Imaginárius kvadratikus testek Abel bővítései

Kiss Zsombor

May 26, 2023

1 Bevezetés

A Kronecker-Weber tétel alapján a racionális számok minden Abel bővítése előáll a körosztási testek egy részteste ként. Ezt felfoghatjuk úgy is hogy minden ilyen bővítést egy 'természetes' analitikus függvény, mégpedig ebben az esetben az exponenciális függvény speciális értékei, ebben az estben az egységgyökök, generálják. Kronecker Jügendtraum-ja (ifjú álma) azt feltételezi, hogy általános számtest esetében is léteznek más 'természetes' függvények, melyek hasonlóan generálják annak ábeli bővítéseit. A sejtést egyenlőre csak speciális esetekre igazolták, például a komplex kvadratikus testek esetében a komplex szorzás használatával.

A félévben a célom ezen tétel bizonyításának megértése és a szükséges háttértudás elsajátítása volt. A múlt félévben az elliptikus görbék komplex szorzásával foglalkoztam, így az akkor készült beszámolóban leírtakat, valamint egyéb tételeket az elliptikus görbékről adottnak veszek Silverman[5] és Washington[6] könyveire hivatkozva.

Ebben a félévben főként algebrai számtestek rendjeiről tanultam Neukirch[4] és Cox[1] könyveit követve, valamint az osztálytestelmélet főbb állításaival ismerkedtem meg Milne[2] online jegyzetéből, melyből a bizonyításokat egyenlőre mellőztem, hogy legyen időm az imaginárius kvadratikus testek ábeli bővítéseinek karakterizálását is megérteni Moreland[3] online elérhető papírját követve.

A tételek bizonyításait sajnos nincs elég helyem leírni, de a fontosabb ötleteiket megpróbáltam ismertetni, ahol azokat össze tudtam foglalni.

2 Algebrai számtestek rendjei

Legyen K egy algebrai számtest $\mathcal{O}_K$ egészekkel és egy adott $\alpha_1, ..\alpha_n$ bázissal $\mathbb{Q}$ felett és tekintsük az ezek által generált M $\mathbb{Z}$-modulust. Az imaginárius kvadratikus esetben ezek a rácsok $\mathbb{C}$ feletti elliptikus görbének felel meg melynek endomorfizmus gyűrűje $\{\alpha \in K | \alpha M \subseteq M\}$. Ha K általános számtest akkor be lehet látni, hogy ez a halmaz egy $\mathbb{Z}$-t tartalmazó gyűrű, valamint felhasználva azt, hogy M Noether azt, hogy ezek algebrai egészek és azt is, hogy létezik egy

egész szám, hogy $c \cdot \alpha_i \in M$, vagyis tartalmazza K egy bázisát. Ezt általánosítva definiáljuk a rendeket:

Definíció 1 *$\mathcal{O}$ rend K-ban, ha $\mathcal{O}_K$ egy egyet tartalmazó részgyűrűje, és tartalmazza K egy $\mathbb{Q}$ bázisát.*

Az említett motiváció mellett sok nagyon természetes gyűrű is rend lesz, amik gyakran az "első tippek" lennének $\mathcal{O}_K$-ra, például $\mathbb{Z}[\sqrt[n]{d}] \subset \mathbb{Q}(\sqrt[n]{d})$.

Kihasználva azt, hogy $\mathcal{O}$ ideáljainak metszete $\mathbb{Z}$-vel nem üres, így minden faktorgyűrű véges, megkapjuk a következőt:

Tétel 1 *$\mathcal{O}$ egy Noether integritási tartomány, melyben minden prímideál maximális, K hányadostesttel.*

A következő tételek nagyrésze minden ilyen gyűrűre igaz, de az némi problémát okoz, hogy ezek lezártja Dedekind gyűrű lesz a Noether tulajdonság igazolása miatt és azért mert nem mindig lesz igaz, hogy $\mathcal{O}$ lezártja egy végesen generált $\mathcal{O}$-modulus lesz. Azonban ha feltesszük, hogy $\mathcal{O}$ vagy egy rend, vagy egy rend lokalizációja akkor ezek egyértelműek, így ezt innentől fel is tesszük. A lokalizációk azért érdekesek, mert ha csak rendekre akarjuk bizonyítani a következő tételeket, a bizonyításaikban fel kell használni, hogy a korábbi tételek lokalizációkra is igazak.

Tétel 2 *Legyen A egy nem nulla ideál $\mathcal{O}$-ban, ekkor*

$$\mathcal{O}/A \cong \bigoplus_P \mathcal{O}_P/A\mathcal{O}_P$$

ahol P $\mathcal{O}$ prímideáljain fut végig.

Ez lényegében a kínai maradéktétel általánosítása, és a bizonyításának fő lépése is a kínai maradéktétel alkalmazása $A\mathcal{O}_P \cap \mathcal{O}$-kra.

Az egyik első kérdés ami felmerül az az, hogy az ideálok egyértelmű faktorizációja igaz marad-e rendekben és a válasz nem. Sőt, nem is lesz minden törtideálnak inverze.

Tétel 3 *Legyen A $\mathcal{O}$ egy törtideálja invertálható akkor és csak akkor, ha $A\mathcal{O}_P$ egy főideál minden P-re.*

Ezt viszonylag könnyű igazolni, ha észrevesszük, hogy ha A inverze létezik, akkor $\{x \in K | xA \subset \mathcal{O}\}$-nak kell lennie.

Definíció 2 *$\mathcal{O}$ Picard csoportja $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$, ahol $I(\mathcal{O})$ az invertálható törtideálok, $P(\mathcal{O})$ pedig a főtörtideálok csoportja.*

Vegyük észre, hogy az $\mathcal{O} = \mathcal{O}_K$ esetben ez az ideálosztálycsoport.

Tétel 4

$$I(\mathcal{O}) \cong \bigoplus_{\mathcal{P}} P(\mathcal{O}_{\mathcal{P}})$$

Ebben a tételben az izomorfizmust $A \to (A\mathcal{O}_{\mathcal{P}})_{\mathcal{P}}$ adja meg és a legnehezebb talán a szürjektivitást igazolni, amit a fenti általánosított kínai maradéktételre alapszik.

A következő tétel a kígyó lemma segítségével írja le a kapcsolatot $\mathcal{O}$ és integrális lezártja $\bar{\mathcal{O}}$ Picard csoportjai között.

Tétel 5

$$1 \to \mathcal{O}^* \to \bar{\mathcal{O}}^* \to \bigoplus_{\mathcal{P}} \bar{\mathcal{O}_{\mathcal{P}}}^*/\mathcal{O}_{\mathcal{P}}^* \to C(\mathcal{O}) \to C(\bar{\mathcal{O}}) \to 1$$

egy egzakt sorozat.

A fenti direkt összeg jellemzésére hasznos egy rend konduktora, $\mathcal{F}$, ami $\bar{\mathcal{O}}$ legnagyobb ideálja amit tartalmaz $\mathcal{O}$. A konduktor másik fontos tulajdonsága:

Tétel 6 *$\mathcal{O}$ egy $\mathcal{P}$ prímideálja invertálható akkor és csak akkor ha nem osztja $\mathcal{F}$-et. Valamint $\mathcal{P} \to \mathcal{P}\bar{\mathcal{O}}$ egy bijekció $\mathcal{O}$ és $\bar{\mathcal{O}}$ konduktort nem osztó prímjei közt.*

Speciálisan a konduktorthoz relatív prím ideálokra igaz az egyértelmű faktorizáció. Ezen felül a konduktor lehetővé teszi a fenti egzakt sorozatban lévő direkt összeg egy megfoghatóbb formáját, amit szintén az általánosított kínai maradéktételből lehet kihozni:

Tétel 7

$$\bigoplus_{\mathcal{P}} \bar{\mathcal{O}_{\mathcal{P}}}^*/\mathcal{O}_{\mathcal{P}}^* \cong (\bar{\mathcal{O}}/\mathcal{F})^*/(\mathcal{O}/\mathcal{F})^*$$

Ezt és az egzakt sorozatot használva konkrét esetekben könnyen kiszámolható egy rend ideálosztályszáma, ha a lezártjának osztályszámát ismerjük. Például tekintsük $K = \mathbb{Q}(\sqrt{-3})$-ban a $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ rendet. Ekkor $\mathcal{O}_K = \mathbb{Z}[(-1+\sqrt{-3})/2]$ és $\mathcal{F} = 2\mathcal{O}_K = 2\mathcal{O} + (-1+\sqrt{-3})\mathcal{O}_K$, továbbá az ideálosztályszám 1, de $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$, tehát $\mathcal{O}$-ban nincs egyértelmű faktorizáció. Valamint azt is látjuk, hogy $2\mathcal{O}$ invertálható, hiszen főideál, de nem relatív prím a konduktorhoz, tehát az egyértelmű faktorizáció még az invertálható ideálokra sem igaz.

A kvadratikus számtestek esetében $\mathcal{O}_K = \mathbb{Z}[\omega_K]$ ahol $\omega_K = \sqrt{d}$ vagy $(1+\sqrt{d})/2$ és a lehetséges rendek $\mathbb{Z}[f\omega_K]$ alakúak valamely $f \in \mathbb{Z}$-re, és ilyenkor a konduktor $f\mathcal{O}_K$. Továbbá igazolható az invertálható ideálok következő karakterizációja az ideálok generátorainak minimálpolinómjaival dolgozva:

Tétel 8 *Egy kvadratikus rend $\mathcal{O}$ törtideálja A pontosan akkor invertálható, ha $\mathcal{O} = \{x \in K | xA \subset A\}$.*

Most ha egy $\mathbb{C}$ feletti elliptikus görbére úgy gondolunk mint a $\mathbb{C}$-beli homeotetikus rácsok ekvivalencia osztályaira akkor látszik, hogy az $\mathcal{O}$ endomorfizmusgyűrűvel rendelkező görbék pont $\mathcal{O}$ invertálható ideálosztályainak felelnek meg.

3 Az osztálytestelmélet tételei

A következőkben egy számtest K prímjei alatt, annak ekvivalens valuációjainak 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 prímje ami nem ágazódik el. Ekkor ha adott egy $\mathcal{P}$ prím $\mathfrak{p}$ felett, akkor $\mathcal{P}$ dekompozíciós csoportja $D_{\mathcal{P}}$ 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:

Tétel 9 *Minden K számtestre létezik egy számtest L ami K legnagyobb Abel bővítése melyben egyetlen véges prím sem ágazódik el és K egyetlen valós beágyazása sem terjed ki L komplex beágyazásává. Erre bővítésre igaz, hogy az Artin leképzés egy izomorfizmust ad K ideálosztálycsoportja és a bővítés Galois csoportja közt. Ezt a testet hívjuk K Hilbert osztálytestének.*

Ebből kiindulva azt mondjuk, hogy egy végtelen prím elágazódik, 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. Ezért érdemes tekinteni 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.

Definíció 3 *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.

Definíció 4 *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.*

Fix K esetén a sugárosztálycsoport meghatározásában nagyon hasznos a következő tétel, amit a kígyó lemmából levezethető kernel-cokernel sorozat segítségével lehet bebizonyítani.

Tétel 10

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

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

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

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 következű analitikus definícióra:

Definíció 5 *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:

Tétel 11 ***Reciprocitás tétel*** *Legyen L egy Abel kiterjesztése 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:*

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

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

Tétel 12 ***Létezés tétel*** *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 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.

Tétel 13 ***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 esetleg véges kivételekkel. Amiből viszont ki lehet hozni, hogy K két Abel bővítése akkor és csak akkor része a másiknak, ha konduktora osztja a másikét.

Az osztálytestelmélet erejét igazolja, hogy a Kronecker-Weber tételt pár sorban lehet igazolni úgy hogy meghatározzuk a megfelelő körosztási testek Galois csoportjait és konduktorait, és a megfelelő sugárosztálycsoportokat.

Ha K egy komplex kvadratikus test, akkor a fentiekben tárgyalt rendek Picard csoportjai realizálhatók egy kongruencia csoportként, hiszen a konduktorhoz relatív prím elemek által generált ideálokkal faktorizálunk, amik tartalmazzák a $K_{f\mathcal{O}_K,1}$-et. A megfelelő bővítést a rend gyűrűosztálycsoportjának hívjuk.

4 Komplex kvadratikus testek Abel bővítései

Az első lépés a komplex kvadratikus testek Abel bővítéseinek meghatározásában bármely adott rend gyűrűosztálycsoportjának meghatározása. Ez már majdnem jó lesz, hiszen bármilyen adott modulusra tudunk találni egy f konduktorú rendet amire a modulus osztja az f-et. A probléma az, hogy a gyűrűosztálytest nem a teljes sugárosztálytest erre a modulusra.

Tétel 14 *Tegyük fel, hogy egy E elliptikus görbe komplex szorzással rendelkezik egy $\mathcal{O}$ renddel. Ekkor $K(j(E))$ az $\mathcal{O}$ gyűrűosztályteste.*

A bizonyítás fő ötlete az, hogy $Gal(\mathbb{C}|K)$ a következőképpen hat az $\mathcal{O}$ endomorfizmus gyűrűvel rendelkező elliptikus görbék j-invariánsain:

Tétel 15 *Legyenek A egy invertálható törtideál $\mathcal{O}$-ban és $\sigma \in Gal(\mathbb{C}|K)$ és H a gyűrűosztálytest, ekkor*

$$\sigma(j(A)) = j(S^{-1}A),$$

ahol S egy olyan törtideál melynek Artin szimbóluma σ megszorítása H-ra.

Ennek, a Chebotarev sűrűségtétel és az elliptikus görbék azon tulajdonságának segítségével, hogy bármely izogénia faktorizálható egy szeparábilis izogéniára és a Frobenius leképzés egy hatványára, bizonyítható (nem könnyen), hogy $H = K(j(A_1), ...j(A_m))$ ahol az A_i-k a Picard csoport reprezentánsai, vagyis az $\mathcal{O}$ endomorfizmus gyűrűjű elliptikus görbék.

Innen már viszonylag könnyebb $K(j(E))$ és $H = K(j(A_1), ...j(A_m))$ rendjét összevetni, amiből kijön a tétel.

A sugárosztálycsoport meghatározásához szükségünk lesz a Weber függvényre:

Definíció 6 *Legyen $P \in E$ egy pont egy elliptikus görbén (x, y) koordinátákkal megadva, ekkor a Weber függvény h-t a következő képpen definiáljuk:*

$$h = \begin{cases} g_2 g_3 x/\Delta & ha\ j(E) \neq 0, 1728 \\ g_2^2 x^2/\Delta & ha\ j(E) = 1728 \\ g_3 x^3/\Delta & ha\ j(E) = 0 \end{cases}$$

Így már kimondhatjuk a sugárosztálytesteket karakterizáló tételt:

Tétel 16 *Legyen K egy komplex kvadratikus test és $\mathfrak{m}$ egy modulus, amit azonosítunk $\mathcal{O}_K$ egy ideáljával hiszen K-nak nincsenek valós prímjei. Legyen $E = \mathbb{C}/A$, ahol A egy $\mathcal{O}_K$ ideál, ekkor E $\mathfrak{m}$-torziója $E[\mathfrak{m}] = \mathfrak{m}^{-1}A/A$ ami véges lesz. Ekkor K $\mathfrak{m}$-hoz tartozó sugárosztályteste $K(j(E), h(E[\mathfrak{m}]).)$*

Felhasznált irodalom

[1] D. A. Cox. *Primes of the Form x2 + ny2*. 2013.

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

[3] G. Moreland. *Class Field Theory for Number Fields and Complex Multiplication*. Elérhető: https://math.uchicago.edu/ may/REU2016/REUPapers/Moreland.pdf.

[4] J. Neukirch. *Algebraic Number Theory*. 1992.

[5] J. H. Silverman. *The Arithmetic of Elliptic Curves*. 1986.

[6] L. C. Washington. *Elliptic Curves - Number Theory and Crytography*. 2008.