékét kétféleképpen kiszámolva megkapjuk, hogy $h(A) = 1$.

□

Tehát elég a következő tételt bebizonyítanunk és készen is vagyunk.

39. Tétel. *Legyen $L \mid K$ lokális testek egy ciklikus bővítése, ekkor $h(G(L \mid K), L^\times) = |L : K|$.*

Bizonyítás. Az ötlet az, hogy h jó tulajdonságait kihasználva U_L-et felszeleteljük bizonyos véges G-modulusokra és az innen szerzett egyre kisebb elemekből egy végtelen szorzat segítségével előállítunk a megfelelő normájú és $\sigma - 1$ képében lévő elemeket.

A "felszeleteléshez" a normál bázis tételt fogjuk használni, ami szerint létezik egy $\alpha \in \mathcal{O}_L$, úgy, hogy $\{\alpha^{\sigma^i}\}$ egy K-bázisa L-nek.[5] Először vegyük észre, hogy

$$1 \to U_L \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 1$$

G-modulusok egzakt sorozata, ahol $\mathbb{Z}$-n a triviális hatását vesszük G-nek. Innen $h(L^\times) = h(U_L)h(\mathbb{Z}) = h(U_L) * |L : K|$, tehát elég megmutatnunk, hogy $h(U_L) = 1$.

Most legyen $M = \bigoplus \mathcal{O}_K \alpha^{\sigma^i}$. Mivel $\mathcal{O}_L$ egy végesen generált $\mathcal{O}_K$-modulus és az α-ák egy K-bázist adnak ezért létezik egy N, amire $\pi_K^N \mathcal{O}_L \subset M$, tehát M nyílt és véges indexű $\mathcal{O}_L$-ben és így egyben zárt is. Ekkor különböző n-ekre a $V^n := 1 + \pi_K^n M$ halmazok egy egységelem körüli bázist adnak. Ha $n \geq N$, akkor V^n részcsoport is lesz, hiszen.

$$\pi_K^{2n} M \cdot M \subset \pi_K^{2n} \mathcal{O}_L \subset \pi_K^n \pi_K^{n-N} \pi_K^N \mathcal{O}_L \subset \pi_K^n M,$$

azaz szorzásra zárt. Ha $1 - \pi_K^n \cdot m \in V^n$ tetszőleges, $m \in M$, akkor $(1 - \pi_K^n \cdot m)^{-1} = 1 + \pi_K^n (\Sigma_{i=1} m^i \cdot \pi_K^{n(i-1)}) \in V^n$, hiszen a végtelen sor részleges összegei mind M-ben lesznek és M zárt, tehát V^n valóban egy részcsoport. No de U_L / V^N véges és így $h(U_L/V^N) = 1$, azaz tovább redukáltuk a feladatot arra hogy $h(V^N) = 1$.

Ezt úgy mutatjuk meg, hogy belátjuk a $H^0(V^N) = H^{-1}(V^N) = 1$ egyenlőséget. Tekintsük a $\beta : M \to V^n / V^{n+1} : \beta(m) = 1 + \pi_K^n \cdot m \pmod{V^{n+1}}$ homomorfizmust. Ennek magja $\pi_K M$ és világos, hogy szürjektív, tehát

$$V^n / V^{n+1} \cong M / \pi_K \cdot M \cong \bigoplus \mathcal{O}_K / \mathfrak{m}_K \alpha^{\sigma^i},$$

ahol az utóbbi alakból könnyen látszik, hogy $H^0(V^n/V^{n+1}) = 1$ és mivel véges, ezért $H^{-1}(V^n/V^{n+1}) = 1$ is. Ahhoz, hogy megmutassuk, hogy $H^0(V^N) = 1$, bármely $a_0 \in \ker \sigma - 1$ elemet elő kell tudnunk állítani egy $b \in V^N$ elem normájaként. Mivel $H^0(V^N/V^{N+1}) = 1$, ezért létezik egy olyan $b_0 \in V^N$, hogy $a_1 := a_0 (N b_0)^{-1} \in V^{N+1}$. Látható, hogy szintén $a_1^\sigma = a_1$, ezt induktívan folytatva kapunk egy $b_i \in V^{N+i}$ sorozatot, melyre $a_0 (N(b_0 b_1 ... b_i))^{-1} \in V^{N+i}$. A $b_i \in V^{N+i}$ tulajdonság miatt $b_0 b_1 ... b_i$ egy Cauchy-sorozat lesz, és így konvergál egy b-hez, melyre $a_0 = N(b)$. A H^{-1} esete hasonlóan zajlik. □

Köszönetnyilvánítás

Szeretnék köszönetet nyilvánítani témavezetőmnek, Zábrádi Gergelynek, hogy megismertette és megszerettette velem az algebrai számelméletet, valamint, hogy segített a szakdolgozatom elkészítésében.

Irodalomjegyzék

[1] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1992. ISBN: 3-540-65399-6.

[2] Zábrádi G. *Algebrai számelmélet jegyzet*. Internetes jegyzet. Elérhető: https://zabradi.web.elte.hu/Jegyzetek/algszamjegyzet.pdf. 2020.

[3] J.S. Milne. *Class Field Theory (v4.03)*. Internetes jegyzet. Elérhető: www.jmilne.org/math/. 2020.

[4] G. B. Folland. *A Course in Abstract Harmonic Analysis*. CRC Press, 1995. ISBN: 0-8493·8490-7.

[5] S. Lang. *Algebra*. Springer-Verlag, 2002. ISBN: 038795385X.

[6] J. Segel. *Recountings, Conversations with MIT Mathematicians*. A K Peters/CRC Press, 2010. ISBN: 9781568817132.

[7] D. A. Cox. *Primes of the form x2+ny2*. John Wiley & Sons, 2013. ISBN: 978-1-118-39018-4.