Tábor Áron

Periódus-index problémák görbéken

Szakdolgozat
matematikus szak

Témavezető:
Szamuely Tamás
MTA Rényi Alfréd Matematikai Kutatóintézet

Eötvös Loránd Tudományegyetem
Természettudományi Kar
Matematikai Intézet
2011

Salát Máté emlékére

Köszönetnyilvánítás

Elsőként szeretnék köszönetet mondani témavezetőmnek, Szamuely Tamásnak, aki kurzusai során felkeltette bennem az érdeklődést a dolgozathoz kapcsolódó különböző területek iránt, és aki tanácsaival és megjegyzéseivel nélkülözhetetlen segítséget nyújtott a szakdolgozat elkészültéhez. A szakdolgozat nem jöhetett volna létre a nélkül az elméleti háttérismeret nélkül, amelyet az ELTE TTK Matematikai Intézet Algebra és Számelmélet Tanszékének oktatóitól tanultam, különösen Kiss Emiltől, Pelikán Józseftől és Fried Ervintől. Hálás lehetek barátaimnak a folyamatos biztatásért, illetve a formai megvalósítással kapcsolatos tanácsokért: ebben Backhausz Ágnestől, Gyenis Zalántól és Titkos Tamástól kaptam sok segítséget.

Tartalomjegyzék

Bevezetés

Tetszőleges k alaptest felett definiált algebrai görbék esetében felmerülhet a kérdés, hogy a görbének van-e k-racionális pontja, és ha nincs, akkor k milyen nagy bővítését kell vennünk, hogy találjunk pontot. Ez vezet el az X görbe *indexének* a definíciójához: ez a legnagyobb közös osztója azon véges bővítések fokának, amelyek fölött X-nek már van racionális pontja. Az index meghatározása azonban sokszor nehézségekbe ütközik, miközben egy hasonló mennyiség, a *periódus* kiszámolása egyszerűbb. Ehhez ismernünk kell a görbe *Picard-csoportjának* a fogalmát. Ha az X görbét a k egy rögzített $\bar{k}$ algebrai lezártja felett tekintjük, akkor értelmezhetjük a $\mathrm{Div}(\bar{X})$ divizorcsoportot mint az $\bar{X}$ pontjai által generált szabad Abel-csoportot. Ennek egy faktorcsoportja adja meg a $\mathrm{Pic}(\bar{X})$ Picard-csoportot, melynek tehát divizorosztályok az elemei, amiken (a görbe pontjain, illetve abból származóan a divizorokon való hatás alapján) természetes módon hat a k abszolút Galois-csoportja. A k-racionális divizorosztályok fokainak legnagyobb közös osztóját nevezzük az X $P(X)$ periódusának.

A definíciókból azonnal adódik, hogy a periódus az index osztója, ugyanis az indexet meghatározhatjuk a k-racionális divizorok fokainak legnagyobb közös osztójaként is. Komolyabb megfontolásokat igényel az, hogy további összefüggéseket állapíthassunk meg az index és a periódus között. Szakdolgozatom célja az erre vonatkozó eredmények áttekintése, illetve a bizonyítások megértéséhez szükséges elméleti felépítés bemutatása.

A dolgozatban szereplő tételek részben tetszőleges, részben p-adikus testek fölötti összefüggésekre vonatkoznak. Lichtenbaum 1968-as [2] cikkében belátta, hogy p-adikus testek fölötti elliptikus görbék esetében a periódus egyenlő az indexszel. Eredményét 1969-es [3] cikkében általánosította. Ebben egyrészt bebizonyította, hogy p-adikus test feletti tetszőleges görbe esetén az index egyenlő a periódussal vagy a periódus kétszeresével (és ez utóbbi csak bizonyos további feltétel teljesülése esetén állhat elő), másrészt tetszőleges test feletti görbék esetére is megállapított összefüggéseket: nevezetesen azt, hogy az index osztója a $2P(X)^2$ értéknek, ahol bizonyos feltételek mellett a 2-es szorzó el is hagyható. Lichtenbaum cikkeiben a Galois-kohomológia és

a Tate-dualitás módszereit használta.

A kutatás további iránya p-adikus testek esetében az volt, hogy a Lichtenbaum cikkében megadott feltételek mellett valóban létezik-e megfelelő görbe. Végül erre Sharif 2007-es [7] cikkében (amely a 2006-os PhD tézisén alapul) igenlő választ adott: a Lichtenbaum cikke által megengedett tetszőleges génusz, periódus és index értékekhez konstruált megfelelő görbét. Dolgozatomban bemutatom Lichtenbaum tételeinek bizonyításait, majd Sharif konstrukcióját. A bizonyítások az idézett cikkek gondolatmenetét követik.

A szakdolgozat a következőképpen épül fel. Az első fejezet áttekinti a p-adikus testek konstrukcióját, bevezeti a (későbbiekben a görbék kapcsán is használt) diszkrét értékelésgyűrűk fogalmát, továbbá ismerteti p-adikus testek bővítéseinek olyan tulajdonságait, amelyekre szükség lesz Sharif konstrukciója során. A második fejezetben összefoglalom az algebrai görbékkel kapcsolatos alapvető ismereteket, külön kitérve a nem algebrailag zárt testek felett definiált görbékkel kapcsolatos fogalmak értelmezésére, illetve a differenciálformák elméletére. Ebben a fejezetben definiálom pontosan a dolgozat szempontjából olyan kulcsfontosságú fogalmakat, mint a Picard-csoport, az index, a periódus, a génusz, továbbá felsorolom azokat a tételeket, amelyek a későbbi bizonyításokban szerepet játszanak. A harmadik fejezet a bizonyításokhoz szintén szükséges elméleteket ismerteti a centrális egyszerű algebrákkal, a Brauer-csoporttal és a Galois-kohomológiaval kapcsolatban. Az első három fejezetben csak az egyszerűbb, illetve a kifejezetten a dolgozat későbbi fejezeteihez szükséges, máshol kevésbé elérhető bizonyítások kerülnek ismertetésre, a további tételek bizonyításainál a megfelelő szakirodalomra hivatkozom.

A negyedik fejezet Lichtenbaum [3] cikkére épül: előbb tetszőleges, majd a p-adikus test feletti periódus-index feltételek bizonyítását ismerteti. A dolgozat utolsó fejezete az adott indexű és periódusú görbék konstrukcióját tartalmazza. Ehhez először ismertetem az elliptikus görbékről, a Tate-görbéről, illetve a görbék csavarásáról szóló definíciókat és tételeket, mivel ezek képezik a konstrukció alapját. Ezt követően Sharif cikke alapján előbb 1 génuszú, majd tetszőleges g érték mellett konstruálom meg a megfelelő görbét.

1. fejezet

A p-adikus testek

Az első fejezetben áttekintjük a p-adikus számtest Kürschák Józseftől származó konstrukcióját, továbbá bevezetjük a diszkrét értékelések és diszkrét értékelésgyűrűk fogalmát. Felidézünk a p-adikus testek bővítésére vonatkozó bizonyos ismereteket, az elágazási index és a nem elágazó bővítések definícióját. A fejezet zárásaként bebizonyítunk nem elágazó bővítésekre vonatkozóan egy lemmát, amelyet a későbbiekben az adott periódusú és indexű görbe konstrukciójánál fogunk felhasználni. A fejezethez Jean-Pierre Serre [5] könyvének I-II. fejezetét, továbbá Fried Ervin *Értékeléselmélet*, illetve Szamuely Tamás *Brauer-csoportok* című kurzusain elhangzottakat használom fel.

1.1. Értékelés, diszkrét értékelésgyűrű

A továbbiakban p legyen pozitív prímszám. A p-adikus számtest konstrukciójához először definiáljuk a p-adikus értékelést a racionális számokon.

1.1.1. definíció. *Legyen $q \in \mathbb{Q}^*$ nemnulla racionális szám. A q p-adikus értékelése legyen az a $v_p(q)$ egész szám, amire $q = \frac{a}{b}p^{v_p(q)}$, ahol a és b p-vel nem osztható egész számok.*

Az így kapott $v_p : \mathbb{Q}^* \to \mathbb{Z}$ értékelés kiterjeszthető a $v_p(0) = \infty$ értékkel, és triviálisan teljesíti az alábbi tulajdonságokat:

1.1.2. állítás. (1) $v_p(xy) = v_p(x) + v_p(y)$

(2) $v_p(x+y) \geq \min(v_p(x), v_p(y))$

(2′) *Sőt,* $v_p(x) \neq v_p(y) \Rightarrow v_p(x+y) = \min(v_p(x), v_p(y))$

Ez alapján definiálható a q szám p-adikus normája $\|q\|_p = e^{-v_p(q)}$ nemnegatív valós. Erre teljesülnek az alábbi normatulajdonságok:

(1) $\|xy\|_p = \|x\|_p\|y\|_p$

(2) $\|x+y\|_p \leq \max(\|x\|_p, \|y\|_p)(\leq \|x\|_p + \|y\|_p)$

A felsorolt tulajdonságok alapján definiálhatjuk általánosan egy K test értékelését:

1.1.3. definíció. *Egy K test diszkrét értékelésének nevezünk egy olyan $v : K \to \mathbb{Z} \cup \{\infty\}$ szürjektív leképezést, amelyre:*

(1) $v(x) = \infty \Leftrightarrow x = 0$

(2) $v(xy) = v(x) + v(y)$

(3) $v(x+y) \geq \min(v(x), v(y))$

Az is belátható az axiómák következményeképpen, hogy a (3) esetben egyenlőség áll fenn, ha x és y értékelései különböznek.

Az $\{x \in K : v(x) \geq 0\}$ elemek részgyűrűt alkotnak K-ban, ezt nevezzük a v értékeléshez tartozó O_v *diszkrét értékelésgyűrűnek (DVR).* Ebben az $M_v = \{x \in K : v(x) > 0\}$ elemek ideált alkotnak. $O_v \backslash M_v = \{x \in K : v(x) = 0\}$ alkotják O_v egységeit, tekintve hogy $v(1) = 0$ a multiplikativitás miatt, ami alapján $v(1/x) = -v(x)$, és így $x \in O_v$ akkor és csak akkor invertálható, ha $v(x) = 0$. Tehát O_v lokális gyűrű, melynek egyetlen maximális ideálját, M_v-t az ő *értékelésideáljának* nevezzük. M_v főideál, amelyet tetszőleges olyan π elem generál, amelyre $v(\pi) = 1$. Az O_v összes ideálját az $M_v^k = (\pi^k)$ főideálok adják meg. O_v tehát főideálgyűrű, továbbá $\bigcap_r M_v^r = (0)$, és minden $x \in K^*$ előáll $x = u\pi^{v(x)}$ alakban, ahol $u \in O_v \backslash M_v$. Az O_v/M_v test az értékeléshez tartozó *maradéktest.*

Az itt belátott tulajdonságok alapján fordított sorrendben, a DVR-ből kiindulva is definiálható az értékelés.

1.1.4. definíció. *Egy A gyűrűt diszkrét értékelésgyűrűnek nevezünk, ha olyan főideálgyűrű, amelynek egyetlen nemnulla prímideálja van.*

Mivel egy főideálgyűrű nemnulla prímideáljait az irreducibilis elemek generálják, ezért a definíció értelmében a diszkrét értékelésgyűrűben invertálható elemmel való szorzás erejéig egyértelmű π irreducibilis elem létezik. Az A nemnulla ideáljait a (π^n) ideálok adják meg, és minden $x \neq 0$ elem egyértelműen előírható $x = \pi^n u$ alakban megfelelő n természetes számmal és u egységgel. Az így kapott n szám az x értékelése, amely kiterjeszthető az A hányadostestére is, ahol a fentiek szerinti diszkrét értékelést adunk meg ezáltal, melyhez A lesz a megfelelő értékelésgyűrű és (π) az értékelésideál.

A következő lemma egy adott test különböző diszkrét értékeléseire vonatkozik.

1.1.5. lemma (Approximációs lemma). *Legyenek $v_1, v_2, \ldots, v_n$ a K test különböző diszkrét értékelései, továbbá $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ adott elemek. Ekkor minden $N > 0$-hoz létezik olyan $x \in K$, melyre $v_i(x - \alpha_i) > N$ teljesül minden i-re.*

Bizonyítás. [13]: VI.10. Theorem 18.

A következő lépésben a teljessé tétel konstrukciójához ismét normát definiálunk, majd ebből a Cauchy-sorozatok fogalma is értelmezhető:

1.1.6. definíció. *A v-hez tartozó normát ismét az $\|x\|_v = e^{-v(x)}$ egyenlőséggel definiálhatjuk.*

1.1.7. definíció. *(x_n) Cauchy-sorozat, ha* $\forall \varepsilon > 0 \quad \exists N > 0 \quad \forall n \geq N \quad \|x_n - x_{n+1}\|_v < \varepsilon$.

A Cauchy-sorozatok kommutatív gyűrűt alkotnak, amelyben a nullsorozatok ($\forall \varepsilon > 0 \quad \exists N > 0 \quad \forall n \geq N \quad \|x_n\|_v < \varepsilon$) ideált alkotnak.

1.1.8. definíció. *A K test v szerinti teljessé tételét a $K_v = \{$Cauchy-sorozatok$\}/\{$0-sorozatok$\}$ faktor adja meg. K_v-re kiterjed a $\|\cdot\|_v$ norma: $\|(x_n)\|_v := \lim_{n\to\infty} \|x_n\|_v$.*

A limesz létezik, hiszen az $\|x_n\|_v$ valós számok is Cauchy-sorozatot alkotnak. Mivel a faktorizáció nullsorozatokkal történik, ezért jóldefiniált a kiterjesztés, továbbá a normatulajdonságok megőrződnek a kiterjesztett normára is.

1.1.9. állítás. *K_v test.*

Bizonyítás. K_v egy nemnulla elemét reprezentál olyan Cauchy-sorozat, melyre $\|x_n\| > \varepsilon$ egy adott N-nél nagyobb n-ekre. Az ezen indexekre $\frac{1}{x_n}$-nel definiált sorozat megfelelő inverzet határoz meg. □

A következő állítások is teljesülnek a kiterjesztett normára (amely persze metrikát és topológiát is meghatároz K_v-n):

1.1.10. állítás. *$v = -\log \|\cdot\|_v$ diszkrét értékelést ad meg K_v-n.*

1.1.11. állítás. *K_v teljes a $\|\cdot\|_v$ normára nézve, és K sűrű K_v-ben.*

A fentiek speciális eseteként kapjuk meg a p-adikus számtestet. Ha $K = \mathbb{Q}$, és v a p-adikus értékelés, akkor K_v-t $\mathbb{Q}_p$-vel jelöljük. A hozzá tartozó értékelésgyűrűt $\mathbb{Z}_p$-vel jelöljük, és a p-adikus egészek gyűrűjének nevezzük. Az értékelésideált $\mathbb{Z}_p$-ben a p elem generálja (ahol értelemszerűen $\mathbb{Q}$ a konstanssorozat képeként ágyazódik be $\mathbb{Q}_p$-be). A $\mathbb{Z}_p/(p\mathbb{Z}_p)$ maradéktest $\mathbb{F}_p$, azaz a p elemű véges test lesz.

1.1.12. lemma. *$\mathbb{Z}_p$ a $\mathbb{Z}$ $\mathbb{Q}_p$-beli lezártja.*

Bizonyítás. $\mathbb{Z} \subseteq \mathbb{Z}_p$, hiszen $\forall x \in \mathbb{Z} \quad v_p(x) \geq 0$. Továbbá $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \|x\|_p \leq 1\}$ a zárt egységgömb $\mathbb{Q}_p$-ben, azaz zárt. Végül tetszőleges $[(x_n)] \in \mathbb{Z}_p$ approximálható egész elemekkel is, ugyanis $v_p(x_n) \geq 0$ miatt $x_n = \frac{a_n}{b_n}$, ahol a_n, b_n egészek és p nem osztja b_n-t. A $b_n y_n \equiv a_n \mod p^n$ kongruencia megoldható y_n-re, és erre

$$v_p(x_n - y_n) = v_p\left(\frac{a_n - b_n y_n}{b_n}\right) \geq n,$$

így $\|x_n - y_n\|_p \to 0$. □

1.1.13. következmény.

$$\forall r > 0 \quad \mathbb{Z}_p/(p^r\mathbb{Z}_p) \simeq \mathbb{Z}/(p^r\mathbb{Z})$$

Bizonyítás. A $\mathbb{Z} \subseteq \mathbb{Z}_p$ beágyazással megadható egy természetes $\mathbb{Z} \to \mathbb{Z}_p/(p^r\mathbb{Z}_p)$ leképezés, melynek magja $p^r\mathbb{Z}$. Másrészt a lemma miatt minden $x \in \mathbb{Z}_p$-hez létezik olyan $y_r \in \mathbb{Z}$, melyre $v_p(x - y_r) \geq r$, és így $x - y_r \in p^r\mathbb{Z}_p$, azaz ez a leképezés szürjektív is. □

Megjegyzés. A későbbiekben a p-adikus testek (és azok véges bővítései) fölötti görbékkel foglalkozunk, a periódus-index-problémára vonatkozó tételeket ilyen testek fölött mondjuk ki. Az állítások azonban ennél általánosabban, *lokális testek* fölött is igazak. Egy K testet lokális testnek nevezünk, ha egy teljes diszkrét értékelésgyűrű hányadosteste, amelyhez tartozó maradéktest véges.

A maradéktest végessége azzal ekvivalens, hogy K lokálisan kompakt a normából származó topológia szerint ([5]: II.1.1). Megmutatható, hogy a lokális testek a következő két típus valamelyikéből kerülnek ki: egy számtest teljessé tétele egy nem-arkhimédeszi normára nézve (ezek a $\mathbb{Q}_p$ p-adikus testek, illetve azok véges bővítései lesznek), vagy megfelelő prímhatvány q esetén a q elemű test feletti $\mathbb{F}_q((t))$ formális Laurent-sorok testje.

1.2. A p-adikus testek bővítései

A p-adikus test bővítéseire is kiterjeszthetők az értékelések. Ezek a bővítések nagy szerepet játszanak majd a megadott periódusú és indexű görbék konstrukciója során. Most ezeknek a bővítéseknek a legfontosabb tulajdonságait ismertetjük, illetve belátunk egy olyan lemmát, amit Sharif felhasznál cikkében. Előtte azonban felidézzük a teljes diszkrét értékelésgyűrűkre vonatkozó Hensel-lemmát, amelyre szükség lesz a későbbi gondolatmenetekben.

1.2.1. lemma (Hensel-lemma). *Legyen A teljes diszkrét értékelésgyűrű, amelynek $M = (\pi)$ a maximális ideálja. Legyenek $f \in A[x]$ és $a_0 \in A$ olyanok, amelyre $f(a_0) \equiv 0 \mod \pi$, és $f'(a_0) \not\equiv 0 \mod \pi$. Ekkor létezik olyan $a \in A$, melyre $f(a) = 0$, és $a \equiv a_0 \mod \pi$.*

Bizonyítás. Megfelelő elemet konstruálhatunk $\mathbb{Z}_p$-ben például a [6]: 2.2. lemma ismételt alkalmazásából származó approximációval ($k = 0$-val és n-re történő indukcióval az ottani jelölések szerint). Általános esetben hasonló módon működik a bizonyítás. □

1.2.2. tétel. *Legyen $K/\mathbb{Q}_p$ véges testbővítés, $[K : \mathbb{Q}_p] = n$. v_p-nek egyértelműen létezik $v_K : K \to \mathbb{Z} \cup \{\infty\}$ diszkrét értékeléssé kiterjesztése, K teljes a v_K normára nézve.*

Bizonyítás. Az egyértelműség abból az analízisből ismert tényből következik, hogy egy adott normára nézve teljes és lokálisan kompakt k test feletti véges dimenziós vektortér bármely két normája ekvivalens. A létezéshez pedig a

$$v_K(x) = \frac{1}{[K : \mathbb{Q}_p]} v_p(\mathrm{Nm}_{K/\mathbb{Q}_p}(x))$$

definició ad megfelelő kiterjesztést. □

Ahhoz, hogy a kiterjesztés a diszkrét értékelés korábbi definíciójának megfeleljen, megfelelő konstanssal kell szoroznunk. Ez nem változtat azon, hogy mely elemek tartoznak a hozzá tartozó értékelésgyűrűbe, illetve -ideálba, viszont úgy kell normálnunk, hogy a K-hoz tartozó értékelésideál generátor elemének legyen 1 az értékelése. Ettől kezdve persze maga az értékelés szigorúan véve nem lesz kiterjesztés, de a megfelelő értékelésgyűrűk továbbra is egymás kiterjesztései maradnak: $O_{v_p} = O_{v_K} \cap \mathbb{Q}_p$, és persze $M_{v_p} = M_{v_K} \cap \mathbb{Q}_p$. Ekkor azonban a $p \in \mathbb{Q}_p$ elem - amelyre persze $v_p(p) = 1$, és generálta M_{v_p}-t - nem feltétlenül lesz 1 értékelésű a bővítésben. Ez az alapja a következő definíciónak:

1.2.3. definíció. *v_K elágazási indexe az $e = v_K(p)$ érték. Legyen továbbá $\kappa = O_{v_K}/M_{v_K}$ a v_K értékelés maradékteste. Ez a v_p maradéktestének lesz véges bővítése. A $[\kappa : \mathbb{F}_p]$ fokot f-fel jelöljük.*

1.2.4. tétel. *Az iménti jelöléseket használva a következő állítás teljesül: $ef = n$.*

Bizonyítás. [5]: II.2. Corollary 1.

1.2.5. definíció. *A $K/\mathbb{Q}_p$ bővítést nem elágazónak nevezzük, ha $e = 1$.*

1.2.6. állítás. *Minden $n > 0$ esetén egyértelműen létezik $\mathbb{Q}_p$-nek nem elágazó n-edfokú bővítése, ez Galois-bővítés.*

Bizonyítás. Legyen $\kappa = \mathbb{F}_p[x]/(\bar{f})$, ahol $\bar{f} \in \mathbb{F}_p[x]$ n-edfokú irreducibilis szeparábilis polinom. Az $\bar{f}$ felemelhető egy $\mathbb{Z}_p$ feletti f polinomra, amelyre $f \mod p = \bar{f}$. Az f $\mathbb{Z}_p$ felett is irreducibilis, hiszen ha tényezőkre bomlana, az $\mathbb{F}_p$ felett is felbontást adna. A Gauss-lemma miatt ekkor $\mathbb{Q}_p$ felett is irreducibilis, így a $K = \mathbb{Q}_p[x]/(f)$ bővítés éppen megfelelő bővítés lesz. (Hiszen $[K : \mathbb{Q}_p] = [\kappa : \mathbb{F}_p] = n$ miatt a bővítés nem elágazó.)

Az egyértelműség a Hensel-lemma következménye, ugyanis tetszőleges nem elágazó bővítésben hasonlóan megkonstruálható az f szeparábilis polinom, melynek a lemma szerint lesz K-beli α gyöke. A $\mathbb{Q}_p(\alpha)$ az előzővel izomorf bővítés, továbbá a fokok egyenlősége miatt ez az egész K-t megadja.

A megadott bővítés valóban Galois, ugyanis ismét a Hensel-lemma többszöri alkalmazásával láthatjuk, hogy az $\mathbb{F}_{p^n}$-ben lineáris tényezőkre bomló $x^{p^n} - x$ polinom minden gyöke felemelhető (egymással inkongruens, így biztosan különböző) K-beli gyökre, tehát a megkonstruált bővítés nem lesz más, mint ennek a polinomnak a $\mathbb{Q}_p$ feletti felbontási teste. □

A továbbiakban p-adikus testen $\mathbb{Q}_p$-t vagy annak egy véges bővítését értjük, a későbbi tételeket ilyen alaptest fölött mondjuk ki, és a következő lemma is ilyen testre vonatkozik.

1.2.7. lemma. *Legyen F/K p-adikus testek véges, nem elágazó bővítése. Ekkor létezik olyan $t \in F$, melyre $F = K(t)$ és $\mathrm{Nm}_{F/K}(t) = 1$.*

Bizonyítás. Legyen $[F : K] = n$, legyen K maradékteste $\mathbb{F}_q$. A bővítés nem elágazó, így F maradékteste ekkor $\mathbb{F}_{q^n}$. Az $\mathbb{F}_{q^n}^* \to \mathbb{F}_q^*$ norma leképezés az $1 + q + q^2 + \cdots + q^{n-1} = \frac{q^n-1}{q-1}$-edik hatványra emeléssel egyezik meg. Ennek magja így legfeljebb ennyi elemből áll, míg a kép legalább $q - 1$ elemből áll. Tehát a norma szürjektív, és pontosan $q - 1$ elemű, a mag pedig egy $\frac{q^n-1}{q-1}$

rendű ciklikus csoport, melyet egy t' elem generál. Viszont ekkor $\mathbb{F}_{q^n} = \mathbb{F}_q(t')$, hiszen t' nem lehet benne $\mathbb{F}_q$ kisebb fokú bővítésében, mert akkor $t'^{q^d} = t'$ is teljesülne megfelelő $d|n$-re.

A $t'^{q^n-1} - 1 = 0$ egyenlőségből és a Hensel-lemmából következik, hogy t' felemelhető egy olyan $t \in F$ egész elemre, amelyre $t^{q^n-1} - 1 = 0$, és amelynek a maximális ideál szerinti képe a maradéktestben t'. A bővítés nem elágazó, ezért - mivel t is egy n fokú bővítést generál - $F = K(t)$ teljesül. Végül belátjuk, hogy $\mathrm{Nm}_{F/K}(t) = 1$ is fennáll.

Egyrészt tetszőleges $\sigma \in \mathrm{Gal}(F/K)$ esetén $v_F(\sigma(x)) = v_F(x)$, hiszen $\mathrm{Nm}_{F/K}(x) = \mathrm{Nm}_{F/K}(\sigma(x))$, és a kiterjesztett értékelés csak a normától függ. Ebből az is következik, hogy $x \in O_{v_F}$ esetén $\sigma(x) \in O_{v_F}$, és $x \in M_{v_F} \Rightarrow \sigma(x) \in M_{v_F}$, továbbá $x_1 \equiv x_2 \mod M_{v_F}$ esetén $\sigma(x_1) \equiv \sigma(x_2) \mod M_{v_F}$ is teljesül. Emiatt a σ automorfizmus az M_{v_F} szerinti mellékosztályokon is automorfizmust ad meg, ezért az így kapott $\bar{\sigma}$ automorfizmusa lesz $\mathbb{F}_{q^n} = O_{v_F}/M_{v_F}$-nek. A bővítés nem elágazó volta miatt a rendek is egyenlőek, ezért $\langle\sigma\rangle = \mathrm{Gal}(F/K)$-ból $\langle\bar{\sigma}\rangle = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is következik. Ebből az is adódik, hogy egy adott $x \in O_{v_F}$ elem esetén $\bar{x}$-sal jelölve az ő maradéktestbeli képét, $\mathrm{Nm}_{F/K}(x)$ képe modulo M_{v_K} szerint éppen $\mathrm{Nm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\bar{x})$ lesz. Azaz, ha most $x \in K$ jelöli $\mathrm{Nm}_{F/K}(t)$-t, akkor $x \equiv 1 \mod M_{v_K}$, így $x = 1 + \pi y$ alakban is felírható, ahol $y \in O_{v_K}$ (és π az M_{v_K} maximális ideál egy generátora). Másrészt $t^{q^n-1} - 1 = 0$ teljesül t-re, és persze minden konjugáltjára is, így a konjugáltak szorzataként adódó normára is, azaz

$$x^{q^n-1} = (1 + \pi y)^{q^n-1} = 1.$$

Ezt kibontva

$$1 + (q^n - 1)\pi y + \pi^2 yz = 1$$

adódik egy megfelelő $z \in O_{v_K}$ elemmel. Persze $q^n \equiv 0 \mod M_{v_K}$, hiszen a maradéktest q-adrendű, azaz $\pi|q^n y$, amiből megfelelő $z' \in O_{v_K}$-val

$$-\pi y + \pi^2 yz' = 0$$

következik. Azaz

$$\pi y(-1 + \pi z') = 0,$$

és ebből pedig $\pi z' = 1$ lehetetlensége miatt (hiszen akkor $1 \in M_{v_K}$ is következne) $y = 0$ adódik, azaz valóban $\mathrm{Nm}_{F/K}(t) = 1$. □

2. fejezet

Algebrai görbék

Ez a fejezet azokat az alapvető algebrai geometriai fogalmakat és ismereteket tekinti át, melyekre szükség lesz a későbbiekben. Külön pontban tárgyaljuk a nem algebrailag zárt testek feletti görbék tulajdonságait, majd definiáljuk a periódus és az index fogalmát, amelyről a későbbiekben a főbb tételeket kimondjuk. A bevezető algebrai geometriai ismeretek kimondásához Szamuely Tamás előadásait és [10] cikkét, illetve Joseph H. Silverman [8] könyvét használom fel.

2.1. Algebrai geometriai alapfogalmak, görbék algebrailag zárt test fölött

Ebben a pontban legyen k algebrailag zárt test. Az *n-dimenziós affin tér pontjait* a k elemeiből álló pont-n-esek alkotják: $\mathbb{A}^n(k) = \{P = (x_1, x_2, \ldots, x_n) : x_i \in k\}$. A $k[X_1, X_2, \ldots, X_n]$ polinomgyűrű egy I ideáljához tartozó *affin zárt halmaznak* nevezzük és $V(I)$-vel jelöljük az I-beli polinomok közös nullhelyeinek ponthalmazát $\mathbb{A}^n(k)$-ban.

2.1.1. definíció. *Egy $V(I)$ affin zárt halmazt algebrai varietásnak nevezünk, ha I prímideál a $k[X_1, X_2, \ldots, X_n]$ polinomgyűrűben.*

Hilbert bázistétele miatt $k[X_1, X_2, \ldots, X_n]$ ideáljai végesen generáltak, azaz az affin zárt halmazok véges sok $f_1, f_2, \ldots, f_k$ közös nullhelyeiként is meghatározhatók. A Hilbert-féle Nullstellensatz következményeként kölcsönösen egyértelmű megfeleltetés van a polinomgyűrű radikálideáljai (amelyek megegyeznek saját radikáljukkal) és az affin zárt halmazok között. Emiatt $V(I)$ pontosan akkor áll egyetlen $(a_1, a_2, \ldots, a_n)$ pontból, ha I maximális ideál

(amely így $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ alakú). Az affin zárt halmazok valóban tekinthetők egy, az affin tér alaphalmazon definiált topológia zárt halmazainak, hiszen teljesítik a $V(IJ) = V(I) \cup V(J)$ és a $V(\sum I_k) = \bigcap V(I_k)$ összefüggéseket. Ezt a topológiát *Zariski-topológiának* nevezzük, az affin zárt halmazokat az altértopológiával látjuk el. Az *irreducibilis* affin zárt halmazok (melyek nem állnak elő két másik zárt halmaz uniójaként) pont a varietások. A következő fogalmak alapvető fontosságúak az algebrai geometriában:

2.1.2. definíció. *Az $X = V(I)$ affin varietáshoz tartozó koordinátagyűrűnek nevezzük az $O(X) = k[X_1, X_2, \ldots, X_n]/I$ faktorgyűrűt. A koordinátagyűrű $K(X)$ hányadosteste az X függvényteste, amelynek transzcendenciafoka az X dimenziója. Az egydimenziós affin varietások az affin görbék.*

Legyen $P = (a_1, a_2, \ldots, a_n)$ az n-dimenziós affin tér egy pontja, és legyen $P \in X$ egy $X = V(I)$ affin varietásra. Jelölje M_P az $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ ideál képét a koordináta-gyűrűben, amely maximális ideál (hiszen az $O(X)/M_P$ faktorból k-ba izomorfizmust ad meg az $f \to f(P)$ leképezés). Az X P-beli *lokális gyűrűjének* nevezzük az $O(X)$ M_P szerinti $O_{X,P}$ lokalizáltját, azaz az $O(X) \setminus M_P$ multiplikatívan zárt részhalmaz szerinti hányadosgyűrűt. Ez olyan f/g racionális függvényekből áll, amelyekre $g(P) \neq 0$, továbbá f_1/g_1 és f_2/g_2 ekvivalens, ha $f_1 g_2 - f_2 g_1 \in I$. Egy $F = f/g \in O_{X,P}$ elemre ezek szerint jóldefiniált az $F(P) = f(P)/g(P)$ függvényérték.

Projektív görbék. Elsőként az *n-dimenziós projektív tér* ($\mathbb{P}^n(k)$) pontjait definiáljuk. Ez $\mathbb{A}^{n+1}(k) \setminus \{(0, 0, \ldots, 0)\}$ azon reláció szerinti ekvivalenciaosztályaiból áll, amely szerint ekvivalensnek tekintjük az $(x_0, x_1, \ldots, x_n)$ és az $(y_0, y_1, \ldots, y_n)$ pontokat, ha létezik olyan $\lambda \in k^*$, melyre $x_i = \lambda y_i$ minden $0 \leq i \leq n$-re. Egy ekvivalenciaosztályt $[x_0, x_1, \ldots, x_n]$-nel jelölünk, ahol az x_i-ket a megfelelő $\mathbb{P}^n(k)$-beli pont *homogén koordinátáinak* nevezzük. $\mathbb{P}^n(k)$ egy X részhalmazát *projektív zárt halmaznak* nevezzük, ha $X = V(I)$ valamely I *homogén* ideálra a $k[X_0, X_1, \ldots, X_n]$ polinomgyűrűre (ami azt jelenti, hogy egy $f \in I$ polinomra annak minden homogén komponense is I-beli). Az affin esethez hasonlóan *projektív varietásnak* hívjuk azon projektív zárt halmazokat, amelyeket meghatározó I prímideál a polinomgyűrűben. Ahogy az affin esetben, most is definiálható a koordinátagyűrű a polinomgyűrű I ideál szerinti faktoraként.

Az n-dimenziós affin tér természetes módon beágyazható az n-dimenziós projektív térbe: minden $0 \leq i \leq n$-re $\varphi_i : \mathbb{A}^n(k) \to \mathbb{P}^n(k)$ jelölje azt a leképezést, amely az $(y_1, \ldots, y_n)$ pontot az $[y_1, \ldots, y_{i-1}, 1, y_i, \ldots, y_n]$ ekvivalencaosztályba viszi. Ez a leképezés bijekciót határoz meg $\mathbb{A}^n(k)$ és $\mathbb{P}^n(k) \setminus V(X_i)$ között, ahol $\varphi_i^{-1}([x_0, x_1, \ldots, x_n]) = (\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i})$. Legyen

$X = V(I) \subseteq \mathbb{P}^n(k)$ projektív zárt halmaz. Ekkor $X \cap \mathbb{A}^n$ (ami alatt $\varphi_i^{-1}(X \cap (\mathbb{P}^n \setminus V(X_i)))$-t értjük) affin zárt halmazt határoz meg, melyet az I ideálhoz tartozó f polinomok $f(X_1, \ldots, X_{i-1}, 1, X_i, \ldots, X_n)$ *dehomogenizáltjainak* a közös nullhelyeiként kaphatunk meg. Ezt az affin zárt halmazt $X^{(i)}$-vel is jelöljük. Az eljárás másik iránya is hasonlóan működik: egy d-edfokú g polinom *homogenizáltjának* nevezzük az $X_i^d g\left(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}\right)$ homogén polinomot. Ha most $X = V(I)$ egy affin zárt halmaz, akkor az így kapott homogenizált polinomok által generált homogén ideálhoz tartozó projektív zárt halmazt az X *projektív lezártjának* nevezzük.

Ez alapján a projektív varietások helyett a sokszor könnyebben kezelhető affin koordinátákkal megadott alakot vizsgálhatjuk. Ennek segítségével definiálható a lokális gyűrű, a függvénytest és a dimenzió fogalma projektív varietásokra. Egy X projektív varietás bármely P pontjához található olyan $X^{(i)} = X \setminus (X \cap V(X_i))$ affin varietás, melyre $P \in X^{(i)}$. Ennek $O_{X^{(i)},P}$ lokális gyűrűjét az X *P-beli lokális gyűrűjének*, $K(X)$ függvénytestét az X *függvénytestének*, dimenzióját az X *dimenziójának* nevezzük. Ezek a fogalmak függetlenek a megfelelő X_i koordináta választásától. Az egydimenziós projektív varietások a *projektív görbék*. A számláló és a nevező azonos fokú polinomra történő homogenizálása után a lokális gyűrű és a függvénytest elemeit homogén polinomok hányadosának is tekinthetjük. A függvénytest egy $f \in K(X)$ elemét *regulárisnak* mondjuk a $P \in X$ egy környezetében, ha $f \in O_{X,P}$.

Racionális leképezések. Legyenek X_1 és $X_2 \subseteq \mathbb{P}^n$ projektív varietások. Egy $\varphi = [f_0, f_1, \ldots, f_n]$ $K(X_1)$-beli elemekből álló függyvény $(n+1)$-est *racionális leképezésnek* nevezünk, ha azon $P \in X_1$ pontokra, amelyekben minden f_i értelmezett, $\varphi(P) = [f_0(P), f_1(P), \ldots, f_n(P)] \in X_2$. A φ racionális leképezést *regulárisnak* nevezzük a $P \in X_1$ pontban, ha létezik olyan $g \in K(X_1)$, amelyre minden gf_i reguláris P-ben, és valamelyik nem tűnik el. Ha ilyen g létezik, akkor $\varphi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]$-ként megkapható (ami a racionális leképezés definíciója szerint szükségképpen X_2 pontja). Egy racionális leképezést, amely minden pontban reguláris, *morfizmusnak* nevezünk.

A $\varphi : X_1 \to X_2$ racionális leképezés által *indukált* φ^* *homomorfizmus* alatt azt a $K(X_2) \to K(X_1)$ természetes homomorfizmust értjük a függvénytestek között, amelyre $\varphi^*(f) = f \circ \varphi$ minden $f \in K(X_2)$ esetén. Ez az indukált leképezés beágyazás, ha $\varphi(X_1)$ sűrű X_2-ben. Az ilyen leképezést *biracionális leképezésnek* nevezzük, ha létezik $\psi : X_2 \to X_1$ racionális leképezés, melynek képe sűrű X_1-ben, és $\varphi \circ \psi = \mathrm{id}_{X_2}$, illetve $\psi \circ \varphi = \mathrm{id}_{X_1}$ a regularitási tartományukban. Ilyen esetben X_1-t és X_2-t *biracionálisan izomorfnak* nevezzük. Ez pontosan akkor teljesül, ha $K(X_1) \cong K(X_2)$.

Sima görbék.

2.1.3. definíció. *Az $X = V(I)$ affin varietást simának (vagy nemszingulárisnak) nevezzük a P pontjában, ha az I ideált generáló $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ polinomokra a*

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{1\le i\le m, 1\le j\le n}$$

parciális deriváltakból álló $m \times n$-es mátrix rangja $n - \dim X$. X sima (vagy nemszinguláris), ha minden pontjában sima.

A P-beli lokális gyűrű M_P maximális ideáljára az M_P/M_P^2 faktor véges dimenziós vektortér $O_{X,P}/M_P \cong k$ felett. A P pontbeli simaság a következő állítás alapján meghatározható ennek segítségével is ([8]: I.1.7.):

2.1.4. állítás. *Az X affin varietás P pontja akkor és csak akkor sima, ha* $\dim M_P/M_P^2 = \dim X$.

Egy X projektív varietás sima a P pontjában, ha a megfelelő $P \in X^{(i)}$ affin varietás sima P-ben. (Ez független az $X^{(i)}$ választásától.) Az állítás szerint a projektív görbe sima egy P pontjában, ha M_P/M_P^2 k fölötti dimenziója 1. Ilyenkor M_P főideál $O_{X,P}$-ben, melyet egy t elem generál. Ebben az esetben a lokális gyűrű minden f eleme előállítható formális hatványsor alakjában: $f - f(P) = f_1 t$ valamely $f_1 \in O_{X,P}$-vel, és az eljárás folytatható egy $f = f(P) + f_1(P)t + f_2(P)t^2 + \ldots$ előállításra. Ezzel $O_{X,P}$ homomorfizmusát adhatjuk meg a $k[[t]]$ formális hatványsorgyűrűbe, amely homomorfizmus beágyazás lesz, hiszen a magját a $\cap(t^n)$ adja meg, ez a metszet pedig triviális. Ellenkező esetben ugyanis végtelen $a_1 = ta_2$, $a_2 = ta_3$, stb. sorozat létezne, és így $(a_1) \subset (a_2) \subset (a_3)$ ideálok szigorúan növő (hiszen t nem lehet egység) végtelen láncát alkotná, ami ellentmondana $O_{X,P}$ Noetherségének. Ebből az is következik, hogy az $O_{X,P}$ nemtriviális ideáljai pontosan az $M_P^n = (t^n)$ ideálok. Ezek szerint minden $f \in O_{X,P}$ előállítható $f = ut^n$ alakban, ahol u egység a lokális gyűrűben, n pedig természetes szám. A hányadostestre is kiterjesztve ezt az előállítást (ahol n már negatív egész is lehet), látható, hogy így egy v_P diszkrét értékelést határoztunk meg $K(X)$-en, $O_{X,P}$ pedig az ehhez tartozó diszkrét értékelésgyűrű. Azt mondjuk, hogy az $f \in K(X)$ függvénynek *n-szeres gyöke* van P-ben, ha $v_P(f) = n > 0$, és *n-edrendű pólusa*, ha $v_P(f) = n < 0$. Ebben az esetben a $t^n f$ függvény már reguláris P-ben, így f formális Laurent-sorba fejthető. A t generátorelemet *lokális paraméternek* nevezzük (ami egységgel való szorzás erejéig egyértelmű).

2.1.5. állítás ([8]: II.1.2.). *Legyen X sima görbe, $f \in K(X)^*$. Ekkor f-nek X véges sok pontjában lehet gyöke vagy pólusa. Ha X sima projektív görbe és f mindenütt reguláris, akkor konstans.*

Az X_1 sima projektív görbéből tetszőleges X_2 projektív varietásba képező $\varphi = (f_0, f_1, \ldots, f_n)$ racionális leképezés morfizmus, hiszen a P pontban a $t^{-n} f_i$ minden i-re reguláris, nem mind 0 függvényeket ad meg az $n = \min v_P(f_i)$ választással. Ha X_1 sima, X_2 pedig tetszőleges projektív görbe, és φ nemkonstans racionális leképezés, akkor az indukált φ^* homomorfizmus $K(X_2)$ beágyazását adja meg $K(X_1)$-be, $K(X_1)$ továbbá $\varphi^*(K(X_2))$ véges bővítése ([8]: II.2.4.), a $[K(X_1) : \varphi^*(K(X_2))]$ fokot pedig a φ *leképezés fokának* nevezzük és $\deg \varphi$-vel jelöljük. A φ-t *szeparábilis* leképezésnek nevezzük, ha ez a testbővítés szeparábilis. Az ehhez a testbővítéshez tartozó norma segítségével a függvénytestek közt a másik irányban is definiálhatunk indukált homomorfizmust: $\varphi_* = (\varphi^*)^{-1} \circ \mathrm{Nm}_{K(X_1)/\varphi^*(K(X_2))}$ egy $K(X_1) \to K(X_2)$ leképezést határoz meg.

2.1.6. definíció. *Legyen $\varphi : X_1 \to X_2$ sima projektív görbék közti leképezés, legyen $P \in X_1$. A φ P-beli elágazási indexének nevezzük és $e_\varphi(P)$-vel jelöljük az*

$$e_\varphi(P) = v_P(\varphi^* t_{\varphi(P)})$$

egész számot, ahol $t_{\varphi(P)} \in K(X_2)$ a $\varphi(P)$-beli lokális paraméter. $e_\varphi(P) \geq 1$ egész szám. Azt mondjuk, hogy φ nem elágazó a P pontban, ha $e_\varphi(P) = 1$, továbbá φ-t nem elágazónak nevezzük, ha X_1 minden pontjában nem elágazó.

Az elágazási indexre a következő állítások teljesülnek ([8]: II.2.6.):

2.1.7. állítás. *Legyen $\varphi : X_1 \to X_2$ sima projektív görbék közti nemkonstans, szeparábilis leképezés.*

(1) *Minden $Q \in X_2$ esetén*

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi.$$

(2) *Véges sok $Q \in X_2$ kivételével a $\varphi^{-1}(Q)$ ősképek száma* $\deg \varphi$.

Divizorok.

2.1.8. definíció. *Az X sima projektív görbe* $\mathrm{Div}(X)$ *divizorcsoportjának nevezzük a görbe pontjai által generált szabad Abel-csoportot. Egy $D = n_1 P_1 + \cdots + n_r P_r$ divizor foka a* $\deg D = n_1 + \cdots + n_r$ *egész szám.*

A deg függvény értelemszerűen egy $\mathrm{Div}(X) \to \mathbb{Z}$ homomorfizmust határoz meg. A homomorfizmus magját a *nulladfokú divizorok* alkotják, ezek csoportját $\mathrm{Div}^0(X)$-szel jelöljük.

Tetszőleges $f \in K(X)\backslash\{0\}$-nek csak véges sok gyöke és pólusa lehet, ezért a gyökeiből és pólusaiból álló, multiplicitással súlyozott lineáris kombináció (ahol a gyökhelyek együtthatója pozitív, a pólusoké pedig negatív) divizort határoz meg. Ezt nevezzük az f *függvénydivizorának*, és $\mathrm{div}(f)$-fel jelöljük. Az f *gyök-*, illetve *pólusdivizorának* nevezzük, ha ebben csak a pozitív, illetve negatív együtthatójú tagokat tartjuk meg. Ha egy g függvény gyök- és pólushelyei megegyeznek f-fel, akkor az f/g mindenütt reguláris X-en, azaz csak (nemnulla) konstans lehet. A függvénydivizorok csoportja tehát $\mathrm{Div}(X)$ részcsoportja, amely a $K(X)^*/k^*$ faktorral izomorf. A valóságban ez a részcsoport $\mathrm{Div}_0(X)$-nek is része a következő állítás miatt ([8]: II.3.1.):

2.1.9. állítás. *Függvénydivizorok foka* 0.

2.1.10. definíció. *A D_1 és D_2 divizorokat lineárisan ekvivalensnek nevezzük, ha $D_1 - D_2$ függvénydivizor.* $\mathrm{Div}(X)$*-nek a függvénydivizorok szerint vett faktorcsoportja az X* $\mathrm{Pic}(X)$*-szel jelölt Picard-csoportja (vagy osztálycsoportja).*

Az előző állítás miatt a deg függvény értelmezhető a Picard-csoport elemeire is, mint az adott osztály elemeinek közös foka. $\mathrm{Div}_0(X)$-nek a függvénydivizorok szerinti faktorcsoportját $\mathrm{Pic}_0(X)$-szel jelöljük. Az eddigieket a következő (a későbbiekben gyakran használt) egzakt sorozatban foglalhatjuk össze:

$$1 \to k^* \to K(X)^* \xrightarrow{\mathrm{div}} \mathrm{Div}_0(X) \to \mathrm{Pic}_0(X) \to 0. \tag{2.1}$$

Legyen $\varphi : X_1 \to X_2$ sima görbék közti nemkonstans racionális leképezés. A függvénytestek közti φ^* és φ_* leképezésekhez hasonlóan definiálhatók a divizorcsoportok között is indukált leképezések:

2.1.11. definíció. *Jelölje φ^* azt a* $\mathrm{Div}(X_2) \to \mathrm{Div}(X_1)$ *leképezést, amely egy egyetlen pontból álló (Q) divizorhoz a*

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)(P)$$

divizort rendeli. Legyen φ_* az a $\mathrm{Div}(X_1) \to \mathrm{Div}(X_2)$ *leképezés, melynél (P) képe az egyetlen pontból álló $(\varphi(P))$ divizor. Mindkét esetben a definíció $\mathbb{Z}$-lineárisan kiterjed tetszőleges divizorra.*

2.1.12. állítás. *A következők teljesülnek ekkor:*

(1) $\deg(\varphi^* D) = (\deg \varphi)(\deg D)$ *minden* $D \in \mathrm{Div}(X_2)$ *esetén;*

(2) $\varphi^*(\mathrm{div} f) = \mathrm{div}(\varphi^* f)$ *minden* $f \in K(X_2)^*$ *esetén;*

(3) $\deg(\varphi_* D) = \deg D$ *minden* $D \in \mathrm{Div}(X_1)$ *esetén;*

(4) $\varphi_*(\mathrm{div} f) = \mathrm{div}(\varphi_* f)$ *minden* $f \in K(X_1)^*$ *esetén.*

Bizonyítás. [8]: II.3.6.

Végezetül a divizorok csoportján bevezethetjük azt a részben rendezést, melynek pozitív elemei azok a divizorok, melyek minden együtthatója pozitív. Így a divizorok segítségével is megfogalmazhatunk olyan feltételeket, hogy a függvénytest mely elemei rendelkeznek előírt helyeken megfelelő rendű gyökkel vagy pólussal. Pontosabban, egy adott D divizor esetén vezessük be az $L(D) = \{f \in K(X) : \mathrm{div}(f) + D \geq 0\}$ jelölést. Az $L(D)$ véges dimenziós vektortér lesz k fölött ([8]: II.5.2.), melynek dimenzióját a későbbiekben a Riemann–Roch-tétel segítségével fogjuk tudni meghatározni. A 2.1.5. állítás második részét ez alapján átfogalmazhatjuk az $L(0) = k$ alakra is. Adott D mellett $|D|$-vel jelöljük és a *D-hez tartozó teljes lineáris rendszernek* nevezzük azon pozitív divizorok halmazát, melyek lineárisan ekvivalensek D-vel. Ekkor $|D| = \{\mathrm{div}(f) + D : f \in L(D)\}$. Mivel $\mathrm{div}(f)$ és $\mathrm{div}(g)$ pontosan akkor egyezik meg, ha $f = cg$ valamely nemnulla konstanssal, ezért $|D|$ az $L(D)$ egydimenziós altereiből álló, $\dim L(D) - 1$ dimenziós projektív térrel azonosítható.

2.2. Görbék nem algebrailag zárt test fölött - index és periódus

Ha a korábbi definíciókat ki akarjuk terjeszteni nem algebrailag zárt test felett definiált görbék esetére, akkor azzal a problémával szembesülünk, hogy egy affin görbét (varietást, zárt halmazt...) nem tudunk értelemszerűen ponthalmaznak tekinteni. Az $x^2 + y^2 + 1$ polinom görbét definiál a $\mathbb{A}^2(\mathbb{C})$ affin térben, de ennek nincsenek valós koordinátájú pontjai. Ettől még az $O(X) = \mathbb{R}[x, y]/(x^2 + y^2 + 1)$ koordinátagyűrű értelmes, továbbá $\mathbb{C}$-vel tenzor szorozva megkapjuk a $\mathbb{C}$ felett definiált görbe koordinátagyűrűjét. A koordinátagyűrű maximális ideáljai $\mathbb{R}$ felett nem feleltethetők meg pontoknak, például az $(x^2 + 1, y)$ lesz egy maximális ideál, ami persze $\mathbb{C}$ felett nem maximális ideál: az $(x - i, y)$ és $(x + i, y)$ ideálok tartalmazzák, melyekhez

az $\{(i,0),(-i,0)\}$ konjugált pontpár tartozik. A koordinátagyűrű maximális ideál szerinti faktora nem feltétlenül az alaptest lesz, például az iménti esetben az $O(X)/(x^2+1,y) \cong \mathbb{C}$. Ez azzal van összhangban, hogy az (x^2+1,y) maximális ideál a görbe komplex test fölött definiált alakjában jelenik meg az affin tér pontjaként. Ezen észrevételek pontos kifejezéséhez vezessük be az alapfogalmakat tetszőleges test fölött definiált görbékre is.

Legyen k tökéletes test, $\bar{k}$ egy rögzített algebrai lezártja. (A tökéletességre vonatkozó feltétel inkább technikai, így a szeparábilis lezárt helyett az algebrai lezárttal dolgozhatunk. A minket a későbbiekben érdeklő esetekben ez teljesülni fog.) Jelölje $G = \mathrm{Gal}(\bar{k}/k)$ a bővítés Galois-csoportját. A $\mathbb{A}^n(\bar{k})$ tér *k-racionális pontjainak* nevezzük az

$$\mathbb{A}^n(k) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n(\bar{k}) : x_i \in k\}$$

halmazt. A Galois-csoport hatását természetes módon értelmezhetjük $\mathbb{A}^n(\bar{k})$-n: minden $\sigma \in G$ és $P = (x_1, \ldots, x_n) \in \mathbb{A}^n(\bar{k})$ esetén

$$P^\sigma = (x_1^\sigma, \ldots, x_n^\sigma).$$

Ekkor a k-racionális pontok éppen a $\{P \in \mathbb{A}^n(\bar{k}) : P^\sigma = P \quad \forall \sigma \in G\}$ feltételt teljesítők lesznek. Jelölje $k(P)$ a $k(x_1, \ldots, x_n)$ testbővítést, ez a legkisebb olyan k fölötti bővítést adja meg, melyre a P pont racionális.

Azt mondjuk, hogy az $X = V(I)$ affin zárt halmaz k *fölött definiált*, ha az I ideál generálható $k[X_1, \ldots, X_n]$-beli polinomokkal. Ilyenkor $X(k)$-val is jelöljük az X k-racionális pontjait, azaz $X(k) = X \cap \mathbb{A}^n(k)$. Egy $f \in k[X_1, \ldots, X_n]$ polinomon a G Galois-csoport az $f(P^\sigma) = f(P)^\sigma$ képlet szerint hat, ezért a k fölött definiált X k-racionális pontjai a $\{P \in X : P^\sigma = P \quad \forall \sigma \in G\}$ halmazként is megkaphatók. Az X k fölötti koordinátagyűrűjét értelmezhetjük a $k[X_1, \ldots, X_n]/(I \cap k[X_1, \ldots, X_n])$ faktorgyűrűként, ennek hányadosteste lesz a k feletti függvénytest. A dimenziót a korábbiakhoz hasonlóan definiálhatjuk. A továbbiakban az egyértelműség kedvéért X-szel a k felett tekintett (ami mint a bevezetőből kiderült, ezúttal nem azonosítható az $X(k)$-val jelölt k-racionális pontok halmazával), míg $\bar{X}$-sal az algebrai lezárt felett értelmezett affin zárt halmazt jelöljük. Ily módon megkülönböztethetjük az $O(X)$ és $O(\bar{X})$ koordinátagyűrűket, illetve a $K(X)$ és $K(\bar{X})$ függvénytesteket is egymástól. Ha most egy $f \in K(\bar{X})$ elemén tekintjük a G Galois-csoport hatását (mint az együtthatókon vett hatást), akkor f^σ-val jelölve az f képét a $\sigma \in G$ elemnél, tetszőleges $P \in X$ pontra az $(f(P))^\sigma = f^\sigma(P)$ összefüggés teljesül. A k felett definiált görbék esetén $O(X)$ pontosan az $O(\bar{X})$-nek, míg $K(X)$ a $K(\bar{X})$-nek a G szerinti hatásnál vett fix elemeiből áll.

A projektív tér esetében k-racionálisnak nevezzük a $\{[x_0, x_1 \ldots, x_n] \in \mathbb{P}^n(\bar{k}) \quad \forall x_i \in k\}$ ekvivalenciaosztályok halmazát. Ebből persze nem következik, hogy egy k-racionális pont bármilyen felírása esetén csupa k-beli homogén koordinátából áll, csak annyi, hogy teszőleges felírás esetén ha az i indexre $x_i \neq 0$, akkor $x_j/x_i \in k$. Egy $P = [x_0, x_1, \ldots, x_n] \in \mathbb{P}^n(\bar{k})$ pontra $k(P)$-vel jelöljük a $k(x_0/x_i, \ldots, x_n/x_i)$ testbővítést (valamely $x_i \neq 0$ koordinátával), ez a legkisebb k-t tartalmazó bővítés, melyre P racionális. A Galois-csoport a homogén koordinátákon is hat: $[x_0, \ldots, x_n]^\sigma = [x_0^\sigma, \ldots, x_n^\sigma]$ tetszőleges $\sigma \in G$ esetén, ekkor $\mathbb{P}^n(k)$ éppen a $\{P \in \mathbb{P}^n(\bar{k}) : P^\sigma = P \quad \forall \sigma \in G\}$ pontokból áll, továbbá $k(P)$ a $\{\sigma \in G : P^\sigma = P\}$ részcsoport fixtestje. Az $X = V(I)$ projektív zárt halmazt az affin esethez hasonlóan k fölött definiáltnak nevezzük, ha I $k[X_0, \ldots, X_n]$ homogén polinomokkal generálható. Ebben az esetben is a k-racionális pontok halmaza az $X(k) = X \cap \mathbb{P}^n(k)$ metszettel kapható meg, mely ismét kifejezhető a Galois-csoport minden eleme által fixen hagyott pontok halmazaként is. Az affin esethez hasonlóan használjuk az X, $\bar{X}$, $O(X)$, $O(\bar{X})$, $K(X)$, $K(\bar{X})$ jelöléseket. $O(\bar{X})$ és $K(\bar{X})$ az $O(X) \otimes_k \bar{k}$, illetve $K(X) \otimes_k \bar{k}$ tenzorszorzattal kapható meg. Az X varietást *geometriailag összefüggőnek* nevezzük, ha az $\bar{X}$ is összefüggő. Ilyenkor a $K(\bar{X})$ test lesz (nem bomlik fel testek direkt összegére). A továbbiakban kizárólag geometriailag összefüggő görbékkel foglalkozunk.

Az eddigieknek megfelelően a $\varphi = [f_0, \ldots, f_n] : \bar{X}_1 \to \bar{X}_2$ racionális leképezésen is hat a G Galois-csoport: $\varphi^\sigma(P) = [f_0^\sigma(P), \ldots, f_n^\sigma(P)]$. Ekkor $\varphi(P)^\sigma = \varphi^\sigma(P^\sigma)$ teljesül. Ha létezik olyan $\lambda \in \bar{k}^*$, melyre $\lambda f_0, \ldots, \lambda f_n \in K(X_1)$, akkor azt mondjuk, hogy a φ leképezés is k fölött definiált.

Hátravan még a lokális tulajdonságok definiálása a nem algebrailag zárt test fölötti görbék esetére. Mint láttuk, az kevéssé tűnik értelmesnek, hogy csak a k-racionális pontokbeli lokális tulajdonságokkal foglalkozzunk, hiszen a korábbi példa esetében még pontja se lenne így a görbének. Ehelyett ésszerűnek tűnik a korábbi esetből kiindulva a koordinátagyűrű prímideáljaihoz kapcsolni a pontok fogalmát.

Legyen X affin görbe k fölött, az $O(X)$ ezek szerint k felett végesen generált, 1 transzcendenciafokú integritási tartomány. Ekkor $O(X)$ minden nemnulla prímideálja maximális ideál (ez Noether normalizációs lemmájának következménye, [11]: 4.1.12.). Az $O(X)$ prímideáljainak feleltetjük meg a pontokat: a (0) ideálhoz tartozó pontot az X *generikus pontjának* nevezzük, míg a többi - maximális ideálhoz tartozó - pontot *zárt pontnak*. Ez utóbbiak algebrailag zárt test felett éppen a szokásos pontokat határozzák meg, hiszen láttuk, hogy akkor egy $(X_1 - a_1, \ldots, X_n - a_n)$ maximális ideál egy $(a_1, \ldots, a_n)$ pontnak feleltethető meg. (Az elnevezés abból adódik, hogy az X-en vett Zariski-topológia rekonstruálható az $O(X)$ prímideáljainak halmazán megadott topologikus térből is, melynek nyílt halmazait a teljes tér,

továbbá azok a részhalmazok alkotják, melyek nem tartalmaznak egy adott $I \subset O(X)$ ideált. Minden nemüres nyílt részhalmaz tartalmazza a (0) ideálból álló pontot, ez a generikus pont. A többi pontot maximális ideálok alkotják, és egyelemű halmazként zárt részhalmazt alkotnak (hiszen komplementerük éppen az őt nem tartalmazó ideálok halmaza), ezek a zárt pontok. Ezzel a tulajdonsággal definiálhatók is az affin görbék, mint egy adott A k fölötti végesen generált, 1 transzcendenciafokú görbéhez tartozó (X, O_X) pár, ahol X topologikus tér, míg O_X az X-en reguláris függvények kévéje. Lásd: [11]: 4.3.)

Legyen M_P a P zárt ponthoz tartozó prímideál (és így maximális ideál) az $O(X)$-ben. Az $O_{X,P}$ lokális gyűrű értelmezhető, mint a koordinátagyűrű M_P szerinti lokalizáltja. (A (0) ideállal való lokalizálásnál a $K(X)$ függvénytestet kapjuk vissza.) Az $O(X)/M_P$ faktor a gyenge Nullstellensatz értelmében ezúttal a k egy véges testbővítése lesz, amit tekinthetünk úgy, mint a rögzített $\bar{k}$ algebrai lezárt résztestje. Az $X_1, X_2, \ldots, X_n$ koordinátafüggvények $O(X)$-beli képei ebben a faktorban valamely $a_1, a_2, \ldots, a_n$ elemeknek felelnek meg. Ekkor persze (hiszen az $O(X)$-et k felett generálják ezek az elemek) ez a testbővítés nem lesz más, mint a $k(a_1, \ldots, a_n)$, amit pedig a korábbi jelölésünkkel összhangban jelölhetünk $k(P)$-vel. (Ez lesz a legkisebb olyan testbővítése k-nak, melyben a P zárt pont racionális.) Az $\overline{M_P} = (X_1 - a_1, \ldots, X_n - a_n)$ maximális ideál lesz a $O(\bar{X})$-ben (illetve a $k(P)$ feletti koordinátagyűrűben), amely ideál az M_P által generált ideált tartalmazza. A G Galois-csoport hatásánál persze az $O(X)$ önmagára képződik, a $k(a_1^\sigma, \ldots, a_n^\sigma)$ pedig szintén $O(X)/M_P$-vel izomorf bővítés lesz, és az $\overline{M_P}^\sigma$ maximális ideál is M_P-t tartalmazza. Ezek a pontok adják meg a P feletti affin pontokat a $\mathbb{A}^n(\bar{k})$ térben, ezeknek az „ősképeknek" a száma pedig éppen $[G : \mathrm{Gal}(\bar{k}/k(P))] = [k(P) : k]$-val egyezik meg.

Projektív görbékre a korábbiak szerint járunk el: a nem algebrailag zárt test fölött definiált projektív tér is lefedhető a $\mathbb{P}^n(k) \setminus V(X_i)$-kkel azonosított, $n+1$ affin térrel. A $\mathbb{P}^n(k) \setminus V(X_i)$-ből $\mathbb{P}^n(k) \setminus V(X_j)$-be menő változótranszformáció az $(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i})$ pontot az $(\frac{x_0}{x_j}, \ldots, \frac{x_{j-1}}{x_j}, \frac{x_{j+1}}{x_j}, \ldots, \frac{x_n}{x_j})$ pontba viszi. A két koordinátagyűrű elemei között a korábban ismertetett homogenizálás, majd dehomogenizálás módszerével adhatunk meg izomorfiát, ez az izomorfia a maximális ideálokat maximális ideálokba viszi, így a projektív görbék esetében is definiálhatók a zárt pontok, mint valamely affin térkép zárt pontjai. A lokális gyűrűt az előzőek alapján értelmezhetjük. A nemszingularitást ezúttal a 2.1.4. állítás alapján definiálhatjuk: az X projektív görbe sima lesz a P-hez tartozó zárt pontjában, ha az M_P/M_P^2 dimenzió 1 lesz. Ilyenkor $O_{X,P}$ az algebrailag zárt esethez hasonlóan diszkrét értékelésgyűrű lesz. Az n-szeres gyök, az n-edrendű pólus és a lokális paraméter

tehát ugyanúgy értelmezhető ilyenkor is, továbbá a 2.1.5. és 2.1.7. állítások is érvényben maradnak.

Végül a divizorok a következőképpen értelmezhetők a nem algebrailag zárt test fölötti görbe esetében:

2.2.1. definíció. *Az X sima projektív görbe* $\mathrm{Div}(X)$ *divizorcsoportjának a görbe zárt pontjai által generált szabad Abel-csoportot nevezzük. Egy* $D = n_1P_1 + \cdots + n_rP_r$ *divizor foka a*

$$\deg D = \sum_{i=1}^{r} n_i[k(P_i) : k]$$

egész szám.

A $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ ismét homomorfizmus, melynek magját a nulladfokú divizorok $\mathrm{Div}_0(X)$ részcsoportja alkotja. A függvénydivizorok meghatározása, a Picard-csoport definiálása is hasonlóképpen történik, mint korábban.

Ha most $D = n_1P_1 + \cdots + n_rP_r \in \mathrm{Div}(\bar{X})$, akkor G értelemszerűen hat a divizorcsoporton is:

$$D^\sigma = \sum_{i=1}^{r} n_iP_i^\sigma.$$

2.2.2. állítás. *Egy* $D \in \mathrm{Div}(\bar{X})$ *divizor pontosan akkor lesz k feletti, ha* $D^\sigma = D$ *minden* $\sigma \in G$ *esetében, azaz* $\mathrm{Div}(\bar{X})^G \cong \mathrm{Div}(X)$.

Bizonyítás. Az állítás kimondása már magában rejti annak feltételezését, hogy X divizoraira tekinthetünk úgy is, mint $\bar{X}$ előző pont szerint definiált divizoraira. Valóban, ugyanis a $D = \sum n_iP_i \in \mathrm{Div}(X)$ megfeleltethető annak a divizornak, ahol a P_i zárt pont feletti, $\mathbb{A}^n(\bar{k})$-beli affin pontok jelennek meg az n_i együtthatókkal. Mivel ezeket az affin pontokat permutálják a Galois-csoport elemei, ezért egy Galois-invariáns divizort definiálunk így. Az ilyen ősképek száma $[k(P) : k]$, tehát ez a megfeleltetés megőrzi a divizor fokát.

A megfeleltetés homomorfizmus az Abel-csoportok között, melynek magja triviális, így injektív. Másrészt valóban minden G-invariáns divizor megadható így, hiszen a Galois-hatás szerint azonos orbitban szereplő pontoknak egyenlő együtthatóval kell szerepelniük, ezeket leválasztva pedig megkaphatjuk a megfelelő zárt pontokat. □

Megjegyzés. Az állításból persze nem következik, hogy a D-ben szereplő egyes pontok mind k-racionálisak, csak az, hogy a Galois-csoport megfelelően

permutálja ezen pontokat. A $\mathrm{Pic}(\bar{X})^G$ nem egyezik meg feltétlenül a $\mathrm{Pic}(X)$ csoporttal.

Ezt követően már definiálhatjuk az X sima projektív görbe periódusát és indexét:

2.2.3. definíció. *Az X $I(X)$ indexének nevezzük azt a legkisebb pozitív fokot, amelyre van k-racionális divizora. A* deg *leképezés a korábbiak szerint értelmezhető $\mathrm{Pic}(\bar{X}) \to \mathbb{Z}$ homomorfizmusként is, illetve ennek megszorítása a $\mathrm{Pic}(\bar{X})^G \to \mathbb{Z}$ homomorfizmus. A legkisebb olyan pozitív fokot, amelyre létezik k-racionális divizorosztály, az X $P(X)$ periódusának nevezzük.*

Az index tehát nem más, mint a $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ homomorfizmus képének $\mathbb{Z}$-beli indexe, azaz $\mathrm{Im}(\deg) = I(X)\mathbb{Z}$. A periódus pedig a $\overline{\deg} : \mathrm{Pic}(\bar{X})^G \to \mathbb{Z}$ homomorfizmus képének $\mathbb{Z}$-beli indexe. A k-racionális divizorok persze k-racionális divizorosztályban vannak benne, ezért a periódus az index osztója. Később további összefüggéseket állapítunk meg (általános esetben, illetve a p-adikus testek fölötti görbék esetén) az index és a periódus között.

Az alpont zárásaként belátunk egy lemmát arról, hogy két görbe közti véges fokú morfizmus esetén hogyan következtethetünk az indexre és a periódusra az egyik görbe megfelelő adatainak ismeretében. A bizonyítás a 2.1.12. állítás egyszerű következményeként adódik (amely állítás nem algebrailag zárt test felett is változatlanul igaz marad).

2.2.4. lemma. *Legyen $\varphi : X \to Y$ d fokú véges k-morfizmus két görbe között. Ekkor*

(1) *$P(Y)|P(X)$ és $I(Y)|I(X)$; továbbá*

(2) *$P(X)|dP(Y)$ és $I(X)|dI(Y)$.*

Bizonyítás. Tekintsük az indexekre vonatkozó állításokat, a periódusra hasonlóképpen történik a bizonyítás, csak a divizorcsoport helyett a Galois-invariáns divizorosztályokra kell az összefüggéseket alkalmazni. A 2.1.11. definícióban megadott $\varphi_* : \mathrm{Div}(X) \to \mathrm{Div}(Y)$ leképezés a 2.1.12. állítás szerint megőrzi a fokot, tehát Y-nak is van $I(X)$ k-racionális fokú divizora, amiből $I(Y)|I(X)$ azonnal adódik. Másrészt a $\varphi^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$ szintén a 2.1.12. állítás miatt d-vel szorozza a fokokat, így $I(X)|dI(Y)$. Mivel φ k fölött definiált morfizmus, így a k-racionális divizorok/divizorosztályok valóban megfelelő k-racionális elemekre képződnek φ_* és φ^* által. □

2.3. Differenciálformák görbéken

2.3.1. definíció. *Az X görbén vett differenciálformák tere (jele: Ω_X) az a $K(X)$-vektortér, melyet a dx szimbólumok generálnak ($x \in K(X)$), és teljesítik a szokásos relációkat:*

(1) $d(x+y) = dx + dy \quad \forall x, y \in K(X)$

(2) $d(xy) = xdy + ydx \quad \forall x, y \in K(X)$

(3) $da = 0 \quad \forall a \in k.$

Ha $\varphi : X_1 \to X_2$ nemkonstans leképezés két görbe között, akkor a korábban meghatározott $\varphi^* : K(X_2) \to K(X_1)$ indukált leképezés leképezést ad meg az $\Omega_{X_2} \to \Omega_{X_1}$ terek közt is, ahol

$$\varphi^* \left(\sum f_i dx_i \right) = \sum (\varphi^* f_i)\, d(\varphi^* x_i).$$

Ez alapján persze a differenciálformákat végtelen sok generátorral és relációval definiáljuk, ami kényelmetlenné teszi a kezelésüket. Szerencsére a következő tétel alapján többet mondhatunk erről a térről.

2.3.2. tétel. *A differenciálformák Ω_X tere egydimenziós $K(X)$-vektortér, melyet tetszőleges olyan dt elem generál, amelyre a $K(X)/k(t)$ véges szeparábilis bővítés.*

Bizonyítás. [8]: II.4.2.

Mivel az X görbe sima P pontjában vett $t \in K(X)$ lokális paraméter esetén a $K(X)/k(t)$ bővítés szeparábilis ([8]: II.1.4.), így ilyenkor meg is adhatunk ilyen dt generátort. Ha most X sima görbe, t pedig lokális paraméter a P pontban, akkor ω/dt-vel is jelölhetjük azt a $g \in K(X)$ függvényt, melyre $\omega = gdt$. A következő állítás segítségével a differenciálforma lokális tulajdonságait is értelmezhetjük:

2.3.3. állítás. *A $v_P(\omega/dt)$ érték nem függ a t lokális paraméter választásától, csak P-től és ω-tól, amit így az ω differenciálforma P-beli értékelésének (gyök vagy pólus multiplicitásának) is nevezhetünk és $v_P(\omega)$-val jelölhetünk. Ha f reguláris függvény a P pontban, akkor df/dt is reguláris P-ben.*

Bizonyítás. [8]: II.4.3.

Ezek szerint értelmezhető az $\omega \in \Omega_X$ differenciálformához tartozó divizor is. Mivel a differenciálformák egydimenziós $K(X)$-vektorteret alkotnak, ezért

azok divizorai egymástól csak függvénydivizorokban térhetnek el, tehát a Picard-csoport azonos mellékosztályában vannak. Ezt a mellékosztályt *kanonikus osztálynak*, a hozzá tartozó divizorokat *kanonikus divizoroknak* nevezzük. A kanonikus osztályt K_X-szel jelöljük. Ha $K = \mathrm{div}(\omega) \in K_X$, akkor az $L(K)$ vektortér azokat az $f \in K(X)$ függvényeket tartalmazza, melyre $\mathrm{div}(f) + \mathrm{div}(\omega) \geq 0$, azaz melyre $f\omega$ az egész X-en reguláris. $L(K)$ dimenzióját a görbe *génuszának (nemének)* nevezzük. A definíció alapján könnyen ellenőrizhető, hogy a $\mathbb{P}^1(k)$ projektív egyenes génusza 0, azaz nincsen rajta reguláris differenciálforma ([10]: 5.1. tétel utáni példa).

A kanonikus divizorokról az alapvető fontosságú Riemann–Roch-tétel ([8]: II.5.4.) alapján mondhatunk még többet:

2.3.4. tétel (Riemann–Roch). *Legyen X g génuszú sima projektív görbe, K egy kanonikus divizor rajta. Ekkor tetszőleges $D \in \mathrm{Div}(X)$ divizor esetén*

$$\dim L(D) - \dim L(K - D) = \deg D - g + 1.$$

A $D = K$ választással (mivel $L(0) = k$), illetve azt használva, hogy negatív D esetén $L(D)$ csak a 0-ból áll, adódnak a következő fontos észrevételek:

2.3.5. következmény. (1) $\deg K = 2g - 2$.

(2) *Ha* $\deg D > 2g - 2$, *akkor*

$$\dim L(D) = \deg D - g + 1.$$

A differenciálformákat most tetszőleges k test felett definiáltuk. Silverman könyve csak az algebrai lezárt felett definiálja $K(\bar{X})$-vektortérként a differenciálformák terét, de az állítások ugyanúgy érvényben maradnak a tetszőleges alaptest feletti geometriailag összefüggő görbe esetén is, a differenciálformák lezárt feletti $\Omega_{\bar{X}}$ tere megkapható a

$$K(\bar{X}) \underset{K(X)}{\otimes} \Omega_X$$

tenzorszorzattal. A Galois-csoport a függvények hatása alapján a differenciálformákon, illetve azok divizorain is hat. A k felett értelmezett differenciálformákat fixen hagyják a Galois-csoport elemei, így ezek divizorait is, tehát a kanonikus divizorok k-racionálisak lesznek.

A későbbi konstrukció során fontos lesz, hogy különböző görbék közti leképezés esetén következtethessünk egy görbe génuszára a másik génusz ismeretében. Ilyen kapcsolatot mond ki (nulla karakterisztikájú alaptest esetén) a *Riemann–Hurwitz-formula*:

2.3.6. tétel (Riemann–Hurwitz). *Legyenek Y, X sima projektív görbék egy nulla karakterisztikájú test fölött, és legyen $\varphi : Y \to X$ nemkonstans szeparábilis leképezés. Ekkor*

$$2g(Y) - 2 = (\deg \varphi)(2g(X) - 2) + \sum_{P \in Y} (e_\varphi(P) - 1).$$

Bizonyítás. [8]: II.5.9. A jobb oldalon lévő összegzés véges sok tagra történik, hiszen a 2.1.7. állítás értelmében véges sok $P \in Y$ pont kivételével az elágazási index 1. □

Példa. Az ebben a fejezetben ismertetett fogalmak használatát a következő egyszerű példán szemléltethetjük. Tekintsük az előző pont bevezetésében ismertetett példát, illetve ennek projektív térbeli változatát: a valós felett definiált $X_0^2+X_1^2+X_2^2 = 0$ egyenletű X görbét, illetve a komplex fölött ehhez tartozó $\bar{X}$-t. Az $X^{(2)}$ affin görbét az $x = \frac{X_0}{X_2}$ és $y = \frac{X_1}{X_2}$ függvényekkel tudjuk paraméterezni, és így kapjuk meg az $x^2+y^2+1 = 0$ képletet, amely az $[i, 1, 0]$ és $[-i, 1, 0]$ pontokkal kiegészülve adja meg a komplex feletti projektív görbe összes pontját. (Valós felett ez a két pont az $(X_0^2 + X_1^2, X_2)$ prímideálhoz tartozó egyetlen zárt pont alakjában áll elő.) A dx differenciálforma divizorát a következőképpen határozzuk meg: a 2.3.3. állítás értelmében dx reguláris mindenütt, ahol x reguláris, azaz pólusa csak az $[i, 1, 0]$ és $[-i, 1, 0]$ pontokban lehet. Ezekben a pontokban a $z = \frac{X_0}{X_1}$ és $w = \frac{X_2}{X_1}$-vel paraméterezhetünk, és persze $x = z/w$. Az $[i, 1, 0]$ pontbeli maximális ideál $(z-i, w)$ alakban áll elő, a görbe egyenlete $(z-i)(z+i)+w^2 = 0$ alakra hozható, amiből $z-i = w^2u$ alakra hozható, ahol u egység a lokális gyűrűben, w pedig lokális paraméter. Felhasználva, hogy $dz = d(z-i) = d(w^2u) = w^2du+2uwdw$ meghatározható dx:

$$dx = -z\frac{1}{w^2}dw + \frac{1}{w}dz = -\frac{z}{w^2}dw + wdu + 2udw.$$

Így dx-nek $[i, 1, 0]$-ban - és persze $[-i, 1, 0]$-ban is - másodrendű pólusa van. A $[\pm i, 0, 1]$ pontokat kivéve x lokális paraméter, tehát dx-nek nincs gyöke. Ezekben a pontokban pedig az $(x \mp i, y)$ alakú a lokális gyűrű maximális ideálja, és az $x \mp i = y^2u$ képletből (u a megfelelő egység) y lesz lokális paraméter, és ekkor $dx = d(x \mp i) = d(y^2u) = y^2du+2uydy$, azaz dx-nek ezekben a pontokban egyszeres gyöke van. Tehát a dx divizora $[i, 0, 1]+[-i, 0, 1]-2[i, 1, 0]-2[-i, 1, 0]$ $\mathbb{C}$ felett, míg $\mathbb{R}$ felett az első, illetve a második konjugált párok adják meg a megfelelő zárt pontokat. A divizor foka -2. Az $\bar{X}$ görbe pontjai paraméterezhetők a $\mathbb{P}^1(\mathbb{C})$ projektív egyenes pontjaival a következőképpen: a $[t, u] \in \mathbb{P}^1(\mathbb{C})$ pontnak megfeleltetjük a $[t^2 - u^2, 2tu, i(t^2 + u^2)]$

pontot. A leképezés inverzét az $[X_0, X_1, X_2] \mapsto [X_0 - iX_2, X_1]$ adja meg az $[i, 0, 1]$ pont kivételével, ahol viszont $[X_1, -X_0 - iX_2]$ alakban írhatjuk fel ugyanezt a morfizmust. (Az $\bar{X}$ többi pontjában a két leképezés megegyezik X eredeti képletéből következően.) Ezért $\bar{X} \cong \mathbb{P}^1(\mathbb{C})$, tehát X génusza 0, ami megfelel a Riemann–Roch-tétel állításának is ebben a speciális esetben.

3. fejezet

Brauer-csoport és Galois-kohomológia

A későbbi bizonyítások a Galois-kohomológia eszközére is építenek: ez homologikus algebrai módszereknek a Galois-csoport hatásán történő alkalmazását jelenti. Ez a fejezet bevezeti az ehhez szükséges fogalmakat, és felsorolja a legfontosabb használt állításokat. A centrális egyszerű algebrák vizsgálata vezet el a Brauer-csoport definíciójához, melyet egy megfelelő kohomológiacsoportként is megkaphatunk. A szükséges ismereteket Philippe Gille és Szamuely Tamás [1] könyve alapján tekintjük át. A fejezet utolsó pontjaként Lichtenbaum [2] cikke alapján belátunk egy tételt, amely összekapcsolja a Picard-csoport fogalmát az alaptest Brauer-csoportjával, és amely kulcsfontosságú lesz a periódusra és indexre vonatkozó tételek bizonyítása során.

3.1. Centrális egyszerű algebrák és a Brauer-csoport

Legyen k egy test, a továbbiakban k feletti véges dimenziós algebrákkal foglalkozunk.

3.1.1. definíció. *Az A k-algebra egyszerű, ha nincsen 0-n és A-n kívül (kétoldali) ideálja. A centrális, ha $Z(A) = k$.*

Minden ferdetest centrális egyszerű algebra a centruma felett. A Wedderburn-tétel szerint a véges dimenziós egyszerű k-algebrák izomorfak egy megfelelő $D \supseteq k$ ferdetest feletti $M_n(D)$ mátrixgyűrűvel, ahol D izomorfia erejéig egyértelmű. Ennek következtében egy algebrailag zárt k test felett minden centrális egyszerű algebra izomorf egy k feletti mátrixgyűrűvel. Általában a

következő tétel segítségével mondhatunk többet a centrális egyszerű algebrákról:

3.1.2. tétel. *A k test feletti A véges dimenziós k-algebra pontosan akkor centrális egyszerű, ha létezik olyan $n > 0$ egész és egy véges K/k testbővítés, melyre $A \otimes_k K$ az $M_n(K)$ mátrixgyűrűvel izomorf.*

Bizonyítás. [1]: 2.2.1.

Azt mondjuk, hogy a K/k bővítés *felhasítja* az A centrális egyszerű algebrát, ha $A \otimes_k K \cong M_n(K)$. A tétel következménye, hogy A k feletti dimenziója négyzetszám, melynek négyzetgyökét az A *fokának* nevezzük. Noether és Köthe tétele azt mondja ki, hogy az A centrális egyszerű k-algebrához létezik őt felhasító, k felett szeparábilis K/k bővítés is ([1]: 2.2.5.).

A centrális egyszerű algebrák további vizsgálatához szükséges a G csoport *első kohomológiahalmazának* fogalmát értelmezni.

3.1.3. definíció. *Tekintsük egy G csoport (balról történő) hatását egy másik A (nem feltétlenül kommutatív) csoporton (azaz egy $(\sigma, a) \mapsto \sigma(a)$ leképezést, melyre $\sigma(ab) = \sigma(a)\sigma(b)$ és $\sigma\tau(a) = \sigma(\tau(a))$ minden $\sigma, \tau \in G$ és $a, b \in A$ esetén). G egy 1-kociklusának nevezünk egy olyan A-értékű $\sigma \mapsto a_\sigma$ leképezést, melyre*

$$a_{\sigma\tau} = a_\sigma \cdot \sigma(a_\tau) \quad \forall \sigma, \tau \in G.$$

Az a_σ és b_σ 1-kociklusokat ekvivalensnek tekintjük, ha létezik olyan $c \in A$ elem, melyre $a_\sigma = c^{-1} b_\sigma \sigma(c)$ minden $\sigma \in G$ esetén. Az 1-kociklusok ezen ekvivalencia szerinti ekvivalenciaosztályait nevezzük a G első kohomológiahalmazának A-ban és $H^1(G, A)$-val jelöljük.

Általános esetben nincs csoportstruktúra definiálva ezen a halmazon, viszont az $a_\sigma \equiv 1$ triviális kociklusból származó elemet megkülönböztethetjük, az ilyen kitüntetett elemmel rendelkező struktúrát pedig *pontozott halmaznak* nevezzük.

Jelölje $CEA_K(n)$ a K felett felhasadó, n-edfokú centrális egyszerű k-algebrák izomorfiaosztályainak halmazát. Ebben kitüntetett elem maga az $M_n(k)$ mátrixgyűrű, tehát ezt is tekinthetjük pontozott halmaznak. A Galois-leszállás általános módszerével a $CEA_K(n)$ halmaz megfeleltethető a $\mathrm{PGL}_n(K)$ projektív általános lineáris csoporton vett kohomológiahalmaznak:

3.1.4. tétel. *Legyen K/k véges Galois-bővítés G Galois-csoporttal. Ekkor bijekció adható meg a $CEA_K(n)$ és a $H^1(G, \mathrm{PGL}_n(K))$ halmazok között, ami a két pontozott halmaz kitüntetett elemeit egymásnak felelteti meg (azaz mint pontozott halmazok izomorfak).*

Bizonyítás. [1]: 2.4.3.

Megmutatható, hogy ha A és B K felett felhasadó centrális egyszerű algebrák, akkor $A \otimes_k B$ is az ([1]: 2.4.4.), így a tenzorszorzás indukál egy $CEA_K(m) \times CEA_K(n) \to CEA_K(mn)$ leképezést. Ez az előző tétel alapján megfeleltethető egy $H^1(G, \mathrm{PGL}_n(K)) \times H^1(G, \mathrm{PGL}_m(K)) \to H^1(G, \mathrm{PGL}_{nm}(K))$ leképezésnek. Ha $n, m > 0$ egészek, akkor a $GL_n(K)$ mátrixcsoport injektíven beágyazható $GL_{nm}(K)$-ba (egy $M \in GL_n(K)$ mátrix képe az a blokkmátrix, melynek diagonálisában m példányban szerepel M és mindenütt máshol nullák vanak). Ez a beágyazás a projektív általános lineáris csoportok, illetve az azokon értelmezett kohomológiákon is indukál egy leképezést, ez a $\lambda_{mn} : H^1(G, \mathrm{PGL}_m(K)) \to H^1(G, \mathrm{PGL}_{nm}(K))$ persze ismét tekinthető a centrális egyszerű algebrák megfelelő izomorfiaosztályai közti leképezésnek, ahol az $A \in CEA_K(n)$ algebra képe az $A \otimes_k M_m(k)$ lesz. A Wedderburn-tétel következményeképpen (és a dimenziók összehasonlításából adódóan) a λ_{mn} leképezés injektív lesz minden $m, n > 0$ egész esetén. Ez vezet el a következő konstrukcióhoz:

3.1.5. definíció. *Az A és A' centrális egyszerű k-algebrákat Brauer-ekvivalensnek nevezzük, ha léteznek olyan m, m' egészek, mellyel $A \otimes_k M_m(k) \cong A' \otimes_k M_{m'}(k)$. Ez ekvivalenciarelációt ad meg a $\bigcup_n CEA_K(n)$ halmazon. Az ekvivalenciaosztályok alkotják a K/k bővítés $\mathrm{Br}(K/k)$-val jelölt relatív Brauer-csoportját. A $\mathrm{Br}(K/k)$ halmazoknak a k feletti K véges Galois-bővítésekre vett unióját $\mathrm{Br}(k)$-val jelöljük, és k Brauer-csoportjának nevezzük.*

A Wedderburn-tétel következtében minden Brauer-ekvivalenciaosztály egyértelműen reprezentálható egy D ferdetesttel, azaz $\mathrm{Br}(K/k)$ a K felett felhasadó ferdetestek osztályozásának is tekinthető. Továbbá ha A és B Brauer-ekvivalens centrális egyszerű k-algebrák, melyek k fölötti dimenziója megegyezik, akkor $A \cong B$.

A $\mathrm{Br}(K/k)$ és $\mathrm{Br}(k)$ halmazokat elláthatjuk az $(A, B) \mapsto A \otimes_k B$ leképezés által indukált szorzással. Ezzel a művelettel Abel-csoportot alkotnak. A kommutativitás és az asszociativitás a tenzorszorzás megfelelő tulajdonságaiból következik, az egységelem az $M_n(k)$ mátrixgyűrűk osztálya lesz. Az A algebra által reprezentált osztály inverzét az A^{op} *oppozitalgebra* osztálya adja meg: ez az algebra ugyanazon a vektortéren definiált, mint A, csak a szorzást az $(x, y) \mapsto yx$ leképezés határozza meg.

A $H^1(G, \mathrm{PGL}_n(K))$ csoportok n-re vett unióját a λ_{mn} beágyazások mentén $H^1(G, \mathrm{PGL}_\infty)$-nel jelöljük. Ezen már értelmezhető csoportművelet a korábban említett $H^1(G, \mathrm{PGL}_n(K)) \times H^1(G, \mathrm{PGL}_m(K)) \to H^1(G, \mathrm{PGL}_{nm}(K))$ leképezés segítségével. Ekkor $H^1(G, \mathrm{PGL}_\infty)$ is Abel-csoport, sőt $\mathrm{Br}(K/k) \cong H^1(G, \mathrm{PGL}_\infty)$.

A Brauer-csoport egy további meghatározásához definiálni kell a magasabb fokú kohomológiákat is, melyeket Abel-csoportokra fogunk csak értelmezni. Ezek használata viszont alapvető fontosságú lesz a későbbi bizonyítások során.

3.2. Galois-kohomológia

A csoportkohomológia technikájáról részletesebb ismertetés található pl. [1] 3. fejezetében. Itt csak a legfontosabb definíciók és tulajdonságok felidézésére szorítkozunk.

Legyen G egy csoport, amely (balról) hat egy A Abel-csoporton. A tekinthető egy $\mathbb{Z}[G]$ feletti balmodulusnak, ahol egy $\sum n_\sigma \sigma \in \mathbb{Z}[G]$ elem az $a \in A$-n a $\left(\sum n_\sigma \sigma\right) a = \sum n_\sigma \sigma(a)$ definíció szerint hat. $\mathrm{Hom}_G(A, B)$-vel jelöljük az olyan $A \to B$ Abel-csoportok közti homomorfizmusok halmazát, melyek kompatibilisek G hatásával, ezek természetes módon Abel-csoportot alkotnak (ezeket G-homomorfizmusnak nevezzük). A korábbiakhoz hasonlóan A^G-vel jelöljük a G-invariáns elemek részcsoportját A-ban.

Definiáljuk a $H^i(G, A)$ Abel-csoportokat, melyek a következő tulajdonságokat teljesítik:

(1) $H^0(G, A) = A^G$ minden A-ra.

(2) Minden $A \to B$ G-homomorfizmusra létezik egy $H^i(G, A) \to H^i(G, B)$ kanonikus leképezés.

(3) Ha adott G modulusok egy

$$0 \to A \to B \to C \to 0$$

rövid egzakt sorozata, akkor létezik Abel-csoportok egy végtelen hosszú egzakt sorozata ($i = 0$-val kezdve):

$$\cdots \to H^i(G, A) \to H^i(G, B) \to H^i(G, C) \to H^{i+1}(G, A) \to \ldots$$

Az ezeket a tulajdonságokat kielégítő csoportokat legegyszerűbben a homologikus algebra nyelvén adhatjuk meg: a definíció az Ext funktor speciális eseteként adódik.

3.2.1. definíció. *A G csoport i-edik kohomológiáját az A G-moduluson a következőképpen határozzuk meg:*

$$H^i(G, A) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A),$$

ahol $\mathbb{Z}$-n $\mathbb{Z}[G]$ triviális hatását tekintjük.

Részletesebb magyarázat a fogalmakról megtalálható pl. [1]: 3.1.-ben. Itt csak annyit idézünk föl, hogy R-modulusok egy $A^\bullet$ komplexusának R-modulusok és köztük lévő homomorfizmusok egy olyan

$$\ldots \overset{d^{i-1}}{\to} A^i \overset{d^i}{\to} A^{i+1} \overset{d^{i+1}}{\to} A^{i+2} \overset{d^{i+2}}{\to} \ldots$$

végtelen sorozatát nevezzük ($i \in \mathbb{Z}$), melyre $d^{i+1} \circ d^i = 0$ teljesül minden i-re. Legyen

$$Z^i(A^\bullet) = \ker d^i, \quad B^i(A^\bullet) = \mathrm{Im} d^{i-1}, \quad H^i(A^\bullet) = Z^i(A^\bullet)/B^i(A^\bullet).$$

Az M R-modulus egy $P_\bullet$ projektív feloldását véve (ez egy P_i projektív modulusokból álló $\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$ egzakt sort jelent, ilyen létezik) tekinthetjük a $\mathrm{Hom}_R(P_\bullet, N)$ komplexust:

$$\mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N) \to \mathrm{Hom}_R(P_2, N) \to \ldots$$

Ekkor

$$\mathrm{Ext}_R(M, N) = H^i(\mathrm{Hom}_R(P_\bullet, N)).$$

3.2.2. állítás. *Az így definiált kohomológiacsoportok teljesítik a felsorolt* (1)-(3) *tulajdonságokat.*

Bizonyítás. [1]: 3.1.9.

A $\mathbb{Z}$ egy rögzített $\cdots \to \mathbb{Z}[G^3] \to \mathbb{Z}[G^2] \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ projektív feloldásából explicit módon is megadhatók ezek a kohomológiák ([1]: 3.2.). A $\mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], A))$ elemeit *i-koláncoknak*, ezek közül a $Z^{i+1}(\mathrm{Hom}_G(\mathbb{Z}[G^\bullet], A))$ elemeit *i-kociklusoknak*, míg $B^{i+1}(\mathrm{Hom}_G(\mathbb{Z}[G^\bullet], A))$ elemeit *i-kohatároknak* nevezzük. Az i-edik kohomológiacsoport az i-kociklusok i-kohatárok szerinti ekvivalenciaosztályaiból áll. Számunkra ezek közül az 1- és 2-kociklusok explicit megadása fog szerepet játszani, ezért most csak azokat idézzük fel:

A G 1-kociklusait már definiáltuk (nem csak kommutatív esetben) a 3.1.3. definícióban, és ez az általános definíció szerint is megfelelő meghatározás lesz. Egy 1-kociklus alatt tehát egy olyan $\sigma \mapsto a_\sigma$ leképezést értünk, melyre $a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma$ (most additívan fölírva). Ez pontosan akkor 1-kolánc, ha $\sigma \mapsto \sigma(a) - a$ alakú valamely $a \in A$-val, így visszakaptuk az első kohomológia halmaz korábbi definícióját. Abban a speciális esetben, amikor G triviálisan hat A-n ($\sigma a = a \quad \forall a \in A$), a $H^1(G, A) = \mathrm{Hom}(G, A)$ összefüggéshez jutunk.

Egy 2-kociklus egy $(\sigma, \tau) \mapsto a_{\sigma,\tau}$ leképezésként definiálhatunk, ami teljesíti a következő összefüggést:

$$\sigma a_{\tau,\nu} - a_{\sigma\tau,\nu} + a_{\sigma,\tau\nu} - a_{\sigma,\tau} = 0.$$

Akkor lesz 2-kohatár, ha $a_{\sigma,\tau} = \sigma b_\tau - b_{\sigma\tau} + b_\sigma$ alakú valamely $\sigma \mapsto b_\sigma$ 1-kolánccal.

A (3) tulajdonságban meghatározott egzakt sorozat létezik az első kohomológiák korábbi értelmezés szerinti nem kommutatív esetében is. Ebben az esetben érdemes a konkrét (nemtriviális) leképezéseket is meghatározni, ezeket ugyanis használjuk a későbbi számolásokban.

3.2.3. állítás. *Legyen G csoport, amely hat csoportok egy $1 \to A \to B \xrightarrow{\psi} C \to 1$ egzakt sorozatán, legyen továbbá $A \subseteq Z(B)$ kommutatív csoport. Ekkor létezik pontozott halmazok egzakt sorozata (ahol a kitüntetett elemek egymásra képződnek):*

$$1 \to A^G \to B^G \to C^G \xrightarrow{\partial} H^1(G,A) \to H^1(G,B) \to H^1(G,C) \xrightarrow{\delta} H^2(G,A).$$

Bizonyítás. Az egzakt sorban ∂ és δ jelzéssel szereplő leképezéseket kell definiálni, a többi triviálisan adódik az eredeti leképezésekből. Ha $c \in C^G$, akkor megadható olyan $b \in B$, melyre $\psi(b) = c$. Ekkor $\psi(b\sigma(b)^{-1}) = 1$ C-ben minden $\sigma \in G$ esetén, tehát $b\sigma(b)^{-1} \in A$. A $\sigma \mapsto b\sigma(b)^{-1}$ leképezés egy 1-kociklust ad meg, ennek ekvivalenciaosztálya lesz $\partial(c)$. Ha $\partial(c) = 1 \in H^1(G,A)$, akkor $b\sigma(b)^{-1} = a\sigma(a)^{-1}$ minden $\sigma \in G$-re valamely $a \in A$-val, de ekkor $a^{-1}b \in B^G$, amely elem ψ-nél szintén c-re képződik, így az egzaktság is teljesül. Az egzaktság a többi helyen is egyszerű számolásokból adódik.

Definiáljuk még a δ leképezést: ehhez legyen $\sigma \mapsto c_\sigma$ egy 1-kociklus, amely reprezentálja $H^1(G,C)$ egy elemét. Emeljük fel c_σ-t egy $b_\sigma \in B$ elemre, és legyen $a_{\sigma,\tau} = b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$. Mivel c_σ 1-kociklus, ennek a ψ-nél vett képe 1, azaz $a_{\sigma,\tau} \in A$. A $(\sigma,\tau) \mapsto a_{\sigma,\tau}$ 2-kociklust határoz meg, melynek $H^2(G,C)$-beli osztálya egyértelmű. Ha ugyanis c_σ-t egy $a_\sigma b_\sigma$-ra emeljük fel, akkor $a_{\sigma,\tau}$ helyett $a_\sigma b_\sigma \sigma(a_\tau b_\tau) b_{\sigma\tau}^{-1} a_{\sigma\tau}^{-1} = a_\sigma \sigma(a_\tau) a_{\sigma\tau}^{-1} a_{\sigma,\tau}$ adódik, ami éppen $a_{\sigma,\tau}$ egy 2-kohatárszorosa (használva, hogy A elemei centrumbeliek). Ha c_σ helyett ekvivalens kociklust veszünk, szintén $A \subseteq Z(B)$-t használva kapjuk a leképezés jóldefiniáltságát. Az egzaktság az előzőhöz hasonló számolással ellenőrizhető. □

A Galois-csoport első kohomológiájára vonatkozik Hilbert 90-es tétele (illetve annak Noether-féle általánosítása):

3.2.4. tétel (Hilbert 90). *Legyen K/k véges Galois bővítés G Galois-csoporttal. Ekkor*

$$H^1(G, K^*) = \{1\}.$$

Bizonyítás. A tételnél általánosabb $H^1(G, \mathrm{GL}_n(K)) = 1$ állítást ($n > 1$ esetben persze nemkommutatív kohomológiával értve) mondja ki [1]: 2.3.4., ami a Galois-leszállás módszerének speciális eseteként adódik. □

A kohomológiacsoport definíciójával a Brauer-csoport másképp is meghatározható:

3.2.5. tétel. *Legyen K/k véges Galois-bővítés G Galois-csoporttal. Ekkor*

$$\mathrm{Br}(K/k) \cong H^2(G, K^*).$$

Bizonyítás. [1]: 4.4.7.

Ha G n rendű véges csoport, akkor tetszőleges A G-modulusra és $i > 0$ egész számra $n \cdot H^i(G, A) = 0$ ([1]: 3.3.8.). Ebből adódik az alábbi következmény:

3.2.6. következmény. *A $\mathrm{Br}(K/k)$ relatív Brauer-csoport minden elemének rendje $[K : k]$ osztója.*

Ahhoz, hogy a $\mathrm{Br}(k)$ Brauer-csoportot is kifejezhessük kohomológiával, külön megállapításokat kell tennünk provéges csoportok kohomológiáira. Ehhez a végtelen testbővítések Galois-elméletének ismeretére van szükség, amiről összefoglaló pl. [1] 4.1. fejezetében található, most csak az alapvető definíciókat ismertetjük.

Csoportok $(G_\alpha, \varphi_{\alpha\beta})$ *inverz rendszerén* a következőt értjük:

- Adott egy $(\Lambda, \leq)$ részben rendezett halmaz, mely irányított abban az értelemben, hogy minden $(\alpha, \beta) \in \Lambda$ esetén létezik olyan $\gamma \in \Lambda$, melyre $\alpha \leq \gamma, \beta \leq \gamma$;
- minden $\alpha \in \Lambda$ esetén adott egy G_α csoport;
- minden $\alpha \leq \beta$ esetén adott egy $\varphi_{\alpha\beta} : G_\beta \to G_\alpha$ homomorfizmus, továbbá $\varphi_{\alpha\gamma} = \varphi_{\alpha\beta} \circ \varphi_{\beta\gamma}$ teljesül minden $\alpha \leq \beta \leq \gamma$ esetén.

A rendszer *inverz limesze* a $\prod_{\alpha\in\Lambda} G_\alpha$ azon (g_α) elemekből álló részcsoportja, melyek a $\varphi_{\alpha\beta}(g_\beta) = g_\alpha$ összefüggést teljesítik minden $\alpha \leq \beta$ esetén. A G_α csoportok inverz limeszét $\varprojlim G_\alpha$-val jelöljük. Véges csoportok inverz limeszét *provéges csoportnak* nevezzük. Ha K/k Galois-bővítés, akkor $\mathrm{Gal}(K/k)$

provéges csoport, amelyik megkapható a véges L/k Galois-részbővítések által alkotott inverz rendszer Galois-csoportjainak inverz limeszeként ([1]: 4.1.3.).

Ha G provéges csoport, akkor *folytonos G-modulus* alatt egy olyan A G-modulust értünk, melyre minden $a \in A$ elem stabilizátora nyílt az inverz limesz diszkrét topológiából származó topológiájára nézve. Ha $G_\alpha = G/U_\alpha$ egyike G standard faktorainak, akkor A^{U_α} természetes módon G_α-modulus is. A $\varphi_{\alpha\beta} : G_\beta \to G_\alpha$ leképezések indukálnak egy $\mathrm{Inf}_\alpha^\beta : H^i(G_\alpha, A^{U_\alpha}) \to H^i(G_\beta, A^{U_\beta})$ leképezést minden $i \geq 0$ esetén. A $H^i(G_\alpha, A)$ csoportok az $\mathrm{Inf}_\alpha^\beta$ leképezésekkel direkt rendszert alkotnak a következő értelemben. Abel-csoportok $(B_\alpha, \psi_{\alpha\beta})$ *direkt rendszere* a következőkből áll:

- egy $(\Lambda, \leq)$ irányított részben rendezett halmaz;
- minden $\alpha \in \Lambda$ esetén egy B_α Abel-csoport;
- minden $\alpha \leq \beta$ esetén $\psi_{\alpha\beta} : B_\alpha \to B_\beta$ homomorfizmusok, melyre $\psi_{\alpha\gamma} = \psi_{\beta\gamma} \circ \psi_{\alpha\beta}$ minden $\alpha \leq \beta \leq \gamma$ esetén.

A rendszer *direkt limesze* a $\bigoplus_{\alpha\in\Lambda} B_\alpha$ direkt összeg lefaktorizálva a $b_\beta - \psi_{\alpha\beta}(b_\alpha)$ alakú elemek által generált részcsoporttal.

3.2.7. definíció. *Legyen $G = \varprojlim G_\alpha$ provéges csoport, A folytonos G-modulus. Ha $i \geq 0$ egész, akkor az i-edik folytonos kohomológiacsoportot, $H^i_{cont}(G, A)$-t úgy értelmezzük, mint a fenti $(H^i(G_\alpha, A^{U_\alpha}), \mathrm{Inf}_\alpha^\beta)$ direkt rendszer direkt limeszét. Ha $G = \mathrm{Gal}(\bar{k}/k)$ a k tökéletes test valamely rögzített $\bar{k}$ algebrai lezártjával, akkor a $H^i_{cont}(G, A)$ csoportot a k i-edik kohomológiacsoportjának nevezzük A-ban.*

Véges G csoportok esetén a korábbi definíciót kapjuk vissza. Provéges G esetén (speciálisan: a $\bar{k}/k$ végtelen bővítések Galois-csoportja esetén) a továbbiakban kizárólag az így definiált kohomológiacsoportokkal foglalkozunk, és a *cont* megkülönböztetést el is hagyjuk. A 3.2.3. állításban meghatározott (illetve a korábbi (3) tulajdonságban szereplő) egzakt sorozat folytonos kohomológiacsoportok esetén is létezik ([1]: 4.3.1.). Hilbert 90-es tétele kiterjeszthető az abszolút Galois-csoportra is, hiszen a direkt limesz minden tagja triviális lesz; így tehát $H^1(G, \bar{k}^*) = \{1\}$. Végül a 3.2.5. tételhez hasonlóan most már a $\mathrm{Br}(k)$ Brauer-csoport is meghatározható:

$$Br(k) \cong H^2(G, \bar{k}^*).$$

3.3. Centrális egyszerű algebra indexe és periódusa. Görbék és a Brauer-csoport

Közelítve a projektív görbék indexe és periódusa közti kapcsolat vizsgálatához, ebben a pontban összekapcsoljuk a Brauer-csoportokról felidézetteket a görbék divizor- és Picard-csoportjainak Galois-kohomológiájával. Előtte azonban még definiáljuk az index és a periódus fogalmát centrális egyszerű algebrákra is.

3.3.1. definíció. *Legyen A k feletti centrális egyszerű algebra, amelyik a Wedderburn-tétel értelmében egy D ferdetest feletti $M_n(D)$ mátrixgyűrűvel izomorf. Az A k feletti indexének nevezzük (és $\mathrm{ind}_k(A)$-val jelöljük) a $\deg_k(D)$ fokot.*

Az $\mathrm{ind}_k(A)$ index csak az $[A] \in \mathrm{Br}(k)$ osztálytól függ, nevezetesen éppen az osztályhoz tartozó ferdetest fokával egyenlő. A indexe pontosan akkor 1, ha A k felett felhasad.

Az index jellemezhető a következőképpen is:

3.3.2. állítás. *Az A centrális egyszerű algebra indexe éppen az A-t felhasító K/k véges szeparábilis bővítések fokainak legnagyobb közös osztója.*

Bizonyítás. [1]: 4.5.8.

Ezt egybevetve azzal az állítással, hogy létezik olyan véges szeparábilis bővítés, melynek foka az A indexe ([1]: 4.5.4.), következik, hogy az index nem más, mint a *legkisebb* A-t felhasító véges szeparábilis bővítés foka, a többi őt felhasító bővítés fokai pedig pontosan az index többszörösei.

3.3.3. definíció. *Az A centrális egyszerű algebra periódusa (vagy exponense) az $[A]$ rendje a $\mathrm{Br}(k)$ Brauer-csoportban, ezt $\mathrm{per}(A)$-val jelöljük.*

A centrális egyszerű algebrák indexe és periódusa közti kapcsolatot Brauer tétele ([1]: 4.5.13.) foglalja össze:

3.3.4. tétel (Brauer). *Legyen A centrális egyszerű k-algebra. Ekkor $\mathrm{ind}_k(A)$ a $\mathrm{per}(A)$ osztója, továbbá a periódus és az index ugyanazokból a prímfaktorokból áll.*

Most visszatérünk a görbékhez, legyen X sima projektív geometriailag összefüggő görbe a k tökéletes test fölött, szokásosan $\bar{k}$ egy rögzített algebrai lezárt, $\bar{X}$ a görbe az algebrai lezárt fölött értelmezve, és G a k abszolút Galois-csoportja. A kohomológiákkal kapcsolatos ismeretek és az 2.1 egzakt sor segítségével látható be a következő lemma:

3.3.5. lemma. *Az alábbi diagram második és harmadik sora egzakt, továbbá megadhatók olyan ϑ_0 és ϑ leképezések, amelyek a diagramot kommutatívvá teszik:*

$$\begin{array}{ccccccccc}
 & & \mathrm{Br}(k) & \xrightarrow{1} & \mathrm{Br}(k) & & & & \\
 & & \uparrow{\scriptstyle \vartheta_0} & & \uparrow{\scriptstyle \vartheta} & & & & \\
0 & \longrightarrow & \mathrm{Pic}_0(\bar{X})^G & \longrightarrow & \mathrm{Pic}(\bar{X})^G & \longrightarrow & \mathbb{Z} & \longrightarrow & H^1(G, \mathrm{Pic}_0(\bar{X})) \\
 & & \uparrow & & \uparrow & & \uparrow{\scriptstyle 1} & & \\
0 & \longrightarrow & \mathrm{Div}_0(\bar{X})^G & \longrightarrow & \mathrm{Div}(\bar{X})^G & \longrightarrow & \mathbb{Z} & &
\end{array}$$

Bizonyítás. A vízszintes sorok egzaktsága azonnal következik a 3.2.3. állításból a triviális

$$0 \to \mathrm{Pic}_0(\bar{X}) \to \mathrm{Pic}(\bar{X}) \to \mathbb{Z} \to 0,$$

illetve

$$0 \to \mathrm{Div}_0(\bar{X}) \to \mathrm{Div}(\bar{X}) \to \mathbb{Z} \to 0$$

egzakt sorokra fölírva. Most a ϑ leképezést konstruáljuk meg, ϑ_0-é analóg módon történhet.

A 2.1 egzakt sorozatát a következőképpen is felírhatjuk:

$$0 \to K(\bar{X})^*/\bar{k}^* \to \mathrm{Div}(\bar{X}) \to \mathrm{Pic}(\bar{X}) \to 0.$$

Itt Galois-kohomológiát véve kapjuk a következő egzakt sort és δ_1 leképezést:

$$\mathrm{Div}(\bar{X})^G \to \mathrm{Pic}(\bar{X})^G \xrightarrow{\delta_1} H^1(G, K(\bar{X})^*/\bar{k}^*).$$

Másrészt a $0 \to \bar{k}^* \to K(\bar{X})^* \to K(\bar{X})^*/\bar{k}^* \to 0$ egzakt sorozatból δ_2-t kapjuk:

$$H^1(G, K(\bar{X})^*) \to H^1(G, K(\bar{X})^*/\bar{k}^*) \xrightarrow{\delta_2} H^2(G, \bar{k}^*) = \mathrm{Br}(k).$$

Az X görbe geometriailag összefüggőségéből következik, hogy tetszőleges véges L/k Galois-bővítés esetén, ha $K_L(X)$ jelöli az X L fölött értelmezett függvénytestét, akkor a $K_L(X)/K(X)$ testbővítés Galois-csoportja megegyezik a $\mathrm{Gal}(L/k)$ csoporttal. Ugyanis, ha α az L/k bővítés primitív eleme és f_α annak minimálpolinomja, akkor

$$K_L(X) = L \underset{k}{\otimes} K(X) = K(X)[t]/(f_\alpha(t)),$$

ami geometriailag összefüggő X esetén nem eshet szét függvénytestek direkt összegére, azaz továbbra is testnek kell maradnia, tehát f_α irreducibilis $K(X)$ felett is. Ekkor a Hilbert 90-es tétel alkalmazásával $H^1(\mathrm{Gal}(L/k), K_L(X)^*) = 0$-hoz jutunk, a direkt limeszt véve pedig $H^1(G, K(\bar{X})^*) = 0$ is következik. Így a δ_2 leképezés injektív, a $\vartheta = \delta_2 \circ \delta_1$ kompozíció pedig megfelelő, a

$$\mathrm{Div}(\bar{X})^G \to \mathrm{Pic}(\bar{X})^G \xrightarrow{\vartheta} \mathrm{Br}(k)$$

sort egzakttá tevő leképezést határoz meg. □

Legyen $D \in \mathrm{Div}(\bar{X})$ olyan divizor, amelyre $[D] \in \mathrm{Pic}(\bar{X})^G$. Legyen K/k egy olyan véges Galois-bővítés, amelyre D K-racionális, jelölje H a $\mathrm{Gal}(K/k)$ Galois-csoportot. A 2.1. pont végén definiált ($\bar{k}$ feletti) $L(D)$ vektortérhez hasonlóan megkapható K fölötti vektortérként az $L_K(D)$, amelynek az $\{f \in K_K(X) : \mathrm{div} f + D \geq 0\}$ függvények az elemei. Ekkor az $L(D) = L_K(D) \otimes_k \bar{k}$ teljesül, és így a $\dim_{\bar{k}} L(D) = \dim_K L_K(D)$ dimenziók megegyeznek, ezt jelöljük most r-rel. Az előző lemma szerint értelmezett ϑ leképezésről a Brauer-csoportról korábban megismertek alapján fogalmazható meg a következő tétel:

3.3.6. tétel (Lichtenbaum). *A $\vartheta([D])$ képnek megfelelő centrális egyszerű algebrákat felhasítja k egy r fokú bővítése, tehát a Brauer-csoportban $r\vartheta([D]) = 0$.*

Bizonyítás. Az állítás második fele a 3.2.6. következményből adódik. Az első felének bizonyításához rögzítsünk egy λ' izomorfizmust a K^r és $L_K(D)$ K-vektorterek között. Ez indukál egy λ izomorfizmust a $\mathbb{P}^{r-1}(K)$ és a $|D|$ lineáris rendszer közt. Ha $\sigma \in H$, akkor a $\lambda^\sigma(x^\sigma) = \lambda(x)^\sigma$ összefüggéssel egy λ^σ izomorfizmust adhatunk meg, továbbá mivel $[D]$ K-racionális, ezért σ a $|D|$ lineáris rendszert önmagára képezi. A $\sigma \mapsto \lambda^{-1}\lambda^\sigma$ H egy 1-kociklusát határozza meg a (nemkommutatív) $\mathrm{PGL}(r, K)$ csoportban. Ehhez egy $\alpha \in H^1(H, \mathrm{PGL}(r, K))$ kohomológiaosztály tartozik (ez független a $[D]$ osztály reprezentásának választásától, illetve λ-tól). A $0 \to K^* \to \mathrm{GL}(r, K) \to \mathrm{PGL}(r, K) \to 0$ egzakt sorozatra Galois-kohomológiát alkalmazva egy $\delta : H^1(H, \mathrm{PGL}(r, K)) \to H^2(H, K^*) = \mathrm{Br}(K/k)$ leképezést kapunk, ahol persze ez utóbbi a $\mathrm{Br}(k)$ Brauer-csoport részcsoportja. Belátjuk, hogy $\delta(\alpha) = -\vartheta([D])$. Ezzel a tétel bizonyítása készen is van, hiszen így $\vartheta([D])$ a Brauer-csoportban $H^1(H, \mathrm{PGL}(r, K))$ képében van, tehát a 3.1.4. tétel szerint K felett felhasadó, r fokú A centrális egyszerű k-algebrával reprezentálható. Az $\mathrm{ind}_k(A)$ index persze osztója r-nek, másrészt a 3.3.2. állítás szerint éppen az index többszörösei adják meg az A-t felhasító bővítések fokait, azaz A-t felhasítja a k egy r fokú bővítése is.

Először $\vartheta([D])$-t számoljuk ki. Ehhez választunk olyan $f_\sigma \in K(\bar{X})$ függvényeket, amikre $\mathrm{div}(f_\sigma) = D - D^\sigma$. A 3.2.3. állítás számolása szerint az $f_\sigma f_\tau^\sigma f_{\sigma\tau}^{-1}$ egy konstans ($\bar{k}$-beli) 2-kociklust határoz meg, amelynek osztálya lesz $\vartheta([D])$ a Brauer-csoportban. Másrészt megadjuk konkrétan a δ leképezést is. Ehhez rögzítsük K^r egy $e_1, e_2, \ldots, e_r$ bázisát, és jelölje $g_i = \lambda'(e_i)$ a bázis $L_K(D)$-beli képét. Legyen $E_i = \mathrm{div}(g_i) + D$, E_i tehát a $|D|$ lineáris rendszerben van. Jelölje $\bar{e_i}$ az e_i elemek képét a $\mathbb{P}^{r-1}(K)$ projektív térben, ekkor tehát $\lambda(\bar{e_i}) = E_i$, továbbá

$$\lambda^\sigma(\bar{e_i}) = \lambda^\sigma(\bar{e_i}^\sigma) = \lambda(\bar{e_i})^\sigma = E_i^\sigma = \mathrm{div}(g_i^\sigma) + D^\sigma = \mathrm{div}(g_i^\sigma h_\sigma) + D,$$

ahol $h_\sigma = f_\sigma^{-1}$. Ekkor $g_i^\sigma h_\sigma$ $L_K(D)$-ben van, tehát felírható $\sum_{j=1}^r a_{ij\sigma} g_j$ alakban. Továbbá $\lambda'^\sigma(e_i) = g_i^\sigma h_\sigma$, és így

$$\lambda'^{-1}\lambda'^\sigma(e_i) = \lambda'^{-1}(g_i^\sigma h_\sigma) = \lambda'^{-1}\left(\sum_{j=1}^r a_{ij\sigma} g_j\right) = \sum_{j=1}^r a_{ij\sigma}\lambda'^{-1}(g_j) = \sum_{j=1}^r a_{ij\sigma} e_j.$$

Jelölje A_σ az $(a_{ji\sigma})$ elemekből álló mátrixot, ekkor (ha A_σ-ra mint az $L_K(D)$ vektortér egy lineáris leképezésére gondolunk) $A_\sigma(g_i) = g_i^\sigma h_\sigma$ teljesül. Másrészt az előző számolás miatt A_σ éppen a $\lambda'^{-1}\lambda'^\sigma$ leképezés e_i bázisnál vett mátrixa, és ekkor (szintén a 3.2.3. állításban szereplő számítás alapján) a $\delta(\alpha)$ képet az $A_\sigma\sigma(A_\tau)A_{\sigma\tau}^{-1}$ 2-kociklus reprezentálja. Ez a mátrix a $\mathrm{GL}(r, K)$ centrumában lesz, azaz egy skalármátrix, azaz a hozzá tartozó skalárt kiszámíthatjuk egy tetszőleges függvény képénél. Tekintsük tehát a $g_1^{\sigma\tau} h_{\sigma\tau}$ függvény képét:

$$A_\sigma\sigma(A_\tau)A_{\sigma\tau}^{-1}(g_1^{\sigma\tau} h_{\sigma\tau}) = A_\sigma\sigma(A_\tau)(g_1) = A_\sigma \sum_{j=1}^r a_{1j\tau}^\sigma g_1 = \sum_{j=1}^r a_{1j\tau}^\sigma A_\sigma(g_1) =$$

$$= \sum_{j=1}^r a_{1j\tau}^\sigma g_1^\sigma h_\sigma = h_\sigma \left(\sum_{j=1}^r a_{1j\tau} g_1\right)^\sigma = h_\sigma g_1^{\sigma\tau} h_\tau^\sigma = h_\sigma h_\tau^\sigma h_{\sigma\tau}^{-1} \cdot h_{\sigma\tau} g_1^{\sigma\tau}.$$

Azaz a $\delta(\alpha)$ képhez tartozó 2-kociklust a $h_\sigma h_\tau^\sigma h_{\sigma\tau}^{-1}$ konstans adja meg, viszont ez - figyelembe véve, hogy a h_σ függvények az f_σ-k inverzei - éppen a reciproka a $\vartheta([D])$-hez tartozó kociklusnak, azaz ezek a kohomológiacsoportban egymás inverzei. $\square$

4. fejezet

Periódus-index feltételek görbéken

A 2.2.3. definícióban meghatároztuk az X görbe periódusának és indexének fogalmát: előbbi az X-en vett k-racionális divizorosztályok fokainak legnagyobb közös osztója, míg utóbbi a k-racionális divizorok fokaira ugyanez. Megállapítottuk, hogy nyilvánvalóan a periódus osztója az indexnek. Ebben a fejezetben Lichtenbaum [3] cikke alapján további összefüggéseket igazolunk a periódus és az index között. Az első pontban belátjuk, hogy tetszőleges test feletti görbék esetén igaz lesz, hogy I osztója $2P^2$-nek. A második pontban Roquette tételének felhasználásával, Lichtenbaum bizonyítása szerint p-adikus testek fölötti görbékre határozunk meg újabb összefüggéseket.

4.1. Periódus-index feltételek tetszőleges alaptest fölött

Ebben a pontban legyen végig k tetszőleges tökéletes test, $\bar{k}$ egy rögzített algebrai lezártja, G az abszolút Galois-csoport. Legyen X g génuszú geometriailag összefüggő sima projektív görbe k fölött. Ekkor a következő tétel teljesül:

4.1.1. tétel (Lichtenbaum). *Az I index és P periódus között a következő kapcsolat áll fenn:*

(1) $P|I|2P^2$;

(2) *Ha továbbá $\frac{2(g-1)}{I}$ páros, akkor $P|I|P^2$. Speciálisan, $g = 1$ esetben ez mindig teljesül.*

A tétel bizonyításában a 3.3.5. lemmában szereplő diagram kis módosítását használjuk. Erről a következő olvasható le:

4.1.2. lemma. *Az I/P érték osztója a $\vartheta(\mathrm{Pic}(\bar{X})^G)$ exponensének (ahol ϑ a 3.3.5. lemmában megadott leképezés).*

Bizonyítás. A periódus és index definícióját használva rajzoljuk fel ismét a korábbi diagramot (és nevezzük el λ_0-nak, illetve λ-nak a megfelelő divizorcsoportokból a Picard-csoportok G-invariáns részcsoportjaiba menő leképezéseket):

$$\begin{array}{ccccccccc}
 & & & & \mathrm{Br}(k) & \xrightarrow{1} & \mathrm{Br}(k) & & \\
 & & & & \uparrow{\scriptstyle \vartheta_0} & & \uparrow{\scriptstyle \vartheta} & & \\
0 & \longrightarrow & \mathrm{Pic}_0(\bar{X})^G & \longrightarrow & \mathrm{Pic}(\bar{X})^G & \longrightarrow & P\mathbb{Z} & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \lambda_0} & & \uparrow{\scriptstyle \lambda} & & \uparrow{\scriptstyle \iota} & & \\
0 & \longrightarrow & \mathrm{Div}_0(\bar{X})^G & \longrightarrow & \mathrm{Div}(\bar{X})^G & \longrightarrow & I\mathbb{Z} & \longrightarrow & 0 \\
 & & & & & & \uparrow & & \\
 & & & & & & 0 & &
\end{array}$$

A kígyó-lemma alapján létezik a következő egzakt sorozat:

$$0 = \ker \iota \to \mathrm{coker}(\lambda_0) \to \mathrm{coker}(\lambda) \to \mathrm{coker}(\iota) \to 0.$$

Viszont $\mathrm{coker}(\lambda_0) = \mathrm{Pic}_0(\bar{X})^G / \ker \vartheta_0 \cong \vartheta_0(\mathrm{Pic}_0(\bar{X}^G))$, és ugyanígy $\mathrm{coker}(\lambda) \cong \vartheta(\mathrm{Pic}(\bar{X}^G))$. Mivel $|\mathrm{coker}(\iota)| = I/P$, ezért az egzakt sorozatból leolvasható, hogy

$$\frac{|\vartheta(\mathrm{Pic}(\bar{X}^G))|}{|\vartheta_0(\mathrm{Pic}_0(\bar{X}^G))|} = \frac{I}{P},$$

továbbá $\vartheta(\mathrm{Pic}(\bar{X})^G)$ az I/P rendű ciklikus csoportra képződik, ami bizonyítja a lemma állítását. □

A tétel bizonyítása. Először tegyük fel, hogy $g > 0$. Definíció szerint a k-invariáns divizorosztályok foka P valamilyen többszöröse. Ekkor $\mathrm{Pic}(\bar{X})^G$-t generálják a P fokú divizorosztályok, a ϑ-nál vett képet pedig a $\{\vartheta([D]) : \deg([D]) = P\}$ halmaz elemei. Legyen K kanonikus divizor, $[K]$ a kanonikus divizorosztály. K k-racionális divizor, tehát $[K]$ a $\lambda(\mathrm{Div}(\bar{X}^G))$ képben van, így $\vartheta([K]) = 0$ és $\vartheta([D] + [K]) = \vartheta([D])$. K foka $2g - 2$, azaz ekkor a

$P + 2g - 2$ fokú $[D]$ divizorosztályok $\vartheta([D])$ képe is generálja $\vartheta(\mathrm{Pic}(\bar{X}^G))$-t. A Riemann–Roch-tétel (2) következménye szerint (használva, hogy $P > 0$ miatt $\deg D > 2g-2$) $\dim L(D) = P+g-1$, így a 3.3.6. tételből következően $(P + g - 1)\vartheta(\mathrm{Pic}(\bar{X}^G)) = 0$.

Másrészt a lemmából következik, hogy $\frac{I}{P}|(P + g - 1)$, azaz $I|P^2 + P(g - 1)$. Mivel K k-racionális divizor, ezért $I|2(g - 1)$ is teljesül, amiből $I|2P^2$ következik, tehát (1)-et ebben az esetben bebizonyítottuk. Ha $2(g - 1) = nI$ valamely n páros számmal, akkor $I|(g - 1)$ is teljesül, amiből (2) következik.

Végül ha $g = 0$, akkor tetszőleges nulladfokú D divizorra alkalmazható a Riemann–Roch-tétel (2) következménye, így $L(D)$ dimenziója 1, azaz létezik olyan f függvény, melyre $\mathrm{div}(f) + D \geq 0$, persze a fokok miatt itt ekkor egyenlőségnek kell állnia, így az $1/f$ függvény divizora éppen D lesz. Tehát 0 génuszú görbe esetén minden nulladfokú divizor előáll függvénydivizorként, ami miatt a $\mathrm{Pic}(\bar{X}) \cong \mathbb{Z}$ mint G-modulus, ilyenkor a periódus tehát 1 lesz. A kanonikus divizor -2 fokú, tehát az index 1 vagy 2, a tétel állításai ezekben az esetekben is teljesülnek. □

4.2. Periódus-index feltételek p-adikus testek fölött

Még többet állíthatunk a periódus és az index közti összefüggésekről, ha megkötéseket teszünk az alaptestre. A továbbiakban p-adikus testek fölötti görbékkel foglalkozunk, a lényegi állítások azonban igazak maradnak lokális testek fölött is. Bizonyos feltételek mellett p-adikus testek esetén az index és a periódus egyenlőségére is következtethetünk (azaz ilyen feltételek esetén minden k-racionális divizorosztály tartalmaz k-racionális divizort is). A következő tételt bizonyítjuk majd be:

4.2.1. tétel (Lichtenbaum). *Legyen X g génuszú sima, geometriailag összefüggő projektív görbe egy p-adikus k test fölött. Ekkor:*

(1) $P|(g - 1)$;

(2) $I = P$ *vagy* $2P$;

(3) *Ha* $I = 2P$, *akkor* $\frac{(g-1)}{P}$ *páratlan. Speciálisan,* $g = 1$ *esetben a periódus egyenlő az indexszel.*

A tétel bizonyítása Lichtenbaum [3] cikke alapján történik, aki ehhez Roquette tételét haszálja fel, melyet pedig a Tate-dualitás módszerével igazol. Ebből csak a Roquette-tételhez szükséges állításokat ismertetjük itt, a bizonyítás a cikkben megtalálható.

4.2.2. tétel (Hasse). *Legyen k p-adikus test. Ekkor* $\mathrm{Br}(k) \cong \mathbb{Q}/\mathbb{Z}$.

Bizonyítás. [5]: XIII.3.6.

Egy A sima projektív varietást *Abel-varietásnak* nevezünk, ha adott a pontjain egy Abel-csoport struktúra, azaz egy $O \in A$ pont, továbbá adottak a $\mu : A \times A \to A$ és $i : A \to A$ morfizmusok, melyek rendre meghatározzák az Abel-csoport nullelemét, összeadás- és inverzleképezését. Egy görbe nulladfokú divizorosztályai olyan Abel-varietásnak feleltethetők meg, melynek dimenziója a görbe génuszával egyezik meg ([9]:III.2.6.). Ezt a varietást az X $\mathrm{Jac}(X)$ *Jacobi-varietásának* nevezünk; ekkor tehát $\mathrm{Pic}_0(X) \cong \mathrm{Jac}(X)$.

Megmutatható, hogy ha A egy Jacobi-varietás egy k p-adikus test fölött, akkor megadható egy $\rho : H^1(G, A) \times H^0(G, A) \to \mathrm{Br}(k) \cong \mathbb{Q}/\mathbb{Z}$ tökéletes párosítás, amely indukál egy kanonikus ρ^* $H^1(G, A) \to H^0(G, A)^*$ homomorfizmust. Itt $H^0(G, A)^*$ a $\mathrm{Hom}_{cont}(H^0(G, A), \mathbb{Q}/\mathbb{Z})$ folytonos homomorfizmusok csoportját (a $H^0(G, A)$ csoport karaktercsoportját) jelöli. Az így meghatározott ρ^* Tate tétele szerint izomorfizmus. (A tétel ebben az alakjában az *általános Tate-dualitás* speciális esete. Aszerint A tetszőleges Abel-varietás lehet, melyhez létezik olyan A^* duális Abel-varietás, amelyre $H^1(G, A) \times H^0(G, A^*) \to \mathbb{Q}/\mathbb{Z}$ megfelelő párosítás. Jacobi-varietások esetében speciálisan $A^* = A$. Ebben a formában megtalálható a tétel Milne [4] könyvében: Corollary I.3.4. A Tate-dualitás eredeti ötlete Tate [12] cikkéből származik.)

Lichtenbaum [3] cikkében konkrétan megadja a megfelelő ρ_0 leképezést az $A = \mathrm{Pic}_0(\bar{X})$ esetben. Ha $\alpha \in H^1(G, \mathrm{Pic}_0(\bar{X}))$ egy a_σ 1-kociklus ekvivalenciaosztálya, akkor ez felemelhető egy b_σ 1-koláncra $\mathrm{Div}_0(\bar{X})$-en, míg a $(\delta b)_{\sigma,\tau} = b_\sigma + \sigma(b_\tau) - b_{\sigma\tau}$ a 3.2.3. állítás szerint egy $f_{\sigma,\tau}$ függvény divizorát definiálja (a szokásos egzakt sor alapján). Ha $E \in \mathrm{Div}_0(\bar{X})$ olyan divizor, amely egy $x \in \mathrm{Pic}_0(\bar{X})^G$ elemet reprezentál, akkor $E^\sigma - E$ egy g_σ függvény divizora, míg $(\sigma, \tau) \mapsto f_{\sigma,\tau}(E) g_\sigma(\sigma(b_\tau))$ egy 2-kociklust határoz meg $\bar{k}$-ba, melynek ekvivalenciaosztálya a $\mathrm{Br}(k)$ egy γ eleme. (Egy függvény kiértékelése egy adott divizorban természetesen a megfelelő pontokban vett értékekből származik lineáris kifejtéssel.) A $\rho_0(\alpha, x)$-et γ-nak definiáljuk, amely valóban jóldefiniált leképezés.

Ha továbbra is $H^0(G, \mathrm{Pic}_0(\bar{X}))^*$-gal jelöljük a $\mathrm{Hom}_{cont}(H^0(G, \mathrm{Pic}_0(\bar{X})), \mathbb{Q}/\mathbb{Z})$ csoportot, akkor az imént definiált ρ_0 ismét indukál egy $\rho_0^* : H^1(G, \mathrm{Pic}_0(\bar{X})) \to H^0(G, \mathrm{Pic}_0(\bar{X}))^*$ leképezést.

4.2.3. tétel (Tate). *Az így definiált ρ_0^* izomorfizmus.*

Bizonyítás. [3]: Theorem 2.

Most jelölje α a $H^1(G, \mathrm{Pic}_0(\bar{X}))$-ben azt az elemet, amit a $0 \to \mathrm{Pic}_0(\bar{X}) \to \mathrm{Pic}(\bar{X}) \to \mathbb{Z} \to 0$ egzakt sorozaton alkalmazott Galois-kohomológia esetén az $1 \in \mathbb{Z}$ képeként kapunk.

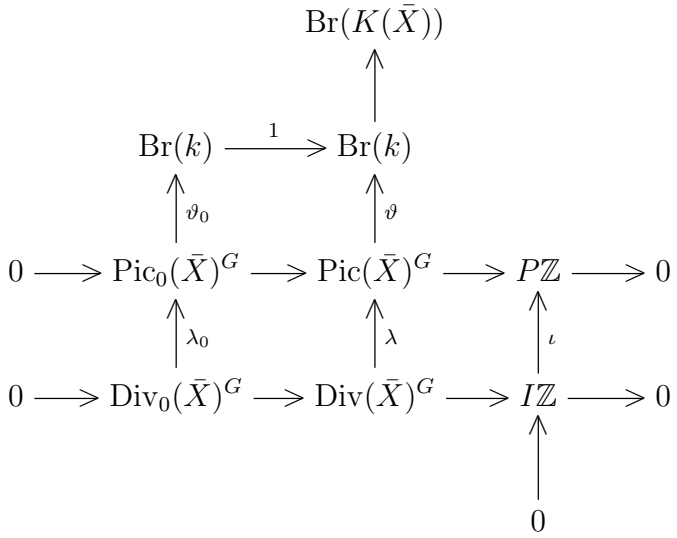
4.2.4. állítás. *Erre az α-ra $\rho_0(\alpha, x) = \vartheta_0(x)$, ahol ϑ_0 a 3.3.5. lemmában definiált leképezés.*

Bizonyítás. Egyrészt ebben az esetben b_σ definiálható $Q^\sigma - Q$ alakú divizorként, ahol Q tetszőleges $\bar{k}$-racionális pont. Ekkor a $(\delta b)_{\sigma,\tau}$ nulla lesz, azaz egy konstansfüggvény divizora, ami persze választható az azonosan 1 függvénynek; a $\rho_0(\alpha, x)$ definíciójának első tényezője így triviális. Ha E olyan divizor, amely x-re képződik, akkor $E^\sigma - E$ egy g_σ függvény divizora, és ekkor $\rho_0(\alpha, x)$ a $g_\sigma(Q^{\sigma\tau} - Q^\sigma)$ 2-kociklus ekvivalenciaosztálya. Másrészt ϑ_0 a korábbi kiszámolása szerint a $c_{\sigma,\tau} = g_\sigma g_\tau^\sigma g_{\sigma\tau}^{-1}$ konstansfüggvénynek megfelelő osztály, ami Q-ban kiértékelve a $g_\sigma(Q) g_\tau^\sigma(Q) g_{\sigma\tau}(Q)^{-1}$. Viszont a $g_\sigma(Q)\sigma(g_\tau(Q)) g_{\sigma\tau}(Q)^{-1}$ 2-kohatárral összehasonlítva ez kohomológ $g_\tau^\sigma(Q)\sigma(g_\tau(Q))^{-1} = g_\tau^\sigma(Q - Q^\sigma)$-val. Ez pedig könnyen kiszámolhatóan (lásd: [3]: Corollary 1.) kohomológ $g_\sigma(Q^{\sigma\tau} - Q^\sigma)$-val. □

A fő tétel bizonyításának utolsó előkészületi lépéseként az eddigiek segítségével bebizonyítjuk Roquette tételét. Ehhez ismét a 4.1.2. lemma bizonyításában szereplő diagramhoz térünk vissza.

4.2.5. tétel (Roquette). *Legyen k p-adikus test, X sima geometriailag összefüggő projektív görbe fölötte. Ekkor a $\mathrm{Br}(k)$ Brauer-csoportban a $K(\bar{X})$ felett felhasadó centrális egyszerű algebrák osztályait tartalmazó részcsoport rendje megegyezik az X indexével.*

Bizonyítás. Tekintsük ismét a korábbi diagramot! A $\mathrm{Pic}(\bar{X})^G \to \mathrm{Br}(k)$ függőleges oszlop persze a 3.3.5. lemma bizonyításának megfelelően folytatódhat $H^2(G, K(\bar{X})^*) = \mathrm{Br}(K(\bar{X}))$ felé, ahol a $\vartheta(\mathrm{Pic}(\bar{X})^G)$ kép éppen a $\mathrm{Br}(k)$ azon részcsoportja, amelyek $\mathrm{Br}(K(\bar{X}))$ egységelemére képződnek, azaz amely azon centrális egyszerű algebrák reprezentánsaiból áll, melyek a függvénytest felett felhasadnak. Tehét erről a képről kell belátni, hogy I rendű.



A 4.1.2. lemma bizonyításában elmondottak miatt ismét

$$\frac{|\vartheta(\mathrm{Pic}(\bar{X}^G))|}{|\vartheta_0(\mathrm{Pic}_0(\bar{X}^G))|} = \frac{I}{P},$$

azaz a bizonyítandó állítás azzal ekvivalens, hogy $|\vartheta_0(\mathrm{Pic}_0(\bar{X}^G))| = P$. Másrészt a $\vartheta_0(x) = \rho_0(\alpha, x)$ állítás miatt ez ugyanazt jelenti, mint hogy $|\{\rho_0(\alpha, x) : x \in \mathrm{Pic}_0(\bar{X})^G\}| = P$, ahol α továbbra is az 1 képe a $\mathbb{Z} \to H^1(G, \mathrm{Pic}_0(\bar{X})$ homomorfizmusnál. Persze ennek a homomorfizmusnak a magja $P\mathbb{Z}$, azaz α rendje P. Mivel ρ_0^* izomorfizmus, és a p-adikus test Brauer-csoportja $\mathbb{Q}/\mathbb{Z}$, így a vizsgált képhalmaz ennek az egyetlen P-rendű részcsoportja, $\mathbb{Z}/P\mathbb{Z}$, ezzel a tételt bebizonyítottuk. □

A 4.2.1. tétel bizonyítása. Először ismét tegyük fel, hogy $g > 0$. Az általános eset bizonyításához hasonlóan abból indulhatunk ki, hogy $\vartheta(\mathrm{Pic}(\bar{X})^G)$-t generálják a $\{\vartheta([D]) : \deg([D]) = P\}$ halmaz elemei. Ismét legyen K egy kanonikus divizor X-en, ekkor továbbra is $\vartheta([D] + [K]) = \vartheta([D])$, így ezúttal is $P + (2g - 2)$ fokú divizorosztályok képe is generálja $\vartheta(\mathrm{Pic}(\bar{X})^G)$-t. Továbbra is a Riemann–Roch-tétel (2) következményéből adódik, hogy $(P+g-1)\vartheta(\mathrm{Pic}(\bar{X}^G)) = 0$, amiből persze $(2P+2g-2)\vartheta(\mathrm{Pic}(\bar{X}^G)) = 0$ is. Roquette tétele szerint azonban $\vartheta(\mathrm{Pic}(\bar{X}^G))$ I rendű ciklikus, így $2P+2g-2 \equiv 0 \mod I$ (a ciklikusság abból következik, hogy a Brauer-csoport, azaz $\mathbb{Q}/\mathbb{Z}$ részcsoportjáról van szó). Viszont $I|2g-2$ (hiszen K k-racionális divizor), azaz $2P \equiv 0 \mod I$. Mivel továbbá a periódus az index osztója, ezért $I = P$ vagy $2P$, amivel (2)-t bizonyítottuk.

Mivel $(P+g-1)\vartheta(\mathrm{Pic}(\bar{X}^G)) = 0$, speciálisan $(P+g-1)\vartheta_0(\mathrm{Pic}_0(\bar{X}^G)) = 0$ is teljesül. Másrészt ez utóbbiról láttuk, hogy P rendű ciklikus, így $P+g-1$ is P többszöröse, ezért $P|(g-1)$, ami (1)-et igazolja.

Végül mivel $\vartheta(\mathrm{Pic}(\bar{X}^G))$ I rendű ciklikus, így $I|(P+g-1)$. Ha $I = 2P$, akkor a $g-1 = nP$ jelölést használva $2P|(n+1)P$, azaz $2|n+1$, így $n = \frac{g-1}{P}$ páratlan, tehát (3)-at is bebizonyítottuk.

A $g = 0$ esetben az általános tételnél leírtak miatt a periódus biztosan 1, a kanonikus divizor foka pedig -2, azaz az index 1 vagy 2, ami mindenképpen teljesíti a kivánt feltételeket. A $\frac{g-1}{P} = -1$ érték mindenképp páratlan, tehát (3) ilyenkor is teljesül. □

Megjegyzés. A $g = 1$ esetben tehát $\frac{g-1}{P} = 0$ mindenképpen páros, így az index egyenlő a periódussal. Ez a p-adikus pestek feletti elliptikus görbékre vonatkozó periódus-index tételt bizonyítja.

A $g = 0$ esetben $I = 1$ pontosan akkor áll fenn, ha X-nek van k-racionális pontja. Tehát ezek szerint $g = 0$ esetben valóban léteznek is olyan görbék, melyekre $I \neq P$. A dolgozat hátralevő részében Sharif cikke alapján megmutatjuk, hogy ennél jóval több is állítható, és az ebben a tételben megfogalmazott feltételeket kielégítő (P, I, g) értékekre valóban létezik is p-adikus test fölött adott génuszú görbe megfelelő indexszel és periódussal.

5. fejezet

Adott indexű és periódusú görbék

Ennek a fejezetnek a célja olyan, p-adikus test felett definiált görbék konstrukciója, amelyek adott, a 4.2.1. tétel feltételeit kielégítő génusszal, periódussal, indexszel rendelkeznek. Az ilyen (g, P, I) számhármasokat röviden *lokálisan megengedett számhármasoknak* nevezzük a továbbiakban. A konstrukció Sharif [7] cikke alapján történik, melyhez első lépésben a Tate-görbe fogalmát és a hozzá kapcsolódó ismereteket kell áttekinteni. Maga a konstrukció két lépésben zajlik. Először 1 génuszú görbéket adunk meg: ilyenkor a periódus és az index megegyezik, tehát azt kell megmutatnunk, hogy tetszőleges $P = I$ egészhez létezik olyan indexű és periódusú görbe. Utána külön lépésben foglalkozunk a magasabb nemű görbékkel. A konstrukciók használják a p-adikus testek bővítéseiről az 1.2. pontban ismertetetteket.

5.1. Elliptikus görbék, Tate-görbe, torzor

Elliptikus görbén olyan 1 génuszú görbét értünk, melynek van egy kitüntetett O alappontja (origója). Az E elliptikus görbe k fölött értelmezett, ha mint görbe, k fölötti, továbbá $O \in E(k)$. A Riemann–Roch-tétel segítségével megmutatható ([8]: III.3.1.), hogy minden elliptikus görbe egy megfelelő $\varphi : E \to \mathbb{P}^2(k), \varphi = [x, y, 1]$ izomorfizmussal egy

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Weierstrass-egyenlettel megadott síkgörbébe vihető, ahol az $a_1, \ldots, a_6$ együtthatók k-beliek és $\varphi(O) = [0, 1, 0]$ (a görbe többi pontja pedig az $X^{(2)}$ affin síkon van). Megfordítva, minden Weierstrass-egyenlettel megadott sima síkgörbe elliptikus görbe a $[0, 1, 0]$-val mint origóval.

Az elliptikus görbék Weierstrass-egyenlettel megadott alakjának segítségével a pontokon megadható egy $\oplus$ összeadási művelet. Ha $P, Q \in E(k)$,

akkor jelölje R a P, Q pontokon átmenő egyenes ($P = Q$ esetben az érintő) harmadik metszéspontját E-vel (ez szintén $E(k)$-beli pont, hiszen a koordináták egy harmadfokú egyenlettel határozhatók meg, melynek két másik gyöke k-beli). Ekkor az R és O pontokon átmenő egyenes E-vel való harmadik metszéspontja lesz $P \oplus Q$.

5.1.1. állítás. *Az így definiált művelettel $E(k)$ Abel-csoport, melynek nulleleme O.*

Bizonyítás. [8]: III.2.2.

A korábban bevezetett fogalommal azt mondhatjuk tehát, hogy az elliptikus görbe Abel-varietás, és valójában definiálhatjuk is az elliptikus görbéket úgy, mint 1 dimenziójú Abel-varietásokat ([9]: III.2.). Másrészt a következő állítás ([8]: III.3.4.) szerint ez a csoportművelet megkapható a $\mathrm{Pic}_0(E)$ összeadásából is, azaz E Jacobi-varietása önmaga:

5.1.2. állítás. *Legyen (E, O) elliptikus görbe. Ekkor minden $D \in \mathrm{Div}_0(E)$-hez egyértelműen létezik egy olyan $P \in E$ pont, amelyre D lineárisan ekvivalens a $(P) - (O)$ divizorral. Ez meghatároz egy $\sigma : \mathrm{Div}_0(E) \to E$ leképezést, ahol $\sigma(D)$ az így értelmezett P pont. A leképezés továbbá szürjektív, és $\sigma(D_1) = \sigma(D_2)$ pontosan akkor, ha D_1 és D_2 lineárisan ekvivalensek, azaz σ izomorfizmust létesít $\mathrm{Pic}_0(E)$ és E között. Ha E-t a Weierstrass-egyenletével adjuk meg, akkor a $\mathrm{Pic}_0(E)$ által indukált összeadás megegyezik az imént definiált $\oplus$ művelettel.*

5.1.3. következmény. *Legyen E elliptikus görbe, $D = \sum n_P(P) \in \mathrm{Div}(E)$. D pontosan akkor függvénydivizor, ha $\sum n_P = 0$ és $\sum n_P P = O$ (mint az elliptikus görbe pontjain értelmezett összeadás).*

Bizonyítás. A 2.1.9. állítás szerint függvénydivizorok foka 0. Ha most $D \in \mathrm{Div}_0(E)$, akkor az előző állítás szerint D pontosan akkor függvénydivizor, ha $\sigma(D) = O$, ami pedig azzal ekvivalens, hogy $\sum n_P \sigma((P)-(O)) = O$. Viszont $\sigma((P) - (O)) = P$, ami éppen a kívánt összefüggéshez vezet. □

A Weierstrass-egyenletet használva az elliptikus görbe további állandói is meghatározhatók. Ha az alaptest karakterisztikája nem 2, akkor y-t $\frac{1}{2}(y - a_1x - a_3)$-mal helyettesítve az egyenlet

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

alakúra hozható, ahol $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ és $b_6 = a_3^2 + 4a_6$. Definiálhatjuk a további mennyiségeket:

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 4b_4,$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$
$$j = \frac{c_4^3}{\Delta}.$$

Az így definiált Δ-t a Weierstrass-egyenlet *diszkriminánsának*, míg j-t az E elliptikus görbe *j-invariánsának* nevezzük. A Weierstrass-egyenlettel meghatározott görbe pontosan akkor sima, ha $\Delta \neq 0$, továbbá két elliptikus görbe pontosan akkor izomorf ($\bar{k}$ fölött), ha a j-invariánsuk megegyezik ([8]: III.1.4.).

Most p-adikus testek feletti elliptikus görbék egy speciális típusára térünk rá, melyek a Tate-görbék. Ehhez először definiáljuk a következő q paraméterű formális végtelen sorokat:

$$s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n}, \quad a_4(q) = -5s_3(q), \quad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}.$$

Ha $\sigma_k(n)$ jelöli az n pozitív egész osztóinak k-adik hatványösszegét, akkor az $s_k(q)$ sor nem más, mint a $\sigma_k(n)$-ből mint együtthatókból álló hatványsor, ugyanis:

$$\sum_{n=1}^{\infty} \sigma_k(n)q^n = \sum_{n=1}^{\infty}\sum_{d|n} d^k q^n = \sum_{d=1}^{\infty}\sum_{l=1}^{\infty} d^k q^{ld} = \sum_{d=1}^{\infty} d^k \sum_{l=1}^{\infty} (q^d)^l = \sum_{d=1}^{\infty} d^k \frac{q^d}{1-q^d}.$$

A hatványsor-alakból, illetve az átalakításokból leolvasható, hogy a sor konvergens (a diszkrét értékelésből származó normára nézve), ha $\|q\| < 1$, azaz ha $v(q) > 0$. Továbbá az is látható, hogy mind a_4, mind a_6 együtthatói egészek, a_6 esetében ugyanis

$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12} = -\sum_{n\geq 1} \frac{5\sigma_3(n) + \sigma_5(n)}{12} q^n = -\sum_{n\geq 1} \left(\sum_{d|n} \frac{5d^3 + 7d^5}{12} \right) q^n,$$

és $5d^3 + 7d^5 \equiv 0 \mod 12$ minden $d \in \mathbb{Z}$ esetén.

5.1.4. definíció. *Legyen k p-adikus test, v diszkrét értékeléssel és az abból származó normával. Legyen $q \in k^*$ tetszőleges elem, melyre $\|q\| < 1$. A k fölötti, q paraméterű E_q Tate-görbének nevezzük azt az elliptikus görbét, amelyet a következő Weierstrass-egyenlet definiál:*

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q).$$

Jelölje

$$q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\} \subseteq \mathbb{Q}_p^*.$$

A következő tétel alapján a Tate-görbe (mint Abel-csoport) megkapható a $\bar{k}^*$ multiplikatív csoport faktoraként is:

5.1.5. tétel. *Az E_q sima elliptikus görbe, melynek diszkriminánsa*

$$\Delta = q\prod_{n\geq 1}(1-q^n)^{24},$$

j-invariánsa pedig

$$j(E_q) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n,$$

ahol a $c(n)$-ek egészek. Továbbá megadható izomorfizmus

$$E_q(\bar{k}) \cong \bar{k}^*/q^{\mathbb{Z}},$$

amely izomorfizmus kompatibilis a $G_k = \mathrm{Gal}(\bar{k}/k)$ Galois-csoport hatásával, azaz minden L/k véges bővítésre

$$E_q(L) \cong L^*/q^{\mathbb{Z}}.$$

Bizonyítás. A definícióba való helyettesítéssel

$$\Delta(q) = -a_6 + a_4^2 - 64a_4^3 - 432a_6^2 + 72a_4a_6$$

adódik, amibe a_4 és a_6 hatványsorát beírva

$$\Delta(q) = q - 24q^2 + \dots$$

összefüggést kapunk, viszont ekkor $v(\Delta(q)) = v(q)$ (használva, hogy $v(q) > 0$), és így $\|\Delta(q)\| = \|q\| \neq 0$, azaz valóban sima görbét definiáltunk. A Δ-ra és j-re vonatkozó képletek [9]: V.1.1c szerint igazak $q \in \mathbb{C}$-re az 1-nél kisebb abszolút értékű komplex számok esetén, de ekkor formális hatványsorként $\mathbb{Z}[[q]]$-ban is igaz lesz, és emiatt 1-nél kisebb normájú q-k esetén k-ban is. Az

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q),$$

$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q)$$

sorok konvergálnak $u \in \bar{k}^*$, $u \notin q^{\mathbb{Z}}$ esetben, és az

$$u \mapsto \begin{cases} (X(u,q), Y(u,q)) & \text{ha } u \notin q^{\mathbb{Z}} \\ O & \text{ha } u \in q^{\mathbb{Z}} \end{cases}$$

leképezés szürjektív homomorfizmust definiál $\bar{k}^*$-ról $E_q(\bar{k})$-ra ([9]: V.3.1c). Ennek magja éppen $q^{\mathbb{Z}}$, ami éppen a kívánt izomorfiához vezet. Végül az 1.2.7. lemma bizonyítása során már említettek miatt a $\sigma \in \mathrm{Gal}(L/k)$ megőrzi az értékelést L-en, és emiatt konvergens sorokra is $(\sum \alpha_i)^\sigma = \sum \alpha_i^\sigma$. Ezt $X(u,q)$-ra és $Y(u,q)$-ra alkalmazva kapjuk, hogy a Galois-csoport hatásával kompatibilis a megadott izomorfizmus. Továbbá az

$$1 \to q^{\mathbb{Z}} \to \bar{k}^* \to E_q(\bar{k}) \to 0$$

rövid egzakt sorra a $G_L = \mathrm{Gal}(\bar{k}/L)$ Galois-csoport szerinti kohomológiát véve az

$$1 \to q^{\mathbb{Z}} \to L^* \to E_q(L) \to H^1(G_L, q^{\mathbb{Z}})$$

egzakt sort kapjuk. Viszont $q \in k$ miatt G_L hatása triviális $q^{\mathbb{Z}}$-n, azaz $H^1(G_L, q^{\mathbb{Z}})$ a G_L provéges csoportnak a $q^{\mathbb{Z}} \cong \mathbb{Z}$ diszkrét csoportba menő folytonos homomorfizmusaiból áll, az pedig csak triviális lehet, és így $E_q(L) \cong L^*/q^{\mathbb{Z}}$. □

A Tate-görbe függvénytestének további vizsgálatához vezessük be a következő $\vartheta : \bar{k}^* \to \bar{k}$ függvényt:

$$\vartheta(u) = (1-u) \prod_{n \geq 1} \frac{(1-q^n u)\left(1-\frac{q^n}{u}\right)}{(1-q^n)^2}.$$

A végtelen szorzat konvergál pozitív értékelésű q-kra, így ϑ jóldefiniált. Továbbá

$$\vartheta(qu) = (1-qu) \prod_{n \geq 1} \frac{(1-q^{n+1}u)\left(1-\frac{q^{n-1}}{u}\right)}{(1-q^n)^2} =$$

$$= \left(1-\frac{1}{u}\right) \prod_{n \geq 1} \frac{(1-q^n u)\left(1-\frac{q^n}{u}\right)}{(1-q^n)^2} = -\frac{1}{u}\vartheta(u)$$

függvényegyenlethez jutunk a tényezők sorrendjének átrendezésével.

Tetszőleges $a \in \bar{k}^*$-ra vezessük be a ϑ_a jelölést arra a függvényre, amelyet a

$$\vartheta_a(u) = \vartheta\left(\frac{u}{a}\right)$$

összefüggés definiál. Legyen valamilyen $\bar{k}^*$-beli μ, t_i és s_i értékekkel

$$h = \mu \frac{\prod \vartheta_{t_i}}{\prod \vartheta_{s_i}}.$$

Ha továbbá $h(qu) = h(u)$ teljesül, akkor h indukál egy $\bar{k}^*/q^{\mathbb{Z}} \to \bar{k}$ függvényt. Az előző tétel szerint ez tekinthető egy $E(\bar{k})$-ról képező függvénynek is, azaz h ilyenkor a $K(\bar{E})$ függvénytest egy elemének megfeleltethető. Az iménti függvényegyenletét használva

$$h(qu) = \mu \frac{\prod \vartheta_{t_i}(qu)}{\prod \vartheta_{s_i}(qu)} = \mu \frac{\prod \vartheta\left(\frac{qu}{t_i}\right)}{\prod \vartheta\left(\frac{qu}{s_i}\right)} = \mu \frac{\prod -\frac{t_i}{u}\vartheta\left(\frac{u}{t_i}\right)}{\prod -\frac{s_i}{u}\vartheta\left(\frac{u}{s_i}\right)} = \left(-\frac{1}{u}\right)^{\#t_i - \#s_i} \frac{\prod t_i}{\prod s_i} h(u),$$

és így ez akkor lesz $h(u)$-val egyenlő, ha (1) $\prod t_i = \prod s_i$, továbbá (2) az s_i-k és t_i-k száma megegyezik. Másrészt ha a felülvonással a $\bar{k}^* \to \bar{k}^*/q^{\mathbb{Z}}$ természetes leképezést jelöljük (ahol ez utóbbira mint az $E(\bar{k})$ pontjaira tekintünk), akkor h divizora a következőképpen adható meg (hiszen ϑ éppen $q^{\mathbb{Z}}$-ben tűnik el):

$$\mathrm{div}(h) = \sum \bar{t}_i - \sum \bar{s}_i.$$

Az 5.1.3. következmény szerint ez a divizor pontosan akkor függvénydivizor, ha az iménti (1) és (2) feltételek teljesülnek.

A későbbi konstrukcióhoz még a *homogén terek* fogalmát kell bevezetnünk.

5.1.6. definíció. *Legyen E elliptikus görbe a k test fölött. Egy X/K sima görbét E-hez tartozó torzornak (principal homogeneous space, „fő"-homogén térnek) nevezünk, ha adott E-nek egy egyszeresen tranzitív algebrai csoporthatása rajta, azaz a torzor egy (X, μ) párnak tekinthető, ahol X/K sima görbe és $\mu : X \times E \to X$ k feletti morfimzus, amely a következő feltételeket teljesíti:*

(1) *$\mu(p, O) = p$ minden $p \in X$ esetén;*

(2) *$\mu(\mu(p, P), Q) = \mu(p, P + Q)$ minden $p \in X$ és $P, Q \in E$-re;*

(3) *minden $p, q \in X$ esetén egyértelműen létezik egy olyan $P \in E$, amelyre $\mu(p, P) = q$.*

A $\mu(p, P)$-t szokás egyszerűen $p + P$-vel is jelölni, a Tate-görbék esetén pedig a multiplikatív jelölést fogjuk használni, hiszen az elliptikus görbe a $\bar{k}^*$ multiplikatív csoport egy faktorának is tekinthető. Két E-hez tartozó X_1, X_2 torzort *ekvivalensnek* tekintünk, ha létezik olyan $\psi : X_1 \to X_2$ izomorfizmus,

amely kompatibilis E hatásával, azaz $\psi(p+P) = \psi(p)+P$. Maga E is tekinthető torzornak, ahogy a transzlációval hat önmagán, E ekvivalenciaosztályát *triviális osztálynak* nevezzük. Az ekvivalenciaosztályokon csoportstruktúra is megadható, ezt a csoportot az E/k-hoz tartozó *Weil-Châtelet-csoportnak* nevezzük. A homogén terek tulajdonságait [8]: X.3. foglalja össze. Itt annyit elevenítünk fel belőle, hogy továbbra is G_k-val jelölve a k abszolút Galois-csoportját, a torzorok ekvivalenciaosztályai megfeleltethetők a $H^1(G_k, E(\bar{k}))$ kohomológiacsoport elemeinek, méghozzá az $X \mapsto \{\sigma \mapsto p_0^\sigma - p_0\}$ megfeleltetéssel, ahol $p_0 \in X$ tetszőleges pont. Belátható ([8]: X.3.6.), hogy ez a megfeleltetés ekvivalens torzorokhoz azonos kohomológiaosztályba tartozó kociklusokat feleltet meg, továbbá bijekciót létesít. A későbbi konstrukcióhoz még szükséges annak felidézése, hogy egy adott ξ 1-kociklushoz hogyan definiálunk torzort, ami a csavart formák általánosabb elméletéből adható meg.

5.1.7. definíció. *Legyen X sima görbe k fölött, jelölje* $\mathrm{Isom}(X)$ *$\bar{X}$ ($\bar{k}$ fölötti) önmagára való izomorfizmusainak csoportját. X egy X' csavarásának nevezünk egy vele $\bar{k}$ fölött izomorf görbét. Két csavarás ekvivalens, ha k fölött izomorfak.*

Ha X' X egy csavarása, akkor tehát megadható egy $\psi : \bar{X} \to \bar{X}'$ $\bar{k}$ fölötti izomorfizmus. A $\xi : G_k \to \mathrm{Isom}(X)$, $\xi_\sigma = \psi^\sigma\psi^{-1}$ definícióval megadott leképezés G_k egy 1-kociklusát adja meg $\mathrm{Isom}(X)$-be, amelynek $H^1(G_k, \mathrm{Isom}(X))$-beli osztályát egyértelműen meghatározza X' k-beli izomorfiaosztálya. Ezek szerint az X csavarásai megfeleltethetők $H^1(G_k, \mathrm{Isom}(X))$-beli osztályoknak, ráadásul ez a megfeleltetés bijekció ([8]: X.2.2.).

Ha most adott az E elliptikus görbén egy ξ 1-kociklus, akkor ez tekinthető $H^1(G_k, \mathrm{Isom}(E))$ egy elemét reprezentáló 1-kociklusnak is, hiszen E beágyazható $\mathrm{Isom}(E)$-be a $P \mapsto \tau_P$ megfeleltetéssel, ahol τ_P a P szerinti transzláció (P hozzáadása az elliptikus görbe pontjain definiált összeadás szerint). Az előzőek miatt tehát ξ-hez tartozik E egy csavarása, azaz megadható egy olyan X sima görbe és egy $\psi : \bar{X} \to \bar{E}$ izomorfizmus, melyre minden $\sigma \in G_k$ esetén $\varphi^\sigma \circ \psi^{-1}$ a $-\xi_\sigma$-val való transzlációval egyezik meg. Ha definiáljuk a $\mu : X \times E \to X$,

$$\mu(p, P) = \psi^{-1}(\psi(p) + P)$$

leképezést, akkor X valóban E-hez tartozó torzor lesz ([8]: X.3.6.). A ξ-hez tartozó X homogén tér tehát egy 1 génuszú görbe (hiszen az algebrai lezárt felett izomorf egy elliptikus görbével), amelyen a G_k Galois-csoport a ξ szerinti csavart hatással hat. Ha tehát $p \in \bar{X}$, akkor

$$\psi^\sigma\psi^{-1}(\psi(p^\sigma)) = \psi(p^\sigma) - \xi_\sigma,$$

azaz $\psi(p)^\sigma = \psi^\sigma(p^\sigma) = \psi(p^\sigma) - \xi_\sigma$, és így

$$\psi(p^\sigma) = \psi(p)^\sigma + \xi_\sigma.$$

Speciálisan, az $X(k)$ k feletti pontok úgy adhatók meg mint amelyek invariánsak a csavart hatásra nézve, azaz

$$X(k) = \{p \in X(\bar{k}) : \psi(p) = \psi(p)^\sigma + \xi_\sigma\}.$$

Ha E_q a q paraméterű Tate-görbe, akkor az így megkapott X görbére is $X(\bar{k}) \cong \bar{k}^*/q^{\mathbb{Z}}$ teljesül. A továbbiakban el is hagyjuk a ψ izomorfizmus jelölését, hiszen mind $E(\bar{k})$, mind $X(\bar{k})$ elemeire ugyanúgy gondolunk mint $\bar{k}$ faktorára. Meg kell viszont különböztetnünk a Galois-csoport kétféle hatását: $\bar{t}^\sigma$ jelöli a szokásos Galois-hatást a $\bar{t} \in E(\bar{k})$ elemen, míg $\sigma(\bar{t})$ a csavart Galois-hatást X-en, melyet a

$$\sigma(\bar{t}) = \xi_\sigma \bar{t}^\sigma$$

összefüggés ad meg (ahol a $\bar{k}^*$-ból származó szorzás szerepel a jobb oldalon).

5.2. Adott indexű és periódusú görbék a $g = 1$ esetben

Most tehát legyen adott egy k p-adikus test, és legyen adott egy P pozitív egész szám. A 4.2.1. tétel (3) állítása értelmében az $I = P$ feltétel szükséges ahhoz, hogy az $(1, P, I)$ hármas lokálisan megengedett legyen. Tehát olyan 1 génuszú k feletti X sima görbét akarunk konstruálni, melynek indexe és periódusa is P-vel egyezik meg.

5.2.1. tétel (Sharif). *Minden P pozitív egészhez megadható olyan X 1 génuszú sima görbe k fölött, melyre $P(X) = I(X) = P$.*

Bizonyítás. Jelölje π a k értékeléséhez tartozó értékelésideál egy generátorelemét, és legyen $q = \pi^P$. Tekintsük az E q paraméterű Tate-görbét, jelölje k_P a k-nak az 1.2.5 állítás alapján egyértelműen létező P fokú nem elágazó bővítését. Ha κ jelöli a k, továbbá κ_P a k_P maradéktestét, akkor $\mathrm{Gal}(k_P/k) \cong \mathrm{Gal}(\kappa_P/\kappa)$, ez utóbbi pedig egy véges testbővítés Galois-csoportja, melyet a κ elemszámának megfelelő hatványozás által megadott Frobenius-endomorfizmus generál. Ez alapján tekinthetjük a Frobenius-elemet mint $\mathrm{Gal}(k_P/k)$ elemét is, jelölje ezt σ. Tekintsük azt a $\mathrm{Gal}(k_P/k) \to E(\bar{k})$ homomorfizmust, amelyet a $\sigma \mapsto \bar{\pi}$ definiál. (Továbbra is azonosítjuk $E(\bar{k})$-t

$\bar{k}^*/q^{\mathbb{Z}}$-vel, ahol a felülvonás a $\bar{k}^*$-beli elemeknek az utóbbi faktorban szereplő képét jelenti.) Használva, hogy

$$\mathrm{Gal}(k_P/k) \cong \mathrm{Gal}(\bar{k}/k)/\mathrm{Gal}(\bar{k}/k_P) = G_k/G_{k_P},$$

ez a homomorfizmus a faktoron keresztül meghatároz egy $G_k \to E(\bar{k})$ homomorfizmust, amit ξ-vel jelölünk. Mivel ξ képe $E(k)$-beli, ezért invariáns a Galois-hatásra, azaz tekinthető egy $H^1(G_k, E(\bar{k}))$-beli elemet reprezentáló 1-kociklusnak is.

Tekintsük az előző pont szerint ξ-hez tartozó X torzort, ami tehát egy 1 génuszú görbe, melyre $X(\bar{k}) \cong \bar{k}^*/q^{\mathbb{Z}}$, és a csavart Galois-hatást ξ határozza meg. Idézzük fel, hogy ez azt jelenti, hogy egy $t \in \bar{k}^*$ esetén

$$\gamma(\bar{t}) = \xi_\gamma \bar{t}^\gamma$$

adja meg a Galois-hatást ($\gamma \in G_k$).

Ha σ-t felemeljük a G_k egy szintén σ-val jelölt elemére, akkor ezúttal

$$\sigma(\bar{t}) = \xi_\sigma \bar{t}^\sigma = \bar{\pi}\bar{t}^\sigma.$$

Ha $\gamma \in G_{k_P}$ tetszőleges elem, akkor persze $\sigma\gamma$ szintén σ-ra képződik $\mathrm{Gal}(k_P/k)$-ban, így

$$\sigma\gamma(\bar{t}) = \bar{\pi}\bar{t}^{\sigma\gamma}.$$

Ebből $t = 1$ választással leolvasható, hogy

$$\sigma\gamma(\bar{1}) = \bar{\pi}\bar{1}^{\sigma\gamma} = \bar{\pi},$$

másrészt

$$\sigma\gamma(\bar{1}) = \sigma(\gamma(\bar{1})) = \bar{\pi}\gamma(\bar{1})^\sigma,$$

ami miatt

$$\gamma(\bar{1}) = \gamma(\bar{1})^\sigma = \bar{1},$$

és így $\bar{1} \in X(k_P)$. Azaz X-nek van k_P-racionális pontja, emiatt az $I(X)$ index P osztója.

Most legyen L egy olyan véges bővítése k-nak, amelyre $X(L) \neq \emptyset$. Megmutatjuk, hogy L tartalmazza k_P-t. Ehhez legyen $\bar{t} \in X(L)$, és legyen $\tau \in G_L$. Ekkor

$$\bar{t} = \tau(\bar{t}) = \xi_\tau \bar{t}^\tau.$$

Ahogy az 1.2.7. lemma bizonyítása során már beláttuk, τ megőrzi az értékelést, így

$$v(\bar{t}) = v(\xi_\tau) + v(\bar{t}^\tau) \equiv v(\xi_\tau) + v(\bar{t}) \mod P$$

miatt $v(\xi_\tau) \equiv 0 \mod P$. Viszont ξ definíciója miatt ebből az is következik, hogy $\xi_\tau = \bar{1}$, azaz τ benne van a

$$G_L \to G_L/G_{k_P} \leq G_k/G_{k_P} \cong \mathrm{Gal}(k_P/k)$$

leképezés magjában. Azaz $\tau \in G_{k_P}$, így $G_L \leq G_{k_P}$, azaz k_P tartalmazza L-et.

Ezzel azt is beláttuk, hogy P osztója az $I(X)$ indexnek, így Lichtenbaum tételével együtt a $P(X) = I(X) = P$ összefüggéshez jutunk, tehát X valóban a kívánt feltételeknek eleget tevő görbe. □

5.3. Tetszőleges génuszú görbe konstrukciója

Most rátérünk az általános esetben történő konstrukcióra, azaz célunk olyan görbét konstruálni, amely a Lichtenbaum-tétel által lokálisan megengedett génusszal, periódussal, indexszel rendelkezik.

5.3.1. tétel (Sharif). *Legyen k p-adikus test, $g > 1$ pozitív egész, és legyen (g, P, I) lokálisan megengedett számhármas. Ekkor létezik olyan Y sima g génuszú projektív görbe k fölött, melyre $P(Y) = P$ és $I(Y) = I$.*

A konstrukció az 1 génuszú eset által megadott görbéből indul ki, X tehát jelölje az előző pontban meghatározott görbét. Legyen $f \in K(X)^*$ olyan eleme a függvénytestnek, melyre $f \notin K(\bar{X})^{*2}$. Ekkor a $K(\bar{X}) \hookrightarrow K(\bar{X})(\sqrt{f})$ leképezés a függvénytestnek egy valódi másodfokú bővítésbe történő beágyazását adja meg. Ez [8]: II.2.5. megjegyzése alapján indukál egy $\varphi : \bar{Y} \to \bar{X}$ leképezést, ahol Y sima, projektív, az algebrai lezárt felett is irreducibilis görbe és $K(\bar{Y}) = K(\bar{X})(\sqrt{f})$ (illetve $K(Y) = K(X)(\sqrt{f})$). Ekkor φ másodfokú morfizmus, és így véges sok pont kivételével az X-beli pontok fölött két őskép lesz. A $P \mapsto [f(P), 1]$ illetve $Q \mapsto [\sqrt{f}(P), 1]$ hozzárendelésekkel megadott $X \to \mathbb{P}^1$ és $Y \to \mathbb{P}^1$ racionális leképezések morfizmusokká terjednek ki, és a projektív egyenesen az $[u, v] \mapsto [u^2, v^2]$ által megadott leképezés teszi kommutatívvá a következő diagramot:

$$\begin{array}{ccc} \bar{Y} & \xrightarrow{[f:1]} & \mathbb{P}^1 \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle [u^2:v^2]} \\ \bar{X} & \xrightarrow{[\sqrt{f}:1]} & \mathbb{P}^1 \end{array}$$

$Y(\bar{k})$ pontjai ez alapján koordinátázhatók (a, Q) párokkal, ahol $Q \in X(\bar{k})$ a φ szerinti vetület, és $a \in \bar{k}$, ahol $a^2 = f(Q)$, kivéve ha Q-ban f-nek

pólusa van, amikor is a „végtelenbeli" pontokról beszélhetünk. A 2.1.7. állítás alapján minden $Q \in X(\bar{k})$-ra a Q ősképeinek elágazási indexeinek összege 2, ami alapján Q vagy elágazási pont, ha egyetlen P ősképe van, amelynek 2 az elágazási indexe, vagy nem elágazó, ha két 1 elágazási indexű ősképpel rendelkezik. Nyilván az előbbi csak f gyökeinél és pólusainál fordulhat elő. Most megmutatjuk, hogy pontosan a $\operatorname{div}(f)$-ben páratlan multiplicitással előforduló pontok lesznek az elágazási pontok.

Legyen először $v_Q(f) = 2k$, azaz ilyenkor $f = t^{2k}u$ alakban írható, ahol t lokális paraméter Q-ban és u egység az $O_{X,Q}$ lokális gyűrűben. Ilyenkor a $K(\bar{X})(\sqrt{f})$ $a + b\sqrt{f}$ elemei írhatók $a + bt^k\sqrt{u}$ alakban is megfelelő $\sqrt{u}$ elemmel. Ha most $a+bt^k\sqrt{u} \in M_P$ egy $P \in Y(\bar{k})$ pontbeli maximális ideálra, akkor u reguláris és nem tűnik el P-ben (mert akkor Q-ban is eltűnne), és így $v_P(\sqrt{u}) = 0$ is teljesül. De ekkor

$$a + bt^k\sqrt{u} \in M_P \Leftrightarrow a, bt^k \in M_P \Leftrightarrow a, bt^k \in (t),$$

és így t generálja az M_P ideált, ezért $e_\varphi(P) = 1$. Ha $v_Q(f) = 2k + 1$, akkor $f = t^{2k+1}u$, és ilyenkor a testbővítés elemei $a+bt^k\sqrt{t}\sqrt{u}$ alakba is írhatók. Ha most $a = 0$, $b = t^{-k}$ $K(\bar{X})$-beli együtthatókat választunk, akkor megkapjuk a $\sqrt{tu}$ függvényt, amely P-ben eltűnik, hiszen $\sqrt{t}(P)^2 = t(P) = 0$, azaz $\sqrt{tu} \in M_P$, és így a P-beli értékelése pozitív. Ekkor

$$v_P(t) = v_P(tu) = 2v_P(\sqrt{tu}) \geq 2,$$

másrészt az elágazási index legfeljebb 2 lehet, azaz $e_\varphi(P) = 2$ ilyenkor.

Az elágazási pontok összeszámolásával meghatározhatjuk az Y görbe génuszát és periódusát. Ehhez először tekintsük az f gyökdivizorát, ami G_k-invariáns (hiszen $K(X)^*$-beli függvényből indulunk ki), így a benne páratlan multiplicitással szereplő pontok is G_k-invariáns divizort alkotnak (hiszen ezek egymás között permutálódnak), így ezek száma m_1P valamilyen m_1 egésszel (ahol $P = P(X) = I(X)$ az X görbe indexe és periódusa). Hasonlóképpen, f pólusdivizorában m_2P a páratlan multiplicitással szereplő pontok száma valamilyen m_2 egésszel. Továbbá az is igaz, hogy m_1 pontosan akkor páros, ha a gyökdivizor foka P páros többszöröse, míg m_2 akkor, ha a pólusdivizorra ez teljesül. Másrészt $\deg \operatorname{div}(f) = 0$, ezért a gyök- és pólusdivizor foka megegyezik, tehát m_1 és m_2 paritása megegyezik, így az összes elágazási pont száma mindenképpen P páros számú többszöröse, legyen ez $2mP$.

A $g(Y)$ génuszt a Riemann–Hurwitz-formula (2.3.6.) alkalmazásával számolhatjuk ki. Esetünkben $g(X) = 1$, továbbá a képletben szereplő összegzés éppen az elágazási pontok számát adja meg, így $2g(Y) - 2 = 2mP$, azaz

$$g(Y) = mP + 1.$$

Ekkor Lichtenbaum tétele (a 4.2.1. tétel (1) pontja) miatt $P(Y)|mP$. Másrészt a 2.2.4. lemma alkalmazásával $P|P(Y)|2P$. Ha m páratlan, akkor ebből azonnal következik, hogy $P(Y) = P$. Páros m esetén $P(Y) = P$ vagy $P(Y) = 2P$, viszont Lichtenbaum tételének (3) állítása miatt ilyenkor az $I(Y)$ index megegyezik a periódussal, azaz ha ilyenkor belátjuk $I(Y) = P$-t, akkor abból $P(Y) = P$ is következik.

A továbbiakban tehát megmutatjuk, hogy megfelelő f függvény választásával minden eset előállhat: minden lokálisan megengedett (g, P, I) hármashoz lesz olyan f, amelyből az így konstruált Y megfelelő számú ($2mP = 2g - 2$) elágazási pontot tartalmaz. Külön vizsgáljuk majd az egyszerűbb $I = P$, illetve a bonyolultabb $I = 2P$ esetet (amikor is viszont m páratlan). Előtte azonban belátunk egy lemmát arról, hogy X egy k-racionális D divizora mikor áll elő függvénydivizorként. Ehhez $D = \sum a_i \bar{t}_i$ alakban írjuk fel, ahol $a_i \in \mathbb{Z}$, míg $\bar{t}_i \in X(\bar{k}) \cong \bar{k}^*/q^{\mathbb{Z}}$.

5.3.2. lemma. *A D egy $f \in K(X)$ függvény divizora pontosan akkor, ha $\sum a_i = 0$ és $\prod \bar{t}_i^{a_i} = \bar{1}$.*

Bizonyítás. Tekintsük a már többször előfordult

$$0 \to \bar{k}^* \to K(\bar{X})^* \to K(\bar{X})^*/\bar{k}^* \to 0$$

rövid egzakt sort, ahol $K(\bar{X})^*/\bar{k}^*$ az $\bar{X}$ függvénydivizorainak csoportjával egyezik meg. G_k-kohomológiát alkalmazva és Hilbert 90-es tételét használva

$$0 \to k^* \to K(X)^* \to H^0(G_k, K(\bar{X})^*/\bar{k}^*) \to H^1(G_k, \bar{k}^*) = 0$$

adódik, amiből következik, hogy $K(X)^*$ szürjektíven képződik az X-en vett függvénydivizorok csoportjára. Emiatt elég azt belátni, hogy a D mint $\bar{X}$ divizora pontosan a kívánt feltételek teljesülésekor függvénydivizor. Viszont [8]: X.3.8. szerint az X torzor $\mathrm{Pic}_0(\bar{X})$ csoportja kanonikusan izomorf E-vel (azaz E az X Jacobi-varietása), így D pontosan akkor függvénydivizor, ha E-n az. Ez az 5.1.3. következmény szerint akkor teljesül, ha nulladfokú, továbbá a divizorban szereplő $\sum m_i P_i$ összeadást mint E pontjainak összeadását elvégezve az O origót kapjuk. Az $X(\bar{k}) \cong \bar{k}^*/q^{\mathbb{Z}} \cong E(\bar{k})$ izomorfizmusok szerint ez pedig éppen a $\bar{t}_i$-k megfelelő hatványainak összeszorzását jelenti. □

Most $\mathrm{Div}(X)$-beli divizorokat definiálunk, amelyek segítségével fogjuk megadni majd a bizonyításban szereplő f függvényt. Legyen F/k Galois-bővítés, és vegyünk egy $t \in X(F)$ elemet. Definiáljuk a $\mathrm{Nm}^*_{F/k}(t)$ divizort a következőképpen:

$$\sum_{\gamma \in \mathrm{Gal}(F/k)} (\gamma(\bar{t})) = \sum_{\gamma \in \mathrm{Gal}(F/k)} (\xi_\gamma \bar{t}^\gamma),$$

ahol az összegzés $\mathrm{Div}(\bar{X})$-ben történik. Az így megadott divizor G_k elemeire invariáns, azaz valóban $\mathrm{Nm}^*_{F/k}(t) \in \mathrm{Div}(X)$. A tétel bizonyításának a menete mindkét esetben a következő lesz: előszöris felidézzük az 1.2.7. lemmát, amelyik szerint p-adikus testek tetszőleges F/k véges nem elágazó bővítése esetén megadható olyan $t \in F$ elem, melyre $F = k(t)$ és $\mathrm{Nm}_{F/k}(t) = 1$. Ilyen t segítségével adunk meg $\mathrm{Div}(X)$-beli normadivizort, amely az előző lemma szerint egy f függvény divizora lesz. Az f függvény által a korábbiakban ismertetett módon megadott Y pedig megfelelő számú elágazási ponttal, így megfelelő periódussal és indexszel rendelkezik majd. Az $I = 2P$ esetben pedig a Tate-görbén megadott ϑ függvény segítségével konkrétan meg is adjuk az f függvényt. Először azonban lássuk a bizonyítást az $I = P$ esetben!

Az 5.3.1. tétel bizonyítása ($I = P$ eset). Legyenek tehát adottak a megfelelő g és $I = P$ számok, és $m = \frac{g-1}{P}$ egész. Először tegyük fel, hogy $m = 1$. Válasszuk meg t-t az 1.2.7. lemma szerint az $F = k_P$ testhez (k_P továbbra is k egyértelműen létező, P-edfokú nem elágazó bővítését jelöli). Ekkor tehát $k_P = k(t)$ és t normája 1 a k_P/k bővítésben. Definiáljuk $D \in \mathrm{Div}(X)$-et:

$$D = \mathrm{Nm}^*_{k_P/k}(1) - \mathrm{Nm}^*_{k_P/k}(t).$$

Ha σ továbbra is a $\mathrm{Gal}(k_P/k)$-t generáló Frobenius-elem, akkor a csavart Galois-hatás definíciója szerint D-ben 1 multiplicitással éppen az $1, \overline{\pi}, \overline{\pi^2}, \ldots \overline{\pi^{P-1}}$ pontok szerepelnek, míg -1 együtthatóval a $\bar{t}, \overline{\pi t^\sigma}, \overline{\pi^2 t^{\sigma^2}}, \ldots \overline{\pi^{P-1} t^{\sigma^{P-1}}}$ pontok. Ebből leolvasható, hogy $\deg D = 0$, továbbá az 5.3.2. lemmában szereplő szorzat éppen $\mathrm{Nm}_{k_P/k}(t)$ reciproka, ami 1. A lemma szerint tehát D valamilyen $f \in K(X)^*$ függvény divizora.

Konstruáljuk meg a korábbi módon leírt f-hez tartozó Y görbét ($f \notin K(\bar{X})^{*2}$, hiszen a divizorában szerepelnek páratlan együtthatójú pontok). Mivel az $\mathrm{Nm}^*(t)$ orbitjában szereplő pontokat k_P/k bővítés primitív elemei adják meg, így ezek halmaza diszjunkt lesz a $\mathrm{Nm}^*(1)$-ben szereplő pontoktól, az elágazási pontok száma így $2P$, azaz Y génusza $g(Y) = P + 1 = g$. Az f gyökdivizorához tartozó pontok P fokú divizort alkotnak, így $I(Y)|P$. Másrészt ahogy már láttuk, $P|P(Y)|I(Y)$, ezért $P(Y) = I(Y) = P$.

Most legyen $m \geq 2$, és jelölje L és L' k-nak az egyértelműen létező nem elágazó $(m-1)P$, illetve mP fokú bővítését. Válasszunk az 1.2.7 lemma szerinti megfelelő elemeket $F = k_P, L$ és L' esetére, ezeket jelölje $t, t_L, t_{L'}$. Az $m = 2$ esetben t és t_L egymás konjugáltjai lehetnek, ilyenkor cseréljük ki t-t $\frac{t}{1+\pi}$-re, t_L-t pedig $t_L(1+\pi)$-re. Ezzel elérhetjük, hogy t, t_L és $t_{L'}$ konjugáltjai mindenképpen különbözőek legyenek, azaz a $\mathrm{Nm}^*_{k_P/k}(t), \mathrm{Nm}^*_{L/k}(t_L)$ és $\mathrm{Nm}^*_{L'/k}(t_{L'})$ divizorok tartói egymástól diszjunktak.

Tekintsük ekkor a

$$D = \mathrm{Nm}^*_{k_P/k}(t) + \mathrm{Nm}^*_{L/k}(t_L) - \mathrm{Nm}^*_{L'/k}(t_{L'})$$

divizort. Definíció szerint $D \in \mathrm{Div}(X)$, foka pedig 0, hiszen az összeadandók rendre P, $(m-1)P$ és $-mP$ fokúak. Ahhoz, hogy D függvénydivizor legyen, még az 5.3.2. lemma szerint azt kell ellenőriznünk, hogy $\bar{t}$, $\bar{t_L}$ és $\bar{t_{L'}}$ csavart Galois-hatással származó „konjugáltjaiból" származó elemek megfelelő szorzata (ahol a pólusoknál reciprokot veszünk) $\bar{1}$. De ez teljesül, hiszen

$$\frac{\prod_{i=0}^{P-1} \overline{\pi^i} t^{\sigma^i} \prod_{i=0}^{(m-1)P-1} \overline{\pi^i} t_L^{\sigma^i}}{\prod_{i=0}^{mP-1} \overline{\pi^i} t_{L'}^{\sigma^i}} = \frac{\mathrm{Nm}_{k_P/k}(t) \cdot \mathrm{Nm}_{L/k}(t_L)}{\mathrm{Nm}_{L'/k}(t_{L'})} = 1$$

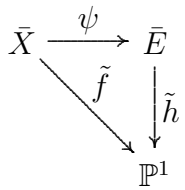
a $t, t_L, t_{L'}$ elemek megválasztásából.

Tehát $D = \mathrm{div}(f)$ valamilyen $f \in K(X)$, $f \notin K(\bar{X})^{*2}$ függvénnyel, ami így ismét meghatároz egy Y görbét. Az összes elágazási pont száma $P + (m-1)P + mP = 2mP$, így ilyenkor $g(Y) = mP + 1 = g$. Azon pontjai Y-nak, melyek $\mathrm{Nm}^*_{k_P/k}(t)$ fölött vannak, elágazóak, így P van belőlük. Ezek összege egy k-racionális divizort határoz meg, azaz $I(Y)|P$. Másrészt ismét $P|P(Y)|I(Y)$, így $P(Y) = I(Y) = P$, tehát az $I = P$ esetben a tételt bebizonyítottuk. □

Az $I = 2P$ eset bizonyításához további előkészületeket kell tennünk. Adottak tehát a g és $I = 2P$ pozitív egészek, és továbbra is $m = \frac{g-1}{P}$. Lichtenbaum tételének (4.2.1.) (3) állítása szerint m-nek páratlan egésznek kell lennie ahhoz, hogy (g, I, P) lokálisan megengedett legyen, ezt tehát mostantól feltételezzük. Jelölje L és L' a k mP, illetve $2mP$ fokú nem elágazó bővítését. Ismét az 1.2.7. lemma alkalmazásával megadhatunk olyan $s, t \in \bar{k}$ elemeket, melyekkel $L = k_P(s)$, $L' = k_P(t)$, továbbá $\mathrm{Nm}_{L/k_P}(s) = \mathrm{Nm}_{L'/k_P}(t) = 1$.

Az előző eset bizonyításához hasonlóan egy adott $D \in \mathrm{Div}(X)$ divizorhoz szeretnénk megfelelő $f \in K(X)^*$ függvényt találni, melyre $\mathrm{div}(f) = D$. A korábbi lemma az ilyen f létezését garantálta, de az csak k^*-beli elemmel való szorzás erejéig egyértelmű, és most ennél pontosabb meghatározásra lesz szükségünk. Ehhez pedig az 5.1. pontban a Tate-görbénél meghatározott h függvény lesz segítségünkre, előtte azonban még tisztáznunk kell, hogy hogyan térünk át az E q paraméterű Tate-görbére. Jelölje tehát ψ a rögzített $\bar{X} \to \bar{E}$ izomorfizmust (ahol továbbra is $\gamma \mapsto \psi^\gamma \circ \psi^{-1}$ adja meg azt az 1-kociklust, amely szerinti csavarással kaptuk X-et). Legyen $\tilde{f}$ az a $\bar{X} \to \mathbb{P}^1$ morfizmus, melyre a $Q \mapsto [f(Q), 1]$ racionális leképezés egyértelműen

kiterjed. Tekintsük a következő $\bar{k}$ fölötti görbékre vonatkozó kommutatív diagramot:



A $h \in K(\bar{E})^*$ függvényt fogjuk megkonstruálni, amely kiterjed egy $\tilde{h} : \bar{E} \to \mathbb{P}^1$ morfizmusra. Ez a diagram alapján meghatározza a $\tilde{f} = \tilde{h} \circ \psi$ morfizmust, amiből megkapjuk az $f \in K(\bar{X})^*$ függvényt. Megfelelően megválasztott h esetén az így kapott f valóban G_k-invariáns lesz, továbbá az előírt divizorral rendelkezik majd. A h függvényt az 5.1. pontban vizsgált $h = \mu \prod \vartheta_{t_i}/\vartheta_{s_i}$ alakban állítjuk elő. Nevezetesen legyen σ a $\mathrm{Gal}(L'/k)$ Frobenius-eleme (ez összhangban áll σ korábbi definíciójával) és jelölje x_i a ξ_{σ^i} valamilyen felemelését k^*-ra, válasszuk például π^j-t, ahol $j \in \{0, 1, \ldots, P-1\}$ és $i \equiv j \mod P$. Ezek segítségével válasszuk meg μ-t, s_i-t és t_i-t a következőképpen:

$$\mu = \pi,$$
$$t_i = x_i \cdot t^{\sigma^i},$$
$$s_i = x_i \cdot s^{\sigma^i},$$

ahol $i = 0, 1, \ldots, 2mP-1$. Az 5.1.-ben ismertettek miatt ahhoz, hogy h egy $K(\bar{E})^*$-beli függvényt adjon meg, az szükséges, hogy a t_i-k és az s_i-k szorzata megegyezzen (hiszen ugyanannyi tényezőből állnak). Ehhez pedig pontosan annak kell teljesülnie, hogy

$$\prod_{i=0}^{2mP-1} t^{\sigma^i} = \prod_{i=0}^{2mP-1} s^{\sigma^i}.$$

A bal oldalon a $\mathrm{Nm}_{L'/k}(t)$, a jobbon pedig $\mathrm{Nm}_{L'/k}(s)$ áll. Viszont $\mathrm{Nm}_{L'/k}(t) = \mathrm{Nm}_{k_P/k}(\mathrm{Nm}_{L'/k_P}(t)) = 1$, és hasonlóan $\mathrm{Nm}_{L'/k}(s) = (\mathrm{Nm}_{L/k}(s))^2 = 1$, tehát valóban teljesül az egyenlőség. Ekkor tehát h egy megfelelő függvényt definiál, amiből $\tilde{f} = \tilde{h} \circ \psi$ segítségével adhatjuk meg f-et.

5.3.3. lemma. *Az így definiált f függvény $K(X)^*$-ban van, továbbá*

$$\mathrm{div}(f) = \mathrm{Nm}^*_{L'/k}(t) - 2\mathrm{Nm}^*_{L/k}(s) = \mathrm{Nm}^*_{L'/k}(t) - \mathrm{Nm}^*_{L'/k}(s).$$

Bizonyítás. Először azt látjuk be, hogy $f \in K(X)^*$, amihez elegendő látni, hogy $f^\sigma = f$ (mert σ generálja a $\mathrm{Gal}(L'/k)$ csoportot). Ha $u \in \bar{k}$ tetszőleges, akkor $f^\sigma(\sigma(\bar{u})) = f(\bar{u})^\sigma$ definíció szerint (ahol $\sigma(\bar{u})$ a csavart Galois-hatást jelenti továbbra is), azaz $f^\sigma(\bar{u}) = f(\sigma^{-1}(\bar{u}))^\sigma$. Viszont

$$f^\sigma(\bar{u}) = (h \circ \psi)^\sigma(\bar{u}) = h(\psi(\sigma^{-1}(\bar{u})))^\sigma = h^\sigma(\psi(\sigma^{-1}(\bar{u}))^\sigma) = h^\sigma(\psi^\sigma(\bar{u})),$$

azaz

$$f^\sigma = h^\sigma \circ \psi^\sigma = h^\sigma \circ \xi_\sigma^{-1} \circ \psi,$$

ahol ξ_σ itt a π-vel való transzlációt jelenti (ugyanis $\psi^\sigma \circ \psi^{-1} = -\xi_\sigma$). Elegendő tehát azt megmutatni, hogy $h^\sigma \circ \xi_\sigma^{-1} = h$, vagy ezzel ekvivalensen $h^\sigma = h \circ \xi_\sigma$. Gondoljunk h-re úgy, mint q szerint periodikus függvényre $\bar{k}^*$-on. Ekkor $q \in k$ miatt σ a következőképpen hat a ϑ függvényeken:

$$\vartheta_a^\sigma(u) = \vartheta_a(u^{\sigma^{-1}})^\sigma = \vartheta\left(\frac{u^{\sigma^{-1}}}{a}\right)^\sigma = \vartheta\left(\frac{u}{a^\sigma}\right),$$

továbbá

$$\vartheta_a \circ \xi_\sigma(u) = \vartheta_a(u\pi) = \vartheta\left(\frac{u\pi}{a}\right) = \vartheta_{a/\pi}(u),$$

azaz $\vartheta_a^\sigma = \vartheta_{a^\sigma}$ és $\vartheta_a \circ \xi_\sigma = \vartheta_{a/\pi}$ teljesül minden $a \in \bar{k}^*$ elemmel. Így

$$\frac{h^\sigma}{h \circ \xi_\sigma} = \prod_{i=0}^{2mP-1} \frac{\vartheta_{t_i^\sigma}}{\vartheta_{t_i/\pi}} \frac{\vartheta_{s_i/\pi}}{\vartheta_{s_i^\sigma}}.$$

Viszont a $P|i$ indexek kivételével

$$t_{i-1}^\sigma \pi = (x_{i-1} t^{\sigma^{i-1}})^\sigma \pi = x_{i-1} \pi t^{\sigma^i} = x_i t^{\sigma^i} = t_i$$

teljesül, azaz ilyenkor $t_i/\pi = t_{i-1}^\sigma$, míg

$$t_{lP-1}^\sigma \pi = \pi\left(\pi^{P-1} t^{\sigma^{lP-1}}\right)^\sigma = \pi^P t^{\sigma^{lP}} = q t_{lP}.$$

Így mind a t-s, mind az s-s tényezők közül a P-vel nem osztható indexűek egyszerűsítés után eltűnnek, és marad a következő összefüggés:

$$\frac{h^\sigma}{h \circ \xi_\sigma} = \prod_{l=0}^{2m-1} \frac{\vartheta_{qt_{lP}/\pi}}{\vartheta_{t_{lP}/\pi}} \frac{\vartheta_{s_{lP}/\pi}}{\vartheta_{qs_{lP}/\pi}}.$$

Viszont ϑ függvényegyenlete miatt

$$\vartheta_{qt_{lP}/\pi}(u) = -\frac{u\pi}{qt_{lP}} \vartheta_{t_l P/\pi}(u),$$

így végül

$$\frac{h^\sigma}{h\circ\xi_\sigma}=\prod_{l=0}^{2m-1}\left(-\frac{u\pi}{qt_{lP}}\right)\left(-\frac{qs_{lP}}{u\pi}\right)=\prod_{l=0}^{2m-1}\frac{s_{lP}}{t_{lP}}=\mathrm{Nm}_{L'/k_P}\left(\frac{s}{t}\right)=1.$$

Ezzel tehát bebizonyítottuk, hogy $f\in K(X)^*$. Végül a kívánt divizoralak egyszerűen következik abból, hogy h divizora a korábbi megállapításunk szerint

$$\mathrm{div}(h)=\sum(\bar{t}_i)-\sum(\bar{s}_i)=\mathrm{Nm}^*_{L'/k}(t)-\mathrm{Nm}^*_{L'/k}(s)=\mathrm{Nm}^*_{L'/k}(t)-2\mathrm{Nm}^*_{L/k}(s),$$

és $\psi(\bar{u})=\bar{u}$ miatt f divizora is így áll elő. □

Ezek után az előkészítő lépések után visszatérhetünk Sharif konstrukciójához. Az így definiált f függvénnyel a korábbiak szerint konstruáljuk meg az Y görbét, továbbra is φ jelölje az $Y\to X$ vetítést. Ahogy már említettük, az f gyökei és pólusai felett lévő pontok kivételével $Y(\bar{k})$ pontjai (a,Q) párokkal koordinátázhatók, ahol $a\in\bar{k}$, $Q\in X(\bar{k})$, $\varphi((a,Q))=Q$ és $a^2=f(Q)$. Az 5.2.1. tétel bizonyításában (X konstrukciója során) leírtak miatt $k(Q)$ (a Q-t tartalmazó legkisebb racionális bővítés) tartalmazza a k_P testet. A következő lemmára azért lesz szükség, hogy megfontolásaink során ki tudjuk kerülni azt, hogy f gyökeit és pólusait külön vizsgálni kelljen.

5.3.4. lemma. *Legyen Y sima projektív görbe egy k test fölött, S jelölje $Y(\bar{k})$-beli pontok egy véges halmazát. Ha $D\in\mathrm{Div}(Y)$, akkor létezik olyan $D'\in\mathrm{Div}(Y)$, amelyik lineárisan ekvivalens D-vel, továbbá a tartója diszjunkt az S halmaztól.*

Bizonyítás. Legyen $S=\{P_1,P_2,\dots,P_r\}$, és jelölje n_i a P_i pont együtthatóját D-ben (ami persze 0 is lehet). A $K(Y)$ függvénytesten a P_i pontokhoz tartozó lokális gyűrűk által megadott diszkrét értékeléseket jelölje v_i. Ezek a függvénytest különböző diszkrét értékeléseit adják meg, hiszen ellenkező esetben a megfelelő lokális gyűrűk is megegyeznének, miközben különböző maximális ideálok szerint lokalizálunk. Először megadunk olyan f_i függvényeket, amelyre $v_i(f_i)=1$, továbbá $v_j(f_i)=0$ minden $j\neq i$ indexre. Ilyen függvényt az 1.1.5. approximációs lemma alkalmazásával határozhatunk meg: legyen ugyanis az ottani jelölések szerint $\alpha_i=t_i$ a P_i pontbeli lokális paraméter, továbbá $\alpha_j=1$ a konstans 1 függvény $j\neq 1$ esetén. A lemma szerint $N=1$-re létezik olyan f_i eleme a függvénytestnek, melyre $v_j(f_i-\alpha_j)>N$, így $v_i(f_i)=\min(v_i(f_i-t_i),v_i(t_i))=v_i(t_i)=1$, továbbá $v_j(f_i)=\min(v_j(f_i-1),v_j(1))=v_j(1)=0$ $j\neq i$-re. Ekkor az $f=\prod f_i^{n_i}$

olyan függvényt ad meg, amely az előírt P_i pontokban éppen n_i multiplicitású gyökkel vagy pólussal rendelkezik, a $D' = D - \mathrm{div}(f)$ divizor pedig éppen teljesíti a kívánt feltételeket. □

A tétel bizonyításához való utolsó lépésként a következő lemma pontosan meghatározza, hogy a már meghatározott X görbéhez egy valamilyen f által az eddigi módon megkonstruált Y indexe mikor egyezik meg éppen P-vel.

5.3.5. lemma. *Az $I(Y)$ index pontosan akkor P, ha létezik olyan $Q \in X(\bar{k})$, melyre $[k(Q) : k_P]$ páratlan és $f(Q) \in k(Q)^{*2}$.*

Bizonyítás. Először tegyük fel, hogy létezik ilyen $Q \in X(\bar{k})$ pont. Ekkor a Q-nak megfelelő, egyetlen zárt pontból álló divizort (az ilyen divizort *irreducibilisnek* nevezzük) D-vel jelölve a $\mathrm{Div}(X)$ csoportban, a 2.2.2. állításnak megfelelően D-t tekinthetjük a következő k-racionális $\mathrm{Div}(\bar{X})$-beli divizornak:

$$D = \sum_{\gamma \in \mathrm{Gal}(k(Q)/k)} (Q^\gamma).$$

Viszont a feltétel szerint létezik olyan $a \in k(Q)$, melyre $a^2 = f(Q)$, amivel tekinthetjük a következő $\mathrm{Div}(\bar{Y})$-beli D' divizort:

$$D' = \sum_{\gamma \in \mathrm{Gal}(k(Q)/k)} (a^\gamma, Q^\gamma).$$

Nyilván $\varphi_*(D') = D$ és $\deg D' = \deg D = [k(Q) : k] = lP$ valamilyen l páratlan számmal, továbbá $a \in k(Q)$ miatt D' is k-racionális divizor. Ekkor $I(Y)|lP$, másrészt a 2.2.4. lemma szerint $I(Y)|2I(X) = 2P$, tehát valóban $I(Y) = P$.

Az ellenkező irány bizonyításához tegyük fel, hogy $I(Y) = P$. Ekkor létezik Y-on k-racionális D' divizor, melynek foka P páratlan többszöröse, és az előző lemma miatt feltehetjük, hogy ez nem tartalmaz f gyökei és pólusai fölött lévő pontokat. Azt is feltehetjük továbbá, hogy D' irreducibilis (hiszen egy ilyen divizort a Galois-hatás szerinti orbitokra szétbontva kell lennie olyan orbitnak, melynek foka P páratlan többszöröse), $\deg D' = lP$, ahol l páratlan. Ha D'-re a korábbiakkal összhangban ismét $\mathrm{Div}(\bar{Y})$-beli divizorként gondolunk, akkor a következő alakban írható:

$$D' = \sum_{\gamma \in \mathrm{Gal}(k((a,Q))/k)} ((a, Q)^\gamma).$$

Viszont $(a, Q)^\gamma = (a^\gamma, Q^\gamma)$, és ha $f(Q) \notin k(Q)^{*2}$ teljesülne, akkor a $\mathrm{Gal}(k((a, Q))/k)$ Galois-csoportnak lenne olyan másodrendű eleme, amely $k(Q)$-t fixen hagyja,

de a-t és $-a$-t megcseréli. Ekkor viszont $\mathrm{Gal}(k((a,Q)/k)$, és így D' foka is P páros többszöröse lenne (mert $k \subseteq k_P \subseteq k(Q) \subseteq k((a,Q)))$, ami ellentmondás. Így tehát $f(Q) \in k(Q)^{*2}$ és $k((a,Q)) = k(Q)$. Ha most vesszük a $D = \varphi_*(D') \in \mathrm{Div}(\bar{X})$ divizort, akkor

$$D = \sum_{\gamma \in \mathrm{Gal}(k(Q)/k)} (\varphi((a,Q)^\gamma)) = \sum_{\gamma \in \mathrm{Gal}(k(Q)/k)} (\varphi((a,Q))^\gamma) = \sum_{\gamma \in \mathrm{Gal}(k(Q)/k)} (Q^\gamma).$$

D tehát szintén irreducibilis divizor, a foka pedig éppen $[k(Q) : k] = lP$, azaz $[k(Q) : k_P] = l$ páratlan. Ezzel a lemmát beláttuk. □

Az 5.3.1. tétel bizonyítása ($I = 2P$ eset). Adottak tehát a g és $I = 2P$ egészek, továbbá $m = \frac{g-1}{P}$ páratlan egész. Az 5.3.3. lemmában megadott f függvénnyel konstruáljuk meg az eddigiek alapján az Y görbét, melynek tehát $2mP$ elágazási pontja van. Emlékezhetünk arra, hogy ilyenkor $g(Y) = mP + 1 = g$, továbbá m páratlansága miatt $P(Y) = P$. Lichtenbaum tétele szerint tehát Y indexe vagy P, vagy $2P$. Az előző lemma segítségével kizárjuk az $I(Y) = P$ esetet. Legyen ugyanis $Q \in X(\bar{k})$ olyan, hogy $[k(Q) : k_P]$ páratlan. Megmutatjuk, hogy ilyenkor $f(Q) \notin k(Q)^{*2}$.

Legyen $Q = \bar{u}$ a korábbi jelölések szerint, ahol $u \in \bar{k}^*$. Jelölje K a $k(Q)$ és L testek kompozitumát, azaz $\bar{k}$-nak azt a legszűkebb résztestjét, amely tartalmazza mindkettőt. Mivel mind L, mind $k(Q)$ páratlan fokú Galois-bővítései k_P-nek, a $[K : k_P]$ fok is páratlan. Elegendő tehát azt megmutatnunk, hogy $h(\bar{u}) \notin K^{*2}$, ahol

$$h(\bar{u}) = \pi \prod_{i=0}^{2mP-1} \frac{\vartheta_{t_i}(u)}{\vartheta_{s_i}(u)}.$$

Viszont használva azt, hogy

$$t_{mP+i} = x_{mP+i} t^{\sigma^{mP+i}} = (x_i t^{\sigma^i})^{\sigma^{mP}} = t_i^{\sigma^{mP}},$$

illetve ugyanezért $s_{mP+i} = s_i^{\sigma^{mP}}$, a g definíciójában szereplő ϑ-s tényezők párokba rendezhetők σ^{mP} hatása szerint:

$$h(\bar{u}) = \pi \prod_{i=0}^{mP-1} \frac{\vartheta_{t_i}(u)\vartheta_{t_i}^{\sigma^{mP}}(u)}{\vartheta_{s_i}(u)\vartheta_{s_i}^{\sigma^{mP}}(u)}$$

Mivel σ^{mP} a $\mathrm{Gal}(L'/L)$ Galois-csoport nemtriviális eleme, és így a szorzatban éppen az $L'K/K$ bővítésből származó normák szerepelnek:

$$h(\bar{u}) = \pi \prod_{i=0}^{mP-1} \frac{\mathrm{Nm}_{L'K/K}(\vartheta_{t_i}(u))}{\mathrm{Nm}_{L'K/K}(\vartheta_{s_i}(u))} = \pi \mathrm{Nm}_{L'K/K} \left(\prod_{i=0}^{mP-1} \frac{\vartheta_{t_i}(u)}{\vartheta_{s_i}(u)} \right).$$

Másrészt $[K : k_P]$ páratlanságából következően $L'K \neq K$, hanem egy valódi másodrendű bővítésről van szó, amelyre ezek szerint

$$\frac{h(\bar{u})}{\pi} \in \mathrm{Nm}_{L'K/K}(L'K)^*.$$

Azonban $\pi \notin \mathrm{Nm}_{L'K/K}(L'K)^*$, hiszen akkor egy $1/2$ értékelésű elemnek lenne a normája. Márpedig ha $L' = L(\sqrt{w})$ és ugyanígy $L'K = K(\sqrt{w})$, akkor egy $a + b\sqrt{w} \in L'K$ elem értékelése csak úgy lehet nem egész, ha a vagy b értékelése nem egész (hiszen $\sqrt{w}$ egész értékelésű, mert L' nem elágazó bővítés), de az 1.2.1. tétel szerint a kiterjesztett értékelés nevezőjében a $[K : k_P]$ szerepelhet csak, ami pedig páratlan. Ekkor viszont $h(\bar{u})$ sincs a norma részcsoportjában, amely azonban másodrendű bővítés esetén tartalmazza a négyzet elemeket, tehát $h(\bar{u}) \notin K^{*2}$.

Az előző lemma szerint ilyenkor $I(Y) \neq P$, azaz Lichtenbaum tétele miatt biztosan $I(Y) = 2P = I$. Ezzel a bizonyítás végére értünk, hiszen Y kívánt génusszal, indexszel és periódussal rendelkező görbe. □

Megjegyzés. Itt csak p-adikus testek fölött konstruáltuk meg a megfelelő görbéket, de Lichtenbaum tétele (4.2.1.) a korábban említett módon általánosabb formában, lokális testek fölött is igaz. Sharif konstrukciója lényegében változatlan formában megismételhető tetszőleges lokális test fölött is, csak a k alaptest karakterisztikájáról fel kell tenni, hogy 2-től különbözik, ugyanis abban az esetben a 2 fokú φ leképezésre vonatkozóan *vad elágazási pontok* (wildly ramified points) is megjelenhetnek, amelyek módosítják a génusz és a periódus Riemann–Hurwitz-formula alapján történő kiszámolását.

Irodalomjegyzék

[1] Gille, Philippe and Szamuely Tamás. *Central Simple Algebras and Galois Cohomology.* Cambridge: Cambridge University Press, 2006.

[2] Lichtenbaum, Stephen. The Period-Index Problem for Elliptic Curves. *American Journal of Mathematics* **90** (1968), 1209-1223.

[3] Lichtenbaum, Stephen. Duality Theorems for Curves over p-adic Fields. *Inventiones Math.* **7** (1969), 120-136.

[4] Milne, J. S. *Arithmetic Duality Theorems.* Orlando: Academic Press, 1986. `http://www.jmilne.org/math/Books/adt1.pdf`

[5] Serre, Jean-Pierre. *Local Fields.* New York: Springer-Verlag, 1995.

[6] Serre, Jean-Pierre. *A Course In Arithmetic.* New York: Springer-Verlag, 1973.

[7] Sharif, Shahed. Curves with prescribed period and index over local fields. *Journal of Algebra* **314** (2007), 157-167.

[8] Silverman, Joseph H. *The Arithmetic of Elliptic Curves.* New York: Springer-Verlag, 1986.

[9] Silverman, Joseph H. *Advanced Topics in the Arithmetic of Elliptic Curves.* New York: Springer-Verlag, 1994.

[10] Szamuely Tamás. A Riemann-Roch tételről. *Matematikai Lapok* **1–2** (1993), 38-92.

[11] Szamuely Tamás. *Galois Groups and Fundamental Groups.* Cambridge: Cambridge University Press, 2009.

[12] Tate, John. *WC-groups over p-adic fields.* Séminaire N. Bourbaki, 1956-58, exp. no. 156, 265-277.

[13] Zariski, Oscar and Samuel, Pierre. *Commutative Algebra.* Vol. 2. New York: Springer-Verlag, 1960.