

Eötvös Loránd Tudományegyetem

Természettudományi Kar

Hasse becslése elliptikus görbék $\text{mod } p$ pontjainak számára

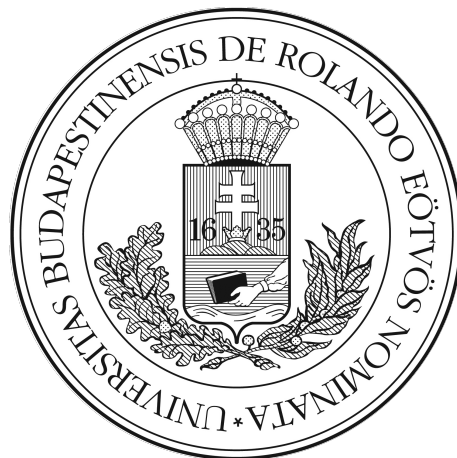
Szakdolgozat

Somogyi Dalma

Matematika BSc

Témavezető: Dr. Zábrádi Gergely

Algebra és Számelmélet Tanszék



Budapest, 2025

Tartalomjegyzék

1	Alapfogalmak	3
1.1	Affin varietások	4
1.2	Projektív varietások	5
2	A rend	6
3	Leképezések görbék között	10
3.1	Szeparábilis és tisztán inszeparábilis testbővítések	10
3.2	Morfizmusok	13
3.3	Az elágazási index	15
3.4	A Frobenius homomorfizmus	16
4	A divizorok	18
4.1	A divizor- és a Picard csoport	18
4.2	$\mathcal{L}(D)$	19
5	A differenciálformák	20
5.1	Néhány alapvető fogalom és állítás	20
5.2	Differenciálformák divizorjai	22
6	Az elliptikus görbék	24
6.1	A Weierstrass-egyenletek és elliptikus görbék	24
6.2	Csoportstruktúra az elliptikus görbéken	26
6.3	Elliptikus görbék divizor csoportja	28
7	Az izogéniák	30
7.1	Az izogéniák és az elliptikus görbe csoportstruktúrája	30
7.2	Kapcsolat az izogéniák tulajdonságai és a görbék algebrai struktúrája között	32
7.3	Az invariáns differenciál alkalmazása	33
7.4	A duális izogénia	35
8	Hasse becslése	38
9	Kitekintés: a Weil-sejtések	39
9.1	A varietás zeta függvénye és a Riemann féle zeta függvény	40
9.2	Véges testek feletti varietások kohomológiája	41

9.3	Alkalmazások	41
-----	------------------------	----

Köszönetnyilvánítás

Hálával tartozom mindazoknak, akik tanulmányaim során mellettem álltak, illetve támogattak e szakdolgozat elkészítésében. Külön köszönet illeti témavezetőmet, Dr. Zábrádi Gergelyt, aki útmutatásával, hasznos tanácsaival nagyban hozzájárult munkámhoz.

Bevezetés

A diofantoszi egyenletek olyan egész együtthatós, általában többváltozós polinomiális egyenletek, melyeket az egészek vagy a racionális számok körében szeretnénk megoldani. Ezek vizsgálata már az ókori görögöket is foglalkoztatta.

A kétváltozós diofantoszi egyenletek megoldhatóságát lineáris és másodfokú esetben már ismerjük: a lineáris $ax + by = c$ $a, b, c \in \mathbb{Z}, ab \neq 0$ alakúaknak pontosan $\gcd(a, b) | c$ esetén vannak egész megoldásaik, a másodfokúak racionális megoldhatóságát pedig a Hasse-Minkowski tétel karakterizálja (ld. [1] Serre: A Course in Arithmetic, Ch. IV., Thm. 8). Vegyük észre, hogy a síkon ezek egyeneseket, illetve kúpszeleteket írnak le.

A magasabb dimenziós diofantoszi egyenletek vizsgálata viszont már jóval nehezebbnek bizonyult (az általuk leírt görbék geometriailag bonyolultabbak), de a 20. században nagy előrelépések születtek ezek területén is. A kutatások első körben a harmadfokú, ún. elliptikus görbéket leíró egyenletekre irányultak, ugyanis az ezekhez kidolgozott módszerek a magasabb fokú egyenletekre is jó eséllyel átültethetők. Az elliptikus görbék aritmetikájának vizsgálata már komolyabb algebrai geometriai megfontolásokat is megkívánt, aminek hatására megszületett a diofantoszi geometria.

A Hasse-Minkowski tétel nyomán az elliptikus görbék esetén is a fő gondolat az, hogy egyet hátralépünk, és először is csak $\bmod p$ keressük a megoldásokat. Azonban míg a négyzetes egyenletek esetén ez már elég ahhoz, hogy $\mathbb{Q}^2$ felett is ismerjük a megoldhatóságot, a harmadfokú esetben még további vizsgálódások szükségesek.

Hasse tétele a harmadfokú egyenletek $\bmod p$ megoldásainak számára fog becslést adni.

Az állítás bizonyítása során központi eszközeink lesznek a görbék függvénytestje, divizorcsoportja, differenciálformái, amelyek segítségével az algebrai struktúrájuk lesz vizsgálható. Emellett időnként nem fogjuk tudni megkerülni az algebrai geometria használatát sem, az ehhez tartozó állítások közül viszont nem fogjuk belátni azokat, melyek túlságosan átlépnek a témánk kereteit.

Alapvetően [2] Silverman: The Arithmetic of Elliptic Curves című könyve nyomán fogunk haladni.

1 Alapfogalmak

Az egész dolgozatra vonatkozólag feltesszük, hogy K egy tökéletes test, ami azt jelenteni, hogy $\text{char}(K) = p$ (p prím) esetén minden eleme felírható egy p . hatványként. Ennek egy következménye, hogy minden irreducibilis polinom szeparábilis. Ugyanis tegyük fel, hogy $f(x) = a_n x^n + \dots + a_0 \in K[x]$ irreducibilisnek van többszörös gyöke. Ekkor a formális deriváltjának 0-nak kell lennie, azaz $f(x) = b_k x^{pk} + \dots + b_1 x^p + b_0 \in K[x]$ alakú. Mivel K perfekt, minden $i = 0, \dots, k$ -ra létezik $c_i \in K$, hogy

$b_i = c_i^p$, így $f(x) = (c_k x^k)^p + \dots + (c_1 x)^p + c_0^p = (c_k x^k + \dots + c_1 x + c_0)^p$ $\text{char}(K) = p$ miatt. Ez pedig ellent mond annak, hogy f irreducibilis.

K algebrai lezártját $\overline{K}$ fogja jelölni.

$\overline{K}|K$ pedig egy Galois-bővítés, ugyanis ezzel az ekvivalens, hogy normális és szeparábilis:

1. szeparábilis, mivel K perfekt, így minden irreducibilis polinom szeparábilis.
2. normális, mivel $\overline{K}$ K -nak algebrai lezártja.

$\overline{K}|K$ Galois-csoportját $\text{Gal}(\overline{K}|K)$ fogja jelölni.

1.1 Affin varietások

Mivel a varietások algebrai struktúráját fogjuk vizsgálni, az algebrai zárttság miatt előnyösebb a varietások projektivizáltját tekinteni. A projektív varietásokhoz tartozó fogalmak azonban erősen az affin esetben bevezetettek alapszanak, így azokat kihagyni nem tudjuk. Az affin definíciók tehát csak a projektívek értelmezéséhez kellenek majd, a további fejezetekben végig projektív terekben dolgozunk.

1.1 Definíció. A K feletti n -**dimenziós affin tér** $\mathbb{A}^n(\overline{K}) = \{P = (x_1, \dots, x_n) : x_i \in \overline{K}\}$. Röviden csak $\mathbb{A}^n$ -nel fogjuk jelölni.

$\mathbb{A}^n$ **K -racionális** (röviden racionális) pontjai $\mathbb{A}(K) = \{P = (x_1, \dots, x_n) : x_i \in K\}$.

1.2 Definíció. Legyen $I \subseteq \overline{K}[X] = \overline{K}[X_1, \dots, X_n]$ -ben ideál. Ekkor ez meghatároz egy pontthalmazt $\mathbb{A}^n$ -ben: $V_I := \{P \in \mathbb{A}^n : f(P) = 0 \text{ minden } f \in I - \text{re}\}$. A V_I alakú részhalmazait $\mathbb{A}^n$ -nek **(affin) algebrai halmazoknak** nevezzük.

Ha V egy algebrai halmaz, akkor az általa meghatározott ideál $I(V) := \{f(X) \in \overline{K}[X] : f(P) = 0 \text{ minden } P \in V - \text{re}\}$.

1.3 Definíció. Azt mondjuk, hogy V **K felett definiált**, ha $I(V)$ generálható $K[X]$ -beli polinomokkal. Ezt $V|K$ -val jelöljük.

Ha V K felett definiált, akkor a K -racionális (vagy röviden csak racionális) pontjai $V(K) := V \cap \mathbb{A}^n(K)$.

1.4 Definíció. Az **(affin) varietás** olyan algebrai halmaz, melyre $I(V) \subseteq \overline{K}[X]$ prímeál (azaz ha $f, g \in \overline{K}[X]$ -re $fg \in I(V)$, akkor $f \in I(V)$ vagy $g \in I(V)$).

1.5 Definíció. Legyen $V|K$ egy varietás. ekkor $V|K$ **(affin) koordináta gyűrűje** $K[V] := K[X]/I(V|K)$.

$K[V]$ hányadosteste $K(V)$, amit V **függvénytestjének** nevezzük.

$\overline{K}[V], \overline{K}(V)$ hasonlóan definiálható, ha K -t $\overline{K}$ -ra cseréljük.

1.5.1 Megjegyzés. Ahhoz, hogy a hányadostestéről beszélhessünk, $K[V]$ -nek integritási tartománynak kell lennie. Mivel $K[X]$ kommutatív gyűrű, $K[V]$ is automatikusan az lesz. Csak a nullosztómentességet kell ellenőrizni, de az pedig következik abból, hogy $I(V|K)$ prímeál.

1.6 Definíció. Egy V **varietás dimenziója** $\dim(V) := \text{trdeg}(\overline{K}(V)|\overline{K})$.

1.7 Definíció. Legyen V egy varietás, $P \in V$, $\{f_1, \dots, f_k\} \subseteq \overline{K}[X]$ pedig $I(V)$ generátorhalmaza. Azt mondjuk, hogy V **sima** P -ben (P sima pontja V -nek), ha $F = (f_1, \dots, f_k) \in \overline{K}[X]^k$ Jacobi mátrixának $n - \dim(V)$ a rangja.

V sima, ha minden pontjában az.

1.8 Definíció. A V varietás **lokális gyűrűje** $P \in V$ -ben $\overline{K}[X]_P = \{F \in \overline{K}(V) : F = f/g \text{ valamely } f, g \in \overline{K}[X] - \text{re, ahol } g(P) \neq 0\}$.

Azt mondjuk, hogy $\overline{K}[X]_P$ elemei regulárisak P -ben.

1.9 Definíció. Legyen V egy affin varietás, $P \in V$. $M_P = \{f \in \overline{K}[V] : f(P) = 0\} \subseteq \overline{K}[V]$ ideál.

1.9.1 Megjegyzés. M_P maximális ideál, mivel $\varphi : \overline{K}[V]/M_P \rightarrow \overline{K}$, $\varphi(f) = f(P)$ izomorfizmus.

1.2 Projektív varietások

1.10 Definíció. $(x_0, \dots, x_n), (y_0, \dots, y_n) \in \mathbb{A}^{n+1}$, $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$, ha létezik $\lambda \in \overline{K} - \{0\}$, hogy $x_i = \lambda y_i$ minden i -re. Ez nyilván egy ekvivalencia reláció, $(x_0, \dots, x_n)$ ekvivalencia osztálya $[x_0, \dots, x_n]$.

A K feletti n -dimenziós **projektív tér** $\mathbb{P}^n(K) = \{P = [x_0, \dots, x_n] : x_i \in \overline{K}, \text{ létezik } j \text{ úgy, hogy } x_j \neq 0\}$. Röviden ezt is csak $\mathbb{P}^n$ -nel jelöljük.

$\mathbb{P}^n$ **racionális pontjai** $\mathbb{P}^n(K) = \{[x_0, \dots, x_n] \in \mathbb{P}^n : x_i \in K \text{ minden } i\text{-re}\}$.

1.11 Definíció. $f \in \overline{K}[X] = \overline{K}[X_0, \dots, X_n]$ egy n -fokú **homogén polinom**, ha minden $\lambda \in \overline{K}$ -ra $f(\lambda X_0, \dots, \lambda X_n) = \lambda^n f(X_0, \dots, X_n)$.

$I \subseteq \overline{K}[X]$ **homogén ideál**, ha homogén polinomok generálják.

1.11.1 Megjegyzés. A projektív térben homogén polinomokkal van értelme foglalkozni, ugyanis ezeknek értelmes gyökét keresni a $\sim$ ekvivalenciareláció szerint (egy osztálynak vagy minden eleme gyöke egy adott polinomnak vagy egyik sem).

1.11.2 Megjegyzés. Általában a $\mathbb{P}^n$ -beli varietásokat is $\overline{K}[X_0, \dots, X_{n-1}]$ -beli polinomokkal adjuk meg, a homogén polinomokban $X_n = 1$ -et állítva, és mindig észben tartjuk a varietás $[x_0, \dots, x_{n-1}, 0]$ alakú pontjait.

1.12 Definíció. A V_I , a **(projektív) algebrai halmaz**, az $I(V)$ a $V(K)$, a K feletti **definiáltság** és a **(projektív) varietás** ugyanúgy definiálható, mint affin esetben, azzal a különbséggel, hogy polinomok és ideálok helyett most mindig homogén polinomokat, illetve -ideálokat kell érteni.

1.1 Állítás. Ha V egy projektív varietás, és $\mathbb{A}^n \subseteq \mathbb{P}^n$, akkor $V \cap \mathbb{A}^n$ egy affin varietás.

Bizonyítás. Nem bizonyítjuk (ld. [3] Hartshorne: Algebraic Geometry, Ch. I., Coll. 2.3).

1.13 Definíció. Legyen $V|K$ egy projektív varietás és legyen $\mathbb{A}^n \subseteq \mathbb{P}^n$ olyan, hogy $V \cap \mathbb{A}^n \neq \emptyset$.

Ekkor V **dimenziója** ($\dim(V)$), **függvénytestjei** ($K(V), \overline{K}(V)$), **simasága egy $P \in V$ pontban**, **illetve simasága**, és **végül $\mathbf{M}_P$** , $K[X]_P$ $V \cap \mathbb{A}^n$ megfelelő attribútumával definiálható (ha V egy adott P pontjára vonatkozik a tulajdonság, akkor $P \in \mathbb{A}^n$ is felteendő).

1.13.1 Megjegyzés. $K(V) = \{f/g : \deg f = \deg g; f, g \text{ homogén, } g \notin I(V)\} / \sim$, ahol $f/g \sim f'/g'$ pontosan akkor, ha $fg' - f'g \in I(V)$. (Azért elég, azokat az f/g -ket nézni, amelyek esetén $\deg f = \deg g$, mivel $I(V)$ -beliek hozzáadásával ez elérhető.)

1.14 Definíció. $\text{Gal}(\overline{K}|K)$ hatását $\mathbb{P}^n$ -n úgy definiáljuk, hogy $\sigma \in \text{Gal}(\overline{K}|K)$ -ra $\sigma([x_0, \dots, x_n]) := [x_0^\sigma, \dots, x_n^\sigma]$.

1.14.1 Megjegyzés. $V(K) = \{P \in V : \sigma(P) = P \text{ minden } \sigma \in \text{Gal}(\overline{K}|K)\text{-re}\}$, hiszen nyilván ha $P \in V(K)$, $\sigma \in \text{Gal}(\overline{K}|K)$, akkor $\sigma(P) = P$, ha pedig $\sigma(P) = P$ minden σ -ra, akkor P minden koordinátája benne van $\text{Fix}(\text{Gal}(\overline{K}|K)) = K$ -ban ($\overline{K}|K$ Galois-bővítés), azaz $P \in V(K)$.

1.15 Definíció. **Görbének** fogjuk nevezni és C -vel fogjuk jelölni az 1 dimenziós projektív varietásokat.

1.15.1 Példa. Egy igen kézenfekvő görbe: a $\mathbb{P}^1 \subseteq \mathbb{P}^1$.

Ez tényleg görbe, hiszen

1. varietás, mivel az $I = 0$ -ra $\mathbb{P}^1 = V(I)$ és $I = 0$ prímeál, hiszen ez éppen $\overline{K}[X]$ nullosztómentességével ekvivalens.
2. görbe is, mivel $\mathbb{P}^1$ lokálisan $\mathbb{A}^1$.

A hányados testje pedig éppen a racionális függvények testje lesz: $K(\mathbb{P}^1) = \text{Quot}(K[X]/0) = K(X)$.

2 A rend

Ebben a fejezetben bevezetünk egy diszkrét értékelést a görbék lokális gyűrűin, ami a későbbiekben egy eléggé hasznos eszköze lesz az algebrai struktúra vizsgálatának.

2.1 Definíció. Legyen C egy görbe, $P \in C$ sima pont. Ekkor definiálhatunk egy $\text{ord}_P : \overline{K}[C]_P \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$, $\text{ord}_P(f) = \max\{d : f \in M_P^d\}$ függvényt.

Ezt $\overline{K}(C) \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$ -re kiterjeszthetjük $\text{ord}_P(f/g) := \text{ord}_P(f) - \text{ord}_P(g)$ -vel. $\text{ord}_P(f)$ f **rendje** P -ben. Azt mondjuk, hogy

- f -nek **gyöke** van P -ben, ha $\text{ord}_P(f) > 0$,

- f -nek **pólusa** van P -ben, ha $\text{ord}_P(f) < 0$, ilyenkor $f(P) := \infty$,
- f **reguláris** P -ben, ha $\text{ord}_P(f) \geq 0$.

2.1.1 Megjegyzés. Szemléletesen a rend f gyökeinek multiplicitását méri az adott pontokban.

2.1 Állítás. Tekintsünk egy $C = V(\langle f \rangle)$ ($f \in \overline{K}[x, y, z]$ homogén) $\mathbb{P}^2$ -beli görbét és egy $P \in C$ pontját. Innentől vehetjük P egy affin környezetét, amiről feltehetjük, hogy az $\{[x, y, 1] \in \mathbb{P}^2\} \cong \mathbb{A}^2$ affin altér és tekinthetjük C -t affin varietásnak, f -et $\overline{K}[x, y]$ -belinek. Így legyen $P = (x_0, y_0) \in C$. Ekkor $\dim_{\overline{K}} M_P/M_P^2 = 1$ pontosan akkor, ha C P -ben sima és ha $\overline{K}[C]_P$ diszkrét értékelés gyűrű (DVR), akkor C P -ben sima.

Bizonyítás. Hilbert nullhelytétele alapján így $\{f \in \overline{K}[C] : f(P) = 0\} = M_P = \langle x - x_0 + (f(x, y)), y - y_0 + (f(x, y)) \rangle$ alakú, azaz maximum két elem generálja.

$M_P/M_P^2 \cong \langle x - x_0, y - y_0 \rangle / \langle (x - x_0)^2, (x - x_0)(y - y_0), (y - y_0)^2, f(x, y) \rangle$, azaz ez egy maximum 2 dimenziós vektortér $\overline{K}$ felett ($\{x - x_0, y - y_0\}$ biztosan generálja, hiszen M_P -ben konstans tagok nincsenek) és pontosan akkor lesz 1-dimenziós, ha $f(x, y) \notin \langle x - x_0, y - y_0 \rangle^2 = \langle (x - x_0)^2, (x - x_0)(y - y_0), (y - y_0)^2 \rangle$.

f Taylor sora alapján $f(x, y) = \frac{\partial}{\partial x} f(x_0, y_0)(x - x_0) + \frac{\partial}{\partial y} f(x_0, y_0)(y - y_0) \pmod{\langle x - x_0, y - y_0 \rangle^2}$. Így $f(x, y) \notin \langle x - x_0, y - y_0 \rangle^2$ ekvivalens azzal, hogy C P -ben sima. Ezzel az állítás első részét beláttuk.

A második részéhez először megmutatjuk, hogy ha $J_P := M_P \overline{K}[C]_P$ (a maximális ideál a lokális gyűrűben), akkor $M_P/M_P^2 \cong J_P/J_P^2$:

$\overline{K}[C]/M_P^n \cong \overline{K}[C]_P/J_P^n$ tetszőleges $n = 1, 2, \dots$ -re, a $\varphi : \overline{K}[C]/M_P^n \rightarrow \overline{K}[C]_P/J_P^n$, $a + M_P^n \mapsto \frac{a}{1} + J_P^n$ izomorfizmus miatt.

1. φ jóldefiniált, hiszen ha $a + M_P^n = a' + M_P^n$, akkor $a - a' \in M_P^n = \{f \in \overline{K}[C] : f(P) = 0\}$, így $\frac{a-a'}{1} = \frac{a}{1} - \frac{a'}{1} \in M_P^n \overline{K}[C]_P = (M_P \overline{K}[C]_P)^n$, azaz $\frac{a}{1} + J_P^n = \frac{a'}{1} + J_P^n$.

2. Az, hogy φ gyűrűhomomorfizmus és injektív triviális.

3. Szürjektivitás: legyen $\frac{a}{s} + J_P^n \in \overline{K}[C]_P/J_P^n$, ahol $s \in \overline{K}[C] \setminus M_P$, azaz $s \in \overline{K}[C]/M_P$ invertálható. Ekkor $\overline{K}[C]/M_P^n$ -ben is az lesz:

Tudjuk, hogy $\overline{K}[C]/M_P$ egy test, így a 0-t kivéve minden eleme invertálható. Ha $s \in \overline{K}[C] \setminus M_P$, akkor tehát létezik $r \in \overline{K}[C]$, hogy $sr = 1 \pmod{M_P}$. Így $t := 1 - sr \in M_P$, $t^n \in M_P^n$. Másrészt $sr = 1 - t$, így $1 = 1 - t^n = (1 - t)(1 + t + \dots + t^{n-1}) = sr(1 + t + \dots + t^{n-1}) \pmod{M_P^n}$. Ezt hasonlóan $1 = rs$ -sel is megcsinálhatjuk. Tehát s -nek $\pmod{M_P^n}$ is van inverze. Ennek a -szorozásának φ szerinti képe pedig éppen $\frac{a}{s} + J_P^n$ lesz.

Tehát $\overline{K}[C]/M_P^2 \cong \overline{K}[C]_P/J_P^2$. Ezeknek a maximális ideáljai rendre M_P/M_P^2 és J_P/J_P^2 , amik így szintén izomorfak lesznek.

Egy lokális gyűrű ponotosan akkor DVR, ha főideálgyűrű és nem test. Ha C -nek P szinguláris pontja lenne, akkor $K[V]_P$ nem lehetne DVR, mert $J_P = M_P \overline{K}[C]_P$ nem lenne főideál (ha az lenne, J_P/J_P^2 is egy elemmel generálható lenne, pedig $\cong M_P/M_P^2$, ami 2-dimenziós P szingularitása miatt). $\square$

2.2 Definíció. Azt mondjuk, hogy $t_P \in \overline{K}(C)$ **prímelem** C -nek P -ben, ha $\text{ord}_P(t) = 1$.

2.2.1 Megjegyzés. Ha $P \in C$ sima, akkor létezik P -ben prímelem: ugyanis a 2.1 Állítás alapján ekkor $\dim_{\overline{K}} M_P/M_P^2 = 1$, azaz $M_P \setminus M_P^2$ nem lehet üres, definíció alapján pedig $M_P \setminus M_P^2$ éppen a P -beli prímelemeket tartalmazza.

2.2.2 Megjegyzés. Ez pontosan azt jelenti, hogy t generátora M_P -nek.

Ugyanis ha $g \in M_P$ generátor, akkor minden M_P -beli elem rendje $\text{ord}_P g (\geq 1$ mivel g M_P -beli) többszöröse, azonban tudjuk, hogy létezik P -beli prímelem, így szükségképpen $\text{ord}_P g = 1$, azaz g is prímelem.

Ha pedig $t_P \in M_P$ prímelem, akkor legyen g generátora M_P -nek ($K[C]_P$ DVR, és így főideálgyűrű), így $t_P = ug^k$ valamely $k \in \mathbb{Z}_{\geq 0}$ -re és u egységre ($\text{ord}_P u = 0$). Mivel t_P prímelem, így $k = 1$ -nek kell lennie. Tehát $g = u^{-1}t_P$, azaz t_P is generátor. $\square$

2.2 Állítás. Ha $P \in C$ egy sima pont, akkor $\overline{K}[C]_P$ DVR, a diszkrét értékelést a rend adja:

$$1, \text{ord}_P(fg) = \text{ord}_P f + \text{ord}_P g.$$

$$2, \text{ord}_P(f + g) \geq \min(\text{ord}_P f, \text{ord}_P g).$$

$$3, \text{ord}_P(f) = 0, \text{ ha } f \in \overline{K} - \{0\}, \text{ és } \text{ord}_P 0 = \infty. \text{ Sőt, ezek a tulajdonságok } \overline{K}(C)\text{-n is igazak.}$$

Bizonyítás. 1, Ha $f, g \in \overline{K}[C]_P$, akkor $\text{ord}_P(fg) = \max(d : fg \in M_P^d) \leq \max(d : f \in M_P^d) + \max(d : g \in M_P^d) = \text{ord}_P f + \text{ord}_P g$, másrészt ha $f = m_1 \in M_P^{\text{ord}_P f}$, $g = m_2 \in M_P^{\text{ord}_P g}$, akkor $fg = m_1 m_2 \in M_P^{\text{ord}_P f + \text{ord}_P g}$, azaz $\text{ord}_P(fg) \geq \text{ord}_P f + \text{ord}_P g$.

$f, g \in \overline{K}(C)$ esetén legyen $f = f_1/f_2, g = g_1/g_2$, ahol $f_1, g_1, f_2, g_2 \in \overline{K}[C]_P$. Ekkor $\text{ord}_P(fg) = \text{ord}_P(\frac{f_1 g_1}{f_2 g_2}) = \text{ord}_P(f_1 g_1) - \text{ord}_P(f_2 g_2) = \text{ord}_P(f_1) + \text{ord}_P(g_1) - \text{ord}_P(f_2) - \text{ord}_P(g_2) = \text{ord}_P(f_1/f_2) + \text{ord}_P(g_1/g_2) = \text{ord}_P(f) + \text{ord}_P(g)$.

2, $f, g \in \overline{K}[C]_P$. Ha $f \in M_P^{\text{ord}_P f}$, akkor $f = \sum a_{i,1} a_{i,2} \dots a_{i,\text{ord}_P f}$, ahol $a_{i,j} \in M_P$,

és hasonlóan $g = \sum b_{j,1} b_{j,2} \dots b_{j,\text{ord}_P g}$.

Így ha az általánosság megsértése nélkül feltesszük, hogy $\text{ord}_P f \geq \text{ord}_P g$, akkor

$f + g = \sum a_{i,1} \dots a_{i,\text{ord}_P g - 1} \cdot (a_{i,\text{ord}_P} \dots a_{i,\text{ord}_P f}) + \sum b_{j,1} b_{j,2} \dots b_{j,\text{ord}_P g} \in M_P^{\text{ord}_P g}$, tehát $\text{ord}_P(f + g) \geq \min(\text{ord}_P f, \text{ord}_P g)$.

$f, g \in \overline{K}(C)$ esetén legyen $f = f_1/f_2, g = g_1/g_2$, ahol $f_1, g_1, f_2, g_2 \in \overline{K}[C]_P$. Ekkor $\text{ord}_P(f + g) = \text{ord}_P(f_1/f_2 + g_1/g_2) = \text{ord}_P(\frac{f_1 g_2 + g_1 f_2}{f_2 g_2}) = \text{ord}_P(f_1 g_2 + g_1 f_2) - \text{ord}_P(f_2 g_2) = \text{ord}_P(f_1 g_2 + g_1 f_2) - \text{ord}_P(f_2) - \text{ord}_P(g_2) \geq \min(\text{ord}_P(f_1 g_2) - \text{ord}_P(f_2) - \text{ord}_P(g_2), \text{ord}_P(g_1 f_2) - \text{ord}_P(f_2) - \text{ord}_P(g_2)) = \min(\text{ord}_P(f_1/f_2), \text{ord}_P(g_1/g_2)) = \min(\text{ord}_P(f), \text{ord}_P(g))$.

3, Triviális.

A 2.1 Állítás alapján P simasága szükséges feltétele annak, hogy $\overline{K}[C]_P$ DVR legyen. $\square$

2.2.1 Példa. Tekintsük az $E : Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$ egyenlettel megadott $\mathbb{P}^2$ -beli görbét és az $O = [0 : 1 : 0] \in E$ pontot.

Ekkor $\text{ord}_O(Z) = 3$:

Mivel $Z = \frac{X^3}{Y^2 + a_1XY + a_3YZ - a_2X^2 - a_4XZ - a_6Z^2}$ ($Y^2 + a_1XY + a_3YZ - a_2X^2 - a_4XZ - a_6Z^2 \in K[E]_O$, hiszen $Y^2 + a_1XY + a_3YZ - a_2X^2 - a_4XZ - a_6Z^2|_O = 1$), amiben O háromszor tűnik el, azaz $\text{ord}_O(Z) \geq 3$.

Az, hogy a rend 3-nál több nem lehet, onnan látszik, hogy X/Y prímelem O -ban, ugyanis generálja M_O -t:

O -ban E egyenlete $x := X/Y, z := Z/Y$ bevezetésével $z + a_1xz + a_3z^2 = x^3 + a_2x^2y + a_4xz^2 + a_6z^3$ alakba írható. Ekkor $M_O = \langle x, z \rangle$, z viszont x -szel kifejezhető, ugyanis E egyenlete z -re 3.fokú polinom x paraméterrel. Tehát $M_O = \langle x \rangle$, ami pedig ekvivalens azzal, hogy $x = X/Y$ prímelem. Tudjuk azt is, hogy $K[E]_O$ DVR, amiből következik, hogy UFD és van egy egyértelmű irreducibilis elem egységgel való szorzás erejéig. Ezek alapján a

$Z = \frac{X^3}{Y^2 + a_1XY + a_3YZ - a_2X^2 - a_4XZ - a_6Z^2} = (X/Y)^3 \frac{Y^3}{Y^2 + a_1XY + a_3YZ - a_2X^2 - a_4XZ - a_6Z^2}$ felírásból látható, hogy Z -nek pontosan 3 lesz a rendje.

2.2.2 Példa. A jelölések ugyanazok, mint az előző példában. Most számoljuk ki $\text{ord}_O(X/Z)$ -t:

Definíció alapján $\text{ord}_O(X/Z) = \text{ord}_O(X) - \text{ord}_O(Z) = \text{ord}_O(X) - 3$.

Az előző alapján $1 = \text{ord}_O(X/Y) = \text{ord}_O(X)$, hiszen $Y|_O = 1$

Így $\text{ord}_O(X/Z) = 1 - 3 = -2$.

2.2.3 Példa. Szintén az előző jelölésekkel végül $\text{ord}_O(Y/Z) = \text{ord}_O(Y) - \text{ord}_O(Z) = 0 - 3 = -3$, mivel $\text{ord}_O(Y) = 0$, hiszen $Y|_O = 1$.

2.3 Állítás. Legyen C egy sima görbe, $f \in \overline{K}(C)$. Ekkor C -nek csak véges sok pontjában van f -nek gyöke vagy pólusa (azaz véges sok kivételtől eltekítve $\text{ord}_P(f) = 0$). Ha f -nek nincsen se gyöke, se pólusa, akkor $f \in \overline{K}$.

Bizonyítás. $f \in \overline{K}(C)$ f_1/f_2 alakú, ahol $f_1, f_2 \in \overline{K}[C] \pmod{I(C)}$. $f = f_1/f_2$ -nek gyöke pontosan ott van, ahol f_1 -nek, ami egy polinom, így véges sok gyöke van. Hasonlóan $f = f_1/f_2$ -nek pólusa pontosan ott van, ahol f_2 -nek gyöke, amiből véges sok van.

Mivel $\overline{K}$ felett tekintjük a polinomokat, így ha 0-nál nagyobb a fokuk, akkor biztosan lesz gyökük. Így az, hogy f -nek se gyöke, se pólusa nincsen, azt jelenti, hogy $f = f_1/f_2$ felírásban f_1 -nek és f_2 -nek sincsen gyöke, azaz 0-fokúak $\pmod{I(C)}$, azaz $\overline{K}$ -beliek. $\square$

2.4 Állítás. Legyen $C|K$ görbe, $t \in K(C)$ prímelem egy sima $P \in C$ pontban. Ekkor $K(C)|K(t)$ egy véges, szeparábilis bővítés.

Bizonyítás. Végesség: A $K(C)|K$ bővítés végesen generált, hiszen ha $C \subseteq \mathbb{P}^n$, akkor $X_0, \dots, X_n$ (a koordináta függvények) biztosan generálják. Másrészt definíció alapján, mivel C egy görbe, $\text{trdeg}(K(C)|K) =$

1. Ezek alapján étezik egy $\alpha \in K(C)$ transzcendens elem, melyre $K(C) = K(\alpha)$. Mivel $t \notin K$, így $t = p(\alpha)$ valamely $p \in K[x] - \{0\}$ polinomra. Így $K(C)|K(t)$ véges bővítés, hiszen $K(t)$ felett (α algebrai és) $\deg \alpha = \deg p$.

Szeparabilitás: Mivel $[K(C) : K] < \infty$, így $K(C)|K(t)$ algebrai bővítés. x algebrai $K(t)$ felett így $\exists a_{i,j} \in K : \sum_{i,j} a_{i,j} t^i x^j = 0$ (beszorozva az esetleges nevezőkkel). Legyen $\Phi(X, T) = \sum_{i,j} X^i T^j \in K[X, T]$, és tegyük fel, hogy Φ -t X -ben minimális fokszámúnál választottuk, azaz $\Phi(X, t)$ x minimálpolinomha $K(t)$ felett.

Legyen $p = \text{char}(K)$ (p prím). Ha $\Phi(X, T)$ -nek van olyan $a_{i,j} T^i X^j$ tagja, amire $j \not\equiv 0 \pmod p$, akkor $d\Phi/dX \not\equiv 0 \pmod p$ ($X^j \equiv X^{j \bmod p+1} \pmod p$), azaz $\Phi(X, t)$ és így x $K(t)$ felett szeparábilis.

Így mostantól tegyük fel, hogy $\Phi(X, T) = \Psi(X^p, T)$. Ha $F(X, T) \in K[T, X]$ tetszőleges polinom, akkor $F(X^p, T^p)$ egy p -hatvány, mivel K tökéletes, így minden eleme egy p -hatvány, azaz $F(X^p, T^p) = \sum (b_{i,j} X^i T^j)^p$ alakú, ami p karakterisztikában $(\sum c_{i,j} X^i T^j)^p$ -vel egyenlő.

Így T kitevőjének $\bmod p$ maradéka szerint összegezve $\Phi(X, T) = \Psi(X^p, T) = \sum_{k=0}^{p-1} \sum c_{i,j,k} T^{ip} X^{jp} T^k = \sum_{k=0}^{p-1} \Phi_k(X, T)^p T^k$.

$\Phi(x, t) \equiv 0$, mivel így vettük fel Φ -t, így $\text{ord}_P(\Phi(x, t)) = \infty$.

Másrészt mivel t prímelem P -ben, $\text{ord}_P(\Phi_k(x, t)^p t^k) = p \cdot \text{ord}_P(\Phi_k(x, t)) + k \cdot \text{ord}_P(t) = p \cdot \text{ord}_P(\Phi_k(x, t)) + k \equiv k \pmod p$, azaz $\sum_{k=0}^{p-1} \Phi_k(x, t)^p t^k$ -ban a tagok rendjei páronként különbözőek. Így szükségképpen $\Phi_k(x, t) \equiv 0$ minden $k = 0, 1, \dots, p-1$ -re, hiszen különben ha j a legkisebb index, amire $\Phi_j(x, t) \not\equiv 0$, akkor $\text{ord}_P(\Phi(x, t)) = j$ lenne, ami ellentmondás.

Valamely k -ra $\Phi_k(X, T)$ -ben szerepel X nem nulla kitevővel, így ekkor $\deg_X \Phi_k \leq \deg_X \Phi < \deg_X \Phi$, ami ellentmond Φ választásának. $\square$

3 Leképezések görbék között

3.1 Szeparábilis és tisztán inszeparábilis testbővítések

A görbék közötti leképezések vizsgálata előtt néhány technikai állítást be kell látnunk a szeparabilitásról, ugyanis ezek elég gyakran elő fognak fordulni a leképezések jellemzésekor.

3.1 Definíció. Legyen $E|F$ egy algebrai testbővítés.

$\alpha \in E$ **szeparábilis**, ha a minimálpolinomja szeparábilis, azaz nincs többszörös gyöke (ekvivalensen,

a deriváltja nem azonosan 0). $E|F$ szeparábilis, ha E minden eleme az.

$\alpha \in E$ **tisztán inszeparábilis**, ha minimálpolinomja $(x - \alpha)^m$ valamely $m \in \mathbb{Z}_+$ -ra. $E|F$ tisztán inszeparábilis, ha E minden eleme az.

3.2 Definíció. Legyen $F|E$ algebrai bővítés. E **szeparábilis lezártja** F -ben $S = \{\alpha \in F : \alpha \text{ szeparábilis } E \text{ felett}\}$. Ekkor $[S : E]$ az $F|E$ bővítés **szeparábilis foka**, amit $\deg_s(F|E) = [F : E]_s$ -sel jelölünk, $[F : S]$ pedig $F|E$ **inszeparábilis foka**, amit $\deg_i(F|E) = [F : E]_i$ -vel jelölünk. Persze $\deg_s \deg_i = \deg$.

3.2.1 Megjegyzés. Az $F|K$ bővítésben $\alpha \in F$ tisztán inszeparábilis pontosan akkor, ha α minimálpolinomja $x^{p^r} - a \in K[x]$ valamely $r \in \mathbb{N}$ -re.

Bizonyítás. Ha α tisztán inszeparábilis, akkor minimálpolinomja $(x - \alpha)^m$ alakú, ahol $m \in \mathbb{Z}_+$. Legyen $m = np^r$, ahol $(n, p) = 1$. Ekkor $((x - \alpha)^m)^{p^r} = ((x - \alpha)^{p^r})^n =$. Kibontva $x^{p^r(n-1)}$ együtthatója $\pm n\alpha^{p^r} \in K$, így mivel $(n, p) = 1$, $n \neq 0$, $1/n(n\alpha^{p^r}) = \alpha^{p^r} \in K$. Így $((x - \alpha)^{p^r})^n = (x^{p^r} - \alpha^{p^r})^n$ α minimálpolinomja, azaz $n = 1$ -nek kell lennie.

A vissza irány K tökéletessége miatt triviális. □

3.2.2 Megjegyzés. Ha $F|K$ véges, tisztán inszeparábilis bővítés, akkor $[F : K] = p^n$ valamely $n \in \mathbb{N}$ -re.

Bizonyítás. $F = K(\alpha_1, \dots, \alpha_m)$ úgy, hogy minden i -re α_i tisztán inszeparábilis K felett, így $K(\alpha_1, \dots, \alpha_{i-1})$ felett is. Így az előző megjegyzés miatt $K(\alpha_1, \dots, \alpha_m)|K(\alpha_1, \dots, \alpha_{m-1})| \dots |K(\alpha_1)|K$ -ben minden bővítés foka p^r ($r \in \mathbb{N}$), így $[F : K]$ is p -hatvány. □

3.2.3 Megjegyzés. Legyen S K szeparábilis lezártja F -ben. Ekkor

1, $S|K$ szeparábilis bővítés

2, $F|S$ tisztán inszeparábilis bővítés

Bizonyítás. 1, Ha $\alpha, \beta \in S$, akkor $K(\alpha, \beta)|K$ is szeparábilis, így $K(\alpha, \beta) \subseteq S$, $\alpha \pm \beta, \alpha\beta^{-1} \in S$, így S test és nyilván szeparábilis K felett. 2, Ha $\alpha \in F$ algebrai K felett, akkor α^{p^r} szeparábilis K felett valamely $r \in \mathbb{Z}_+$ -ra, ugyanis $\deg_K \alpha = 1$ -re triviálisan teéjesül, $\deg_K \alpha > 1$ -re pedig indukcióval visszavezethető kisebb esetre: ha α nem szeparábilis, akkor az m_α minimálpolinomjára $m'_\alpha \equiv 0$, így $m_\alpha = f(x^p)$ alakú, vagyis α^p algebrai, $\deg_K \alpha^p < \deg_K \alpha$.

Így, ha $\alpha \in F$, akkor létezik r , hogy $\alpha^{p^r} \in S$, így α gyöke $(x - \alpha)^{p^r} = x^{p^r} - \alpha^{p^r} \in S[x]$ -nek, vagy $F|S$ bővítésben α minimálpolinomja $(x - \alpha)^{p^r}$ divizorja, azaz maga is $(x - \alpha)^m$ alakú. Tehát α tisztán inszeparábilis S felett. □

3.1 Lemma. Legyenek $F|E|K$, $N|K$ testbővítések. Ekkor $\#\{F \rightarrow N \text{ } E\text{-monomorfizmusok}\} \cdot \#\{E \rightarrow N \text{ } K\text{-monomorfizmusok}\} = \#\{F \rightarrow N \text{ } K\text{-monomorfizmusok}\}$

Bizonyítás. Legyen $\{F \rightarrow N \text{ } E\text{-monomorfizmusok}\} = \{\sigma_1, \dots, \sigma_n\}$ és $\{E \rightarrow N \text{ } K\text{-monomorfizmusok}\} = \{\tau_1, \dots, \tau_m\}$.

Mindegyik τ_i kiterjed egy $\tilde{\tau}_i : N \rightarrow N$ K -automorfizmussá. $\tilde{\tau}_i \circ \sigma_j$ egy $F \rightarrow N$ K -automorfizmus. Ezek páronként különbözőek lesznek:

Ha $\tilde{\tau}_i \sigma_j = \tilde{\tau}_k \sigma_l$, akkor $\tilde{\tau}_k^{-1} \tilde{\tau}_i \sigma_j = \sigma_l$. Mivel $\sigma_j|_E = \sigma_l|_E = \text{id}_E$, így $\tilde{\tau}_k^{-1} \tilde{\tau}_i|_E = \text{id}_E$, azaz $\tilde{\tau}_k = \tilde{\tau}_i$, vagyis $i = k$.

Mivel $\tilde{\tau}_i$ injektív, így $\tilde{\tau}_i \sigma_j = \tilde{\tau}_i \sigma_l$ -ből $\sigma_j = \sigma_l$, azaz $j = l$ következik.

Másrészt ha $\tau : F \rightarrow N$ egy K -monomorfizmus, akkor $\tau|_E$ egy $E \rightarrow N$ K -monomorfizmus, vagyis $\tau|_E = \tau_i$ valamely $i \in \{1, \dots, n\}$ -re. $\tilde{\tau}_i^{-1} \tau|_E$ egy $E \rightarrow N$ K -monomorfizmus, azaz $\tilde{\tau}_i^{-1} \tau|_E = \sigma_j$ valamely $\sigma \in \{1, \dots, m\}$ -re. Azaz $\tau = \tilde{\tau}_i \sigma_j$, minden $F \rightarrow N$ K -monomorfizmus előáll ilyen alakban.

Tehát $\#\{F \rightarrow N \text{ } K\text{-monomorfizmusok}\} = \#\{\tilde{\tau} \sigma : \tau \in \{E \rightarrow N \text{ } K\text{-monomorfizmusok}\}, \sigma \in \{F \rightarrow N \text{ } E\text{-monomorfizmusok}\}\} = \#\{F \rightarrow N \text{ } E\text{-monomorfizmusok}\} \cdot \#\{E \rightarrow N \text{ } K\text{-monomorfizmusok}\}$.

□

3.2.4 Megjegyzés. Legyen $N|F|K$ olyan, hogy $N|K$ normális, $F|K$ véges. Ekkor $\#\{F \rightarrow N \text{ } K\text{-monomorfizmusok}\} = \deg_s(F|K)$.

Bizonyítás. Legyen S K szeparábilis lezártja F -ben.

Először megmutatjuk, hogy $\#\{F \rightarrow N \text{ } K\text{-monomorfizmusok}\} = \#\{S \rightarrow N \text{ } K\text{-monomorfizmusok}\}$:

Tegyük fel, hogy $\sigma, \tau \in \{F \rightarrow N \text{ } K\text{-monomorfizmusok}\}$ olyanok, hogy $\sigma|_S = \tau|_S$. Tetszőleges $a \in F$ esetén valamely n -re $a^{p^n} \in S$ (hiszen $F|S$ tisztán inszeparábilis). Így $\sigma(a)^{p^n} = \sigma(a^{p^n}) = \tau(a^{p^n}) = \tau(a)^{p^n}$, ahonnan $\sigma(a) = \tau(a)$ (mivel $F|S$ bővítésben $\sigma(a)$ minimálpolinomja $x^{p^n} - \tau(a)^{p^n} = (x - \tau(a))^{p^n}$). Tehát $\sigma|_S = \tau|_S$ -ből $\sigma = \tau$ következik, azaz az S -re való megszorítás egy injekció $\{F \rightarrow N \text{ } K\text{-monomorfizmusok}\}$ -ből $\{S \rightarrow N \text{ } K\text{-monomorfizmusok}\}$ -be. A másik irányba injekció: egy $S \rightarrow N$ K -monomorfizmus kiterjeszthető egy $N \rightarrow N$ K -automorfizmussá, ami pedig egy $F \rightarrow N$ K -monomorfizmussá.

Így feltehető, hogy $F|K$ szeparábilis, azaz $S = F$. Ekkor $[F : K] = [F : K]_s$ és minden $F|E|K$ közbülső testre $F|E$, $E|K$ is szeparábilisak, azaz $[F : E] = [F : E]_s$, $[E : K] = [E : K]_s$.

Ezt felhasználva $[F : K]$ szerinti indukcióval bizonyítjuk az állítást:

1, Ha $[F : K] = 1$, akkor $F = K$ és $[F : K]_s = [F : K] = 1 = \#\{K \rightarrow K \text{ } K\text{-monomorfizmusok}\} = \#\{F \rightarrow N \text{ } K\text{-monomorfizmusok}\}$.

2, $[F : K] > 1$ esetén legyen $a \in F \setminus K$, ekkor $[K(a) : K] > 1$.

Ha $[K(a) : K] < [F : K]$, akkor az indukciós feltevés alapján $[K(a) : K]_s = \#\{K(a) \rightarrow N \text{ } K\text{-monomorfizmusok}\}$.

A 3.1 Lemma alapján pedig $\#\{F \rightarrow N \text{ } K\text{-monomorfizmusok}\} = \#\{F \rightarrow N \text{ } K(a)\text{-monomorfizmusok}\} \cdot \#\{K(a) \rightarrow N \text{ } K\text{-monomorfizmusok}\} = [F : K(a)]_s \cdot [K(a) : K]_s = [F : K(a)] \cdot [K(a) : K] = [F : K] = [F : K]_s$.

Ha pedig $[K(a) : K] = [F : K]$, akkor $F = K(a)$ és $[F : K(a)] = \deg m_{K,a}$. Ha σ egy $F \rightarrow N$ K -monomorfizmus, akkor azt $\sigma(a)$ egyértelműen meghatározza. $\sigma(a)$ gyöke $m_{K,a}$ -nak, így maximum $\deg m_{K,a} = [F : K(a)]$ ilyen monomorfizmus van. Másrészt mivel $m_{K,u}$ felbomlik N -ben és szeparábilis is, így pontosan ennyi $F \rightarrow N$ K -monomorfizmus lesz. $\square$

3.2.5 Megjegyzés. Tekintsük a következő bővítést: $M|L|K$. Ekkor $[M : L]_s[L : K]_s = [M : K]_s$ és $[M : L]_i[L : K]_i = [M : K]_i$.

Bizonyítás. Az előző megjegyzés alapján az $\overline{K}|M|L$ bővítést tekintve $[M : L]_s = \#\{M \rightarrow \overline{K} \text{ } L\text{-monomorfizmusok}\}$, az $\overline{K}|L|K$ bővítést tekintve $[L : K]_s = \#\{L \rightarrow \overline{K} \text{ } K\text{-monomorfizmusok}\}$, és végül az $\overline{K}|M|K$ bővítést tekintve $[M : K]_s = \#\{M \rightarrow \overline{K} \text{ } K\text{-monomorfizmusok}\}$.

A 3.1 Lemma alapján pedig $\#\{M \rightarrow \overline{K} \text{ } L\text{-monomorfizmusok}\} \cdot \#\{L \rightarrow \overline{K} \text{ } K\text{-monomorfizmusok}\} = \#\{M \rightarrow \overline{K} \text{ } K\text{-automorfizmus}\}$, azaz $[M : L]_s[L : K]_s = [M : K]_s$. Ebből és a triviális $[F : E]_s[F : E]_i = [F : E]$ -ből bármilyen $F|E$ bővítésre, adódik $[M : L]_i[L : K]_i = [M : K]_i$. $\square$

3.2.6 Megjegyzés. $\deg_s = \deg$ és $\deg_i = 1$ pontosan akkor, ha $E|F$ szeparábilis:

Ha $E|F$ szeparábilis bővítés, akkor nyilván $S = E$ és $\deg = \deg_s$, és így $\deg_i = 1$. Ha pedig $[E : F] = \deg = \deg_s = [E : F]_s = [S : F]$, akkor szükségképpen $E = S$, vagyis $E|F$ szeparábilis.

Hasonlóan $E|F$ tisztán inszeparábilis pontosan akkor, ha $\deg_i = \deg$ és $\deg_s = 1$:

Ha $E|F$ inszeparábilis, akkor $P = E$, azaz $\deg_i = \deg$, visszafelé pedig ha $[E : F] = \deg = \deg_i = [E : F]_i = [P : F]$, akkor $E = P$, vagyis $E|F$ tisztán inszeparábilis. $\square$

3.2.7 Megjegyzés. Ha $L|K$ és $M|L$ is szeparábilis, akkor $M|K$ is az.

Bizonyítás. Az előző megjegyzést álitása alapján:

Mivel $L|K$ szeparábilis, így $[L : K] = [L : K]_s$ és $[L : K]_i = 1$.

Mivel $M|L$ szeparábilis, így $[M : L] = [M : L]_s$ és $[M : L]_i = 1$.

Így $[M : K] = [M : L][L : K] = [M : L]_s[L : K]_s = [M : K]_s$ és $[M : K]_i = [M : L]_i[L : K]_i = 1 \cdot 1 = 1$, azaz $M|K$ szeparábilis. $\square$

3.2 Morfizmusok

A morfizmusok lesznek most nekünk a "szép" leképezések, amiket algebrailag vizsgálni tudunk.

3.3 Definíció. Legyen $C_1, C_2 \subseteq \mathbb{P}^n$ két görbe. $\phi : C_1 \rightarrow C_2$ egy **(racionális) leképezés**, ha $\phi = [f_0, \dots, f_n]$ alakú, ahol $i = 0, \dots, n$ -re $f_i \in \overline{K}(C_1)$ és $\phi(P) = [f_0(P), \dots, f_n(P)]$ azon $P \in V_1$ -ekre, melyekre $f_0, \dots, f_n$ mindegyike reguláris.

3.4 Definíció. Egy $\phi = [f_0, \dots, f_n] : C_1 \rightarrow C_2$ **racionális leképezés reguláris** $P \in C_1$ -ben, ha létezik $g \in \overline{K}(C_1)$, amire

1. gf_i reguláris P -ben minden i -re

2. van olyan i , amire $gf_i(P) \neq 0$.

Ekkor $\phi(P)$ -re $[gf_0(P), \dots, gf_n(P)]$ -ként tekintünk. Ha létezik $\lambda \in \overline{K} - \{0\}$ úgy, hogy $\lambda f_0, \dots, \lambda f_n \in K(V_1)$, akkor ϕ K felett definiált.

3.5 Definíció. Azt a racionális leképezést, mely C_1 minden pontjában reguláris, **morfizmusnak** nevezzük.

3.1 Állítás. Legyen C egy görbe, $V \subseteq \mathbb{P}^N$ egy varietás, P egy sima pont C -n és $\phi : C \rightarrow V$ egy racionális leképezés. Ekkor ϕ reguláris P -ben.

Speciálisan, ha C sima, akkor ϕ morfizmus.

Bizonyítás. Legyen $\phi = [f_0, \dots, f_N]$, $f_i \in \overline{K}(C)$ és legyen $t \in \overline{K}(C)$ egy prímelem P -ben. Legyen $n = \min_{0 \leq i \leq N} \text{ord}_P(f_i)$.

Ekkor $\text{ord}_P(t^{-n}f_i) \geq 0 \ \forall i = 0, \dots, N$ -re és, ha j -n vétetik fel a minimum, akkor $\text{ord}_P(t^{-n}f_j) = 0$.

Tehát $\forall i$ -re $t^{-n}f_i$ reguláris P -ben és $(t^{-n}f_j)(P) \neq 0$, így ϕ reguláris P -ben. $\square$

3.1.1 Következmény. Egy morfizmus, amit gyakran fogunk használni:

Legyen $C|K$ egy sima görbe, $f \in K(C)$.

Ekkor f indukál egy $\hat{f} : C \rightarrow \mathbb{P}^1$, $\hat{f}(P) := \begin{cases} [f(P), 1] & \text{ha } f \text{ } P\text{-ben reguláris} \\ [1, 0] = \infty & \text{ha } f\text{-nek } P\text{-ben pólusa van} \end{cases}$ leképezést, ami az állítás miatt morfizmus.

Másrészt ha $\phi : C \rightarrow \mathbb{P}^1$, $\phi = [f, g]$ egy K felett definiált racionális leképezés, akkor $g = 0$ esetén $\phi \equiv \infty$ konstans leképezés, különben ϕ az $f/g \in K(C)$ -hez tartozó leképezés.

Ezek alapján kaptunk egy $1 : 1$ megfeleltetést $K(C) \cup \infty$ és $\{\phi : \phi : C \rightarrow \mathbb{P}^1 \text{ } K \text{ felett definiált}\}$ között.

3.2 Állítás. Legyen C_1, C_2 két görbe, $\phi : C_1 \rightarrow C_2$ morfizmus közöttük. Ekkor ϕ konstans vagy szürjektív.

Bizonyítás. Nem bizonyítjuk (ld. [3] Hartshorne: Algebraic Geometry, Ch. II., Prop. 6.8).

3.6 Definíció. Legyen $C_1|K, C_2|K$ két görbe, $\phi : C_1 \rightarrow C_2$ K felett definiált nem konstans racionális leképezés. Ekkor ϕ egy K -t fixáló ϕ^* injekciót indukál $K(C_2)$ és $K(C_1)$ között: $\phi^* : K(C_2) \rightarrow K(C_1)$, $\phi^*f = f \circ \phi$. Ezt a leképezést ϕ **duálisának** nevezzük.

3.6.1 Megjegyzés. Ez tényleg injekció, ugyanis a 3.2 Állítás alapján ϕ szürjektív, így ha $\phi^*f = \phi^*g$, akkor $f = g$ C_2 minden pontjában.

3.3 Állítás. Legyen $C_1|K, C_2|K$ két görbe.

1, Ha $\phi : C_1 \rightarrow C_2$ egy K felett definiált, nemkonstans leképezés, akkor $K(C_1)$ véges bővítése $\phi^*K(C_2)$ -nek.

2, Legyen $\iota : K(C_2) \rightarrow K(C_1)$ K -t fixáló injekció. Ekkor egyértelműen létezik egy $\phi : C_1 \rightarrow C_2$ K felett definiált, nem konstans leképezés, amire $\phi^* = \iota$.

Bizonyítás. 1, Mivel ϕ^* injekció, és $K(C_1), K(C_2)$ véges bővítései K -nak, így $C(K_1)|\phi^*K(C_2)|K$, és szükségképpen $K(C_1)$ véges bővítése $\phi^*K(C_2)$ -nek.

2, Tekintsük C_2 $\mathbb{P}^N$ -beliként, és tegyük fel (esetleg koordinátacserével), hogy $C_2 \cap \{X_0 = 0\} = \emptyset$.

Legyen $g_i \in K(C_2), g_i : [X_0, \dots, X_N] \mapsto X_i/X_0$.

Ekkor $\phi := [1, \iota g_1, \dots, \iota g_N] : C_1 \rightarrow C_2$ és $\phi^* = \iota$, mivel $\phi^*f([x_0, \dots, x_n]) = f \circ \phi([x_0, \dots, x_n]) = f([1, \iota g_1, \dots, \iota g_N]([x_0, \dots, x_n])) = f([1, \iota g_1, \dots, \iota g_N]([1, x_1/x_0, \dots, x_n/x_0])) = \iota f$, hiszen ι polinomiálisan terjed ki $K(C_2)$ egy K feletti bázisáról, azaz például $\{X_1/X_0, \dots, X_n/X_0\}$ -ről.

Ha $\psi = [f_0, \dots, f_N]$ is olyan, hogy $\psi^* = \iota$, akkor minden i -re $f_i/f_0 = \psi^*g_i = \phi^*g_i = \iota g_i$, ahonnan $\psi = \phi$. $\square$

3.7 Definíció. Legyen C_1, C_2 két görbe, $\phi : C_1 \rightarrow C_2$ K felett definiált leképezés közöttük. Ha ϕ konstans, akkor $\deg \phi = 0$, különben $\deg \phi = [K(C_1) : \phi^*K(C_2)]$ a ϕ **leképezés foka**. Az utóbbi esetben azt mondjuk, hogy ϕ **véges**.

ϕ szeparabilitása, inszeparabilitása, tisztán szeparabilitása, valamint szeparabilis-, inszeparabilis foka $K(C_1)|\phi^*K(C_2)$ megfelelő jellemzőjének felel meg.

3.3.1 Következmény. Legyen C_1, C_2 két sima görbe, $\phi : C_1 \rightarrow C_2$ morfizmus közöttük és $\deg \phi = 1$. Ekkor ϕ izomorfizmus.

Bizonyítás. $1 = \deg \phi = [\overline{K}(C_1) : \phi^*\overline{K}(C_2)]$, így $\overline{K}(C_1) = \phi^*\overline{K}(C_2)$. Tehát ϕ^* izomorfizmus $\overline{K}(C_1)$ és $\overline{K}(C_2)$ között (tudjuk, hogy ϕ^* injektív, és az előzőek alapján szürjektív is). Tehát létezik $(\phi^*)^{-1} : \overline{K}(C_1) \rightarrow \overline{K}(C_2)$ injekció (valójában izomorfizmus).

Így a 3.3 Állítás 2, része miatt létezik egy $\psi : C_2 \rightarrow C_1$ leképezés, melyre $\psi^* = (\phi^*)^{-1}$. Mivel C_2 sima, így a 3.1 Állítás miatt ψ morfizmus.

$(\phi \circ \psi)^* = \psi^* \circ \phi^* = (\phi^*)^{-1} \circ \phi^* = \text{id}_{\overline{K}(C_2)}$ és hasonlóan $(\psi \circ \phi)^* = \phi^* \circ \psi^* = \text{id}_{\overline{K}(C_1)}$. Így a 3.3 Állítás 2, részének egyértelműsége vonatkozó része miatt ez azt jelenti, hogy $\psi \circ \phi = \text{id}_{C_1}$ és $\phi \circ \psi = \text{id}_{C_2}$. Így ϕ és ψ is izomorfizmus, mert egymás inverzei (azaz injektívek és a 3.2 Állítás alapján szürjektívek). $\square$

3.3 Az elágazási index

Az elágazási index alapvetően geometriai intuíción alapszik, de algebrailag formálizálva szintén egy hasznos eszközünk lesz.

3.8 Definíció. Legyen C_1, C_2 két sima görbe, $\phi : C_1 \rightarrow C_2$ nem konstans leképezés közöttük, $P \in C_1$. ϕ **elágazási indexe** P -ben $e_\phi(P) = \text{ord}_P(\phi^* t_{\phi(P)})$, ahol $t_{\phi(P)} \in K(C_2)$ prímelem $\phi(P)$ -ben. Azt mondjuk, hogy ϕ **nem elágazó** P -ben, ha $e_\phi(P) = 1$, és ϕ nem elágazó, ha C_1 minden pontjában az.

3.8.1 Megjegyzés. Szemléletesen az elágazási index azt méri, hogy az adott pontban ϕ hányszorosan képezi rá C_1 -et C_2 -re.

3.8.2 Megjegyzés. Látható, hogy $e_\phi(P) \geq 1$, hiszen $\text{ord}_{\phi(P)} t_{\phi(P)} = 1$, azaz $t_{\phi(P)} \in M_{\phi(P)}$, így $\phi^* t_{\phi(P)} \in M_P$, tehát $\text{ord}_P(\phi^* t_{\phi(P)}) \geq 1$.

3.4 Állítás. Legyen C_1, C_2 két sima görbe, $\phi : C_1 \rightarrow C_2$ nem konstans leképezés közöttük. Ekkor

$$1, \forall Q \in C_2 : \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi.$$

$$2, \text{ véges sok kivétellel } \forall Q \in C_2 : \#\phi^{-1}(Q) = \deg_s \phi.$$

$$3, \text{ ha } \psi : C_2 \rightarrow C_3 \text{ egy másik nem konstans leképezés, akkor } \forall P \in C_1 \ e_{\psi \circ \phi}(P) = e_\phi(P) e_\psi(\phi(P)).$$

Bizonyítás. 1, 2, Nem bizonyítjuk (ld. [3] Hartshorne: Algebraic Geometry, Ch.II., Prop. 6.8, 6.9).

3, Legyen $t_{\phi(P)}, t_{\psi \circ \phi(P)}$ prímelem az adott pontokban. $\text{ord}_{\phi(P)}(t_{\phi(P)}^{e_\psi(\phi(P))}) = e_\psi(\phi(P)) \text{ord}_{\phi(P)}(t_{\phi(P)}) = e_\psi(\phi(P))$, valamint $\text{ord}_{\phi(P)}(\psi^* t_{\psi \circ \phi(P)}) = e_\psi(\phi(P))$ definíció alapján.

$$\text{Így } e_\phi(P) e_\psi(\phi(P)) = \text{ord}_P(\phi^* t_{\phi(P)}^{e_\psi(\phi(P))}) = \text{ord}_P(\phi^* \psi^* t_{\psi \circ \phi(P)}) = \text{ord}_P((\psi \phi)^* t_{\psi \circ \phi(P)}) = e_{\psi \circ \phi}(P). \quad \square$$

3.5 Állítás. C_1, C_2 két sima görbe, $\phi : C_1 \rightarrow C_2$ nem elágazó pontosan akkor, ha $\#\phi^{-1}(Q) = \deg \phi$ $\forall Q \in C_2$

Bizonyítás. A 3.4 Állítás 1, részéből $\deg \phi = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)$. Ez pontosan akkor egyenlő $\#\phi^{-1}(Q)$, ha $\forall P \ e_\phi(P) = 1$ (mivel $e_\phi(P) \geq 1$), azaz ϕ nem elágazó. $\square$

3.4 A Frobenius homomorfizmus

Számunkra a legfontosabb morfizmus az ún. Frobenius homomorfizmus lesz, ugyanis ennek a görbe K -racionális pontjai fixpontjai lesznek.

3.9 Definíció. Legyen $\text{char}(K) = p > 0$, $q = p^r$, $f \in K[X]$. Ekkor $f^{(q)}$ az a polinom, amit f együtthatóinak q -adik hatványra emelésével kapunk.

Ha $C|K$ egy görbe, akkor belőle a $C^{(q)}|K$ új görbe az a görbe lesz, amelyre $I(C^{(q)})$ a $\{f^{(q)} : f \in I(C)\}$ által generált ideál.

A $\phi : C \rightarrow C^{(q)}$, $\phi([x_0, \dots, x_n]) = [x_0^q, \dots, x_n^q]$ leképezést a q -adik **Frobenius homomorfizmusnak** nevezzük.

3.9.1 Megjegyzés. $C^{(q)}$ tényleg görbe lesz: az világos, hogy varietás, a dimenziója pedig $\dim(C^{(q)}) = \text{trdeg}(\bar{K}(C^{(q)})|\bar{K}) = \text{trdeg}(\bar{K}(C)|\bar{K})$, mivel $I(C^{(q)}) \cong I(C)$.

3.9.2 Megjegyzés. A q -adik Frobenius homomorfizmus tényleg $C^{(q)}$ -ba képez:

Ehhez elég belátni, hogy $\forall P = [x_0, \dots, x_n] \in C$ $\phi(P)$ gyöke $I(C^{(q)})$ generátorainak. Ez pedig $\text{char}(K) = p$ miatt valóban teljesül:

$$f^{(q)}(\phi(P)) = f^{(q)}(x_0^q, \dots, x_n^q) = (f(x_0, \dots, x_n))^q = 0.$$

3.6 Állítás. Ha $\text{char}(K) = p > 0$, $q = p^r$, $C|K$ görbe, $\phi : C \rightarrow C^q$ a q -adik Frobenius homomorfizmus.

Ekkor

$$1, \phi^* K(C^{(q)}) = K(C)^q := \{f^q : f \in K(C)\}.$$

$$2, \deg \phi = q.$$

Bizonyítás. 1, $K(C) = \{f/g : f, g \in \text{homogén}, \mathbb{P}^n - \text{beli}, \deg f = \deg g\}$.

$$K(C) > \phi^* K(C^{(q)}) = \{\phi^*(f^{(q)}/g^{(q)}) : f, g \in \text{homogén}\} \stackrel{\text{mivel } K \text{ tökéletes}}{=} \{f^{(q)}/g^{(q)} : f, g \in \text{homogén}\}$$

$$\{f^{(q)}/g^{(q)} : f, g \in \text{homogén}, \mathbb{P}^n - \text{beli}, \deg f = \deg g\} = \{f(x_0^q, \dots, x_n^q)/g(x_0^q, \dots, x_n^q)\}.$$

$$K(C) > K(C)^q = \{f(x_0, \dots, x_n)^q/g(x_0, \dots, x_n)^q\}.$$

Mivel K tökéletes és $\text{char}(K) = p$, így $(K[X_0, \dots, X_n])^q = K[X_0^q, \dots, X_n^q]$, azaz $\phi^* K(C^{(q)}) = K(C)^q$.

Ezzel azt is nyertük, hogy ϕ , azaz $K(C)|\phi^* K(C^{(q)})$ tisztán inszeparábilis, azaz $K(C)$ minden eleme egy $x^q = a$, $a \in \phi^* K(C^{(q)})$ alakú egyenlet gyöke.

2, Legyen $t \in K(C)$ egy P -beli prímelem. Ekkor $K(C)|K(t)$ szeparábilis a 2.4 Állítás alapján, $K(C)|K(C)^q$ tisztán inszeparábilis.

$$K(C)|K(C)^q(t)|K(C)^q$$

$$K(C)|K(C)^q(t)|K(t)$$

Legyen $f \in K(C)$ és jelölje $m_{K(C)|F}$ a $K(C)|F$ bővítésbeli minimálpolinomját. $m_{K(C)|K(C)^q}(x) = x^q - a$ alakú, ahol $a \in K(C)^q$, azaz $\exists b \in K(C) : a = b^q$. Így $m_{K(C)|K(C)^q}(x) = x^q - b^q = (x - b)^q$, mivel $\text{char}(K) = p$.

$m_{K(C)|K(t)}(x)$ szeparábilis.

Így $m_{K(C)|K(C)^q(t)}(x) \mid (x - b)^q$ és $m_{K(C)|K(C)^q(t)}(x) \mid m_{K(C)|K(t)}(x)$, ami miatt $m_{K(C)|K(C)^q(t)}(x)$ is szeparábilis. Ez csakis úgy lehetséges, hogy $m_{K(C)|K(C)^q(t)}(x) = x - b$, azaz $K(C) = K(C)^q(t)$.

Az 1. rész miatt $\deg \phi = [K(C) : \phi^* K(C^{(q)})] = [K(C)^q(t) : K(C)^q]$. Mivel $t^q \in K(C)^q$, az előbbi gondolatmenethez hasonlóan ekkor $t^q K(C)^q(t)|K(C)^q$ -beli minimálpolinomja $(x - t^q)$ divizorja. Ha a minimál polinom $(x - c)^s$ lenne, ahol $1 \leq s \leq q$, akkor a konstans tagot tekintve $t^s \in K(C)^q$, azaz $\exists g \in K(C) : t^s = g^q$. Ekkor $s = \text{ord}_P(t^s) = \text{ord}_P(g^q) = q \text{ord}_P(g)$, azaz $q|s$, ami csakis $q = s$ esetén állhat fenn. $\square$

3.7 Állítás. Legyen C_1, C_2 két sima görbe, $\phi : C_1 \rightarrow C_2$ leképezés közöttük, $\text{char}(K) = p > 0$. Ekkor ϕ felbontható $C_1 \xrightarrow{\phi_1} C_1^{(q)} \xrightarrow{\phi_2} C_2$, ahol $q = \deg_i \phi$, és ϕ_1 a q -adik Frobenius homomorfizmus, ϕ_2 szeparábilis.

Bizonyítás. Legyen $L = \phi^* K(C_2)$ szeparábilis lezártja $K(C_1)$ -ben. Ekkor $K(C_1)|L$ tisztán inszeparábilis és $[K(C_1) : L] = q$, így $K(C_1)^q \subseteq L$.

A 3.6 Állítást felhasználva $K(C_1)^q = \phi_1^* K(C_1^{(q)})$, $[K(C_1) : \phi_1^* K(C_1^{(q)})] = q$.

Ekkor a bővítések fokait összevetve azt kapjuk, hogy $L = \phi_1^* K(C_1^{(q)})$, azaz $K(C_1)|\phi_1^* K(C_1^{(q)})|\phi^* K(C_2)$.

Emiatt létezik $\iota : K(C_2) \rightarrow K(C_1^{(q)})$ injekció ($\iota := (\phi_1^*)^{-1} \circ id_{\phi_1^* K(C_1^{(q)})} \circ \phi^*$), ami fixen hagyja K -t. A

3.3 Állítás 2, része alapján így létezik egy $\phi_2 : C_1^{(q)} \rightarrow C_2$ leképezés, amire $\phi_2^* = \iota$. Ekkor tetszőleges $f \in \phi^* K(C_2)$ -re $(\phi_2 \circ \phi_1)^* f = (\phi_1^* \circ \phi_2^*) f = \phi_1^* (\phi_1^*)^{-1} \circ id_{\phi_1^* K(C_1^{(q)})} \circ \phi^* f = \phi^* f$.

Tehát $\phi = \phi_2 \circ \phi_1$. □

4 A divizorok

A Hasse becslés bizonyításában központi szerepet töltenek be ezek a görbékhez asszociált formális összegek. Ahogyan később látni fogjuk, többféle felírásukkal információkat tudunk kinyerni például a görbe struktúrájáról vagy egy $\overline{K}(C)$ -beli függvényről.

4.1 A divizor- és a Picard csoport

4.1 Definíció. Egy C görbe **divizor csoportja** a pontjai által generált szabad Abel-csoport, amit $\text{Div}(C)$ -vel jelölünk, elemeit **divizoroknak** hívjuk. A P ponthoz tartozó divizort (P) -vel jelöljük.

Tehát $\text{Div}(C) = \left\{ \sum_{P \in C} n_P (P) : n_P \in \mathbb{Z} \text{ és csak véges sok nem } 0 \right\}$.

4.2 Definíció. Egy $D \in \text{Div}(C)$ **divizor foka** alatt $\deg D = \sum_{P \in C} n_P$ -t értjük.

4.2.1 Megjegyzés. A 0-fokú divizorok $\text{Div}^0(C) < \text{Div}(C)$ részcsoportját alkotják az divizoroknak.

4.3 Definíció. Ha $C|K$, $\sigma \in \text{Gal}(\overline{K}|K)$, és $D \in \text{Div}(C)$, akkor $D^\sigma := \sum_{P \in C} n_P (P^\sigma)$.

D K felett definiált, ha $D^\sigma = D \ \forall \sigma \in \text{Gal}(\overline{K}|K)$.

4.3.1 Megjegyzés. A K felett definiált divizorok is csoportot alkotnak, amit $\text{Div}_K(C)$ -vel jelölünk.

4.4 Definíció. Legyen $0 \neq f \in \overline{K}(C)$. Az f -hez **rendelt divizor** $\text{div}(f) = \sum_{P \in C} \text{ord}_P f (P)$.

4.4.1 Megjegyzés. A 2.3 Állítás miatt csak véges pont együtthatója nem 0.

4.5 Definíció. Egy $D \in \text{Div}(C)$ divizor **fődivizor**, ha előáll $D = \text{div}(f)$ alakban, valamely $0 \neq f \in \overline{K}(C)$ -re.

$D_1, D_2 \in \text{Div}(C)$ **lineárisan ekvivalens**, $D_1 \sim D_2$, ha $D_1 - D_2$ fődivizor.

$\text{Pic}(C) := \text{Div}(C) / \sim$ C **Picard-csoportja**.

4.6 Definíció. Duális leképezést divizor csoportok között is definiálhatunk:

Legyen C_1, C_2 két sima görbe, $\phi : C_1 \rightarrow C_2$ nem konstans leképezés közöttük. ϕ indukál egy leképezést az divizor csoportok között: $\phi^* : \text{Div}(C_2) \rightarrow \text{Div}(C_1)$, $(Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)$, tetszőleges divizorokra pedig lineárisan terjed ki.

4.1 Állítás. 1, $\deg(\phi^* D) = \deg \phi \cdot \deg D \ \forall D \in \text{Div}(C_2)$

2, $\phi^* \text{div}(f) = \text{div}(\phi^* f)$ minden $f \in \bar{K}(C_2) - \{0\}$ -ra

3, Ha $\psi : C_2 \rightarrow C_3$ egy másik nem konstans leképezés, akkor $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.

Bizonyítás. 1, Legyen $D = \sum_{Q \in C_2} n_Q Q$.

$$\text{Ekkor } \deg(\phi^* D) = \deg\left(\sum_{Q \in C_2} n_Q \phi^*(Q)\right) = \deg\left(\sum_{Q \in C_2} n_Q \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)\right) = \sum_{Q \in C_2} \sum_{P \in \phi^{-1}(Q)} n_Q e_\phi(P).$$

A 3.4 Állítás 1, része alapján $\deg \phi = \sum_{P \in \phi^{-1}(R)} e_\phi(P)$ tetszőleges $R \in C_2$ -re.

Másrészt $\deg D = \sum_{Q \in C_2} n_Q$.

$$\text{Így } \deg D \cdot \deg \phi = \sum_{Q \in C_2} n_Q \cdot \sum_{P \in \phi^{-1}(R)} e_\phi(P) = \sum_{Q \in C_2} n_Q \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \sum_{Q \in C_2} \sum_{P \in \phi^{-1}(Q)} n_Q e_\phi(P) = \deg(\phi^* D).$$

2, Legyen $P \in C_1$ tetszőleges, $t_{\phi(P)}$ egy prímelem $\phi(P)$ -ben. Ekkor $\text{ord}_P(\phi^* f) = \text{ord}_{\phi(P)}(f) = \text{ord}_{\phi(P)}(t_{\phi(P)}) \text{ord}_{\phi(P)}(f) = \text{ord}_P(\phi^* t_{\phi(P)}) \text{ord}_{\phi(P)}(f) = e_\phi(P) \text{ord}_{\phi(P)}(f)$.

$$\text{Ezt felhasználva } \phi^*(\text{div} f) = \phi^*\left(\sum_{Q \in C_2} \text{ord}_Q(f)(Q)\right) = \sum_{Q \in C_2} \text{ord}_Q(f) \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) = \sum_{Q \in C_2} \sum_{P \in \phi^{-1}(Q)} \text{ord}_Q(f) e_\phi(P)(P) = \sum_{Q \in C_2} \sum_{P \in \phi^{-1}(Q)} \text{ord}_P(\phi^* f)(P) = \sum_{P \in C_1} \text{ord}_P(\phi^* f)(P) = \text{div}(\phi^* f).$$

3, A 3.4 Állítás 3, része alapján $e_{\psi \circ \phi}(P) = e_\phi(P) e_\psi(\phi(P))$. Legyen $R \in C_3$, ekkor $(\phi^* \circ \psi^*)(R) =$

$$\begin{aligned} \phi^*(\psi^*(R)) &= \phi^*\left(\sum_{Q \in \psi^{-1}(R)} e_\psi(Q)(Q)\right) = \sum_{Q \in \psi^{-1}(R)} e_\psi(Q) \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) = \\ &= \sum_{Q \in \psi^{-1}(R)} \sum_{P \in \phi^{-1}(Q)} e_\psi(Q) e_\phi(P)(P) = \sum_{Q \in \psi^{-1}(R)} \sum_{P \in \phi^{-1}(Q)} e_{\psi \circ \phi}(P)(P) = \sum_{P \in (\psi \circ \phi)^*(R)} e_{\psi \circ \phi}(P)(P) = \\ &= (\psi \circ \phi)^*(R). \end{aligned} \quad \square$$

4.2 Állítás. Legyen C egy sima görbe, $f \in \bar{K}(C) - \{0\}$. Ekkor $\deg \text{div}(f) = 0$.

Bizonyítás. Az egyszerűbb írásmód kedvéért a $[0, 1]$ -et 0-ként írjuk a bizonyítás további részében.

A 4.1 Állítás 2, része alapján $\hat{f}^* \text{div}(id) = \text{div}(\hat{f}^* id) = \text{div}(id \circ \hat{f}) = \text{div}(f)$, másrészt $\text{div}(id) = \sum_{P \in \mathbb{P}^1} \text{ord}_P(id)(P) = (0) + \text{ord}_\infty(id)(\infty) = (0) + \text{ord}_0(1/x)(\infty) = (0) - \text{ord}_0(id)(\infty) = (0) - (\infty)$. Tehát $\text{div}(f) = \hat{f}^*((0) - (\infty))$.

A 4.1 Állítás 1, részét felhasználva $\deg \text{div}(f) = \deg(\hat{f}^*((0) - (\infty))) = \deg \hat{f}^*((0)) - \deg \hat{f}^*((\infty)) = \deg \hat{f} \cdot \deg((0)) - \deg \hat{f} \cdot \deg((\infty)) = \deg \hat{f} - \deg \hat{f} = 0$. $\square$

4.2 $\mathcal{L}(D)$

4.7 Definíció. C egy görbe, a $D = \sum_{P \in C} n_P P \in \text{Div}(C)$ divizor **pozitív**, ha $n_P \geq 0$ minden P -re. Ezt $D \geq 0$ -bal jelöljük.

$D_1, D_2 \in \text{Div}(C)$, $D_1 \geq D_2$, ha $D_1 - D_2 \geq 0$.

4.8 Definíció. C egy görbe, $D \in \text{Div}(C)$. Ekkor legyen $\mathcal{L}(D) := \{f \in \overline{K}(C) - \{0\} : \text{div}(f) \geq -D\} \cup \{0\}$ véges dimenziós $\overline{K}$ -vektortér.

A dimenzióját $\dim_{\overline{K}} \mathcal{L}(D) =: \ell(D)$ -vel jelöljük.

4.3 Állítás. C egy görbe, $D, D' \in \text{Div}(C)$.

- 1, Ha $\deg D < 0$, akkor $\mathcal{L}(D) = \{0\}$ és $\ell(D) = 0$.
- 2, $\mathcal{L}(D)$ valóban egy véges dimenziós $\overline{K}$ -vektortér.
- 3, Ha $D \sim D'$, akkor $\mathcal{L}(D) \cong \mathcal{L}(D')$ (és $\ell(D) = \ell(D')$).

Bizonyítás. 1, Tegyük fel, hogy $f \in \mathcal{L}(D) \neq \{0\}$, $f \neq 0$. A 4.2 Állítás alapján $0 = \deg \text{div}(f) \geq \deg(-D) = -\deg(D)$, amiből $\deg(D) \geq 0$, ami ellentmondás.

2, Legyen $D = \sum_{P \in C} n_P P$.

$\mathcal{L}(D)$ vektortér: $f, g \in \mathcal{L}(D)$, $k \in \overline{K}$, ekkor $\text{ord}_P(f + g) \geq \min(\text{ord}_P(f), \text{ord}_P(g)) \geq -n_P$, azaz $\text{div}(f + g) \geq -D$, $f + g \in \mathcal{L}(D)$, valamint $\text{ord}_P(kf) = \text{ord}_P(k) + \text{ord}_P(f) = 0 + \text{ord}_P(f) = \text{ord}_P(f) \geq -n_P$, azaz $\text{div}(kf) \geq -D$, $kf \in \mathcal{L}(D)$.

Végesség: Mivel $\overline{K}(C)|\overline{K}$ véges, és $\overline{K}(C)|\mathcal{L}(D)|\overline{K}$, így szükségszerűen $\mathcal{L}(D)|\overline{K}$ is az.

3, $D \sim D'$, azaz létezik $f \in \overline{K}(C)$, amire $D - D' = \text{div}(f)$. Ekkor $\mathcal{L}(D) \rightarrow \mathcal{L}(D'), g \mapsto gf$ egy izomorfizmus, hiszen $\text{div}(g) \geq -D \iff \text{div}(gf) \geq -D'$ ($\text{div}(gf) = \text{div}(g) + \text{div}(f) = \text{div}(g) + D - D'$). □

5 A differenciálformák

A differenciálformák a deriváltfüggvények algebrai megfelelői, az analitikus jelentés helyett algebrailag vizsgáljuk őket (ld. már csak definíciót is). Nekünk a szeparábilis leképezések vizsgálatánál, a görbék geometriai jellemzésénél, illetve később az elliptikus görbék esetén bizonyos morfizmusok linearizációjánál lesznek hasznosak.

5.1 Néhány alapvető fogalom és állítás

5.1 Definíció. Legyen C egy görbe. A $\{dx : x \in \overline{K}(C)\}$ szimbólumok által generált $\overline{K}(C)$ -vektortér, melyre

- 1, $d(x + y) = dx + dy \ \forall x, y \in \overline{K}(C)$
- 2, $d(xy) = xdy + ydx \ \forall x, y \in \overline{K}(C)$
- 3, $da = 0 \ \forall a \in \overline{K}$,

a C görbe **differenciálformáinak tere**, amit Ω_C -vel jelölünk.

5.2 Definíció. Duális leképezések:

Legyen C_1, C_2 két görbe, $\phi : C_1 \rightarrow C_2$ nem konstans leképezés közöttük. Ekkor a $\phi^* : \overline{K}(C_2) \rightarrow$

$\overline{K}(C_1)$ indukál egy leképezést a differenciálformák terei között: $\phi^* : \Omega_{C_2} \rightarrow \Omega_{C_1}$, $\phi^*(\sum_{i=1}^n f_i dx_i) := \sum_{i=1}^n (\phi^* f_i) d(\phi^* x_i)$.

5.1 Állítás. Legyen C egy görbe. Ekkor Ω_C egy 1-dimenziós $\overline{K}(C)$ -vektortér, továbbá $x \in \overline{K}(C)$ -re dx bázis pontosan akkor, ha $\overline{K}(C)|\overline{K}(x)$ véges, szeparábilis bővítés.

Bizonyítás. Nem bizonyítjuk (ld. [4] Shafarevich: Basic Algebraic Geometry 1, Ch.3, §5, Thm.3.17).

5.2 Állítás. Legyenek C_1, C_2 görbék. Ha $\phi : C_1 \rightarrow C_2$ nem konstans leképezés, akkor ϕ szeparábilis pontosan akkor, ha $\phi^* : \Omega_{C_2} \rightarrow \Omega_{C_1}$ injektív.

Bizonyítás. Legyen dy Ω_{C_2} bázisa, azaz az 5.1 Állítás miatt $\overline{K}(C_2)|\overline{K}(y)$ szeparábilis.

Így $\phi^* \overline{K}(C_2)|\phi^* \overline{K}(y) = \overline{K}(\phi^* y)$ is szeparábilis.

ϕ^* pontosan akkor injektív, ha $d(\phi^* y) \neq 0$, ami az 5.1 Állítás miatt ekvivalens azzal, hogy $d(\phi^* y)$ bázisa Ω_{C_1} -nek, ami pedig szintén az 5.1 Állítás miatt ekvivalens azzal, hogy $\overline{K}(C_1)|\overline{K}(\phi^* y)$ szeparábilis, ami pedig a 3.2.7 Megjegyzés alapján ekvivalens azzal, hogy $\overline{K}(C_1)|\phi^* \overline{K}(C_2)$ szeparábilis azaz ϕ szeparábilis. $\square$

5.3 Állítás. C egy görbe, $P \in C$, $t \in \overline{K}(C)$ prímelem P -ben. Ekkor

1, tetszőleges $\omega \in \Omega_C$ -re létezik egyértelműen egy $g \in \overline{K}(C)$ úgy, hogy $\omega = gdt$. Ezt a g -t ω/dt -vel jelöljük.

2, ha $f \in \overline{K}(C)$ reguláris P -ben, akkor df/dt is az.

3, $\text{ord}_P(\omega/dt)$ csak ω -tól és P -től függ, t -től független. Ezt $\text{ord}_P(\omega)$ -val jelöljük.

4, ha $x \in \overline{K}(C)$ olyan, hogy $\overline{K}(C)|\overline{K}(x)$ szeparábilis és $x(P) = 0$, akkor minden $f \in \overline{K}(C)$ -re $\text{ord}_P(fdx) = \text{ord}_P(f) + \text{ord}_P(x) - 1$.

5, legfeljebb véges sok kivétellel minden $P \in C$ -re $\text{ord}_P(\omega) = 0$.

Bizonyítás. 1, 5.1 Állításból azonnal következik.

2, A deriválási szabályokból (az analízisben tanultakhoz hasonlóan) könnyen adódik, hogy $d(\frac{x}{y}) = \frac{y \cdot dx - x \cdot dy}{y^2}$ minden $x, y \in \overline{K}(C)$ -re. Így az $f = \frac{f_1}{f_2}$; $f_1, f_2 \in K[C]$ függvényre $df = d(\frac{f_1}{f_2}) = \frac{f_2 \cdot df_1 - f_1 \cdot df_2}{f_2^2} = \frac{f_2 \cdot (df_1/dt) - f_1 \cdot (df_2/dt)}{f_2^2} \cdot dt$, így az 1. rész alapján $df/dt = \frac{f_2 \cdot (df_1/dt) - f_1 \cdot (df_2/dt)}{f_2^2} = \frac{f_2 \cdot df_1 - f_1 \cdot df_2}{f_2^2 \cdot dt}$. Mivel dt bázisa Ω_C -nek, így szükségképpen nem lehet se gyöke, se pólusa egyik pontban sem, az pedig, hogy f P -ben reguláris, éppen azt jelenti, hogy $f_2 \notin M_P$, és így $f_2^2 \notin M_P$. És a számlálóból sem származhat pólus, mivel a deriválási szabályokból az is könnyen következik, hogy nem vezetnik ki $K[C]$ -ből. Tehát ekkor df/dt is reguláris P -ben.

3, Legyen t, t' két prímelem P -ben. Ekkor a 2. rész alapján dt/dt' és dt'/dt reguláris P -ben, ami $\text{ord}_P(dt/dt') = -\text{ord}_P(dt'/dt)$ miatt csak $\text{ord}_P(dt/dt') = 0$ esetén lehetséges.

Másrészt $\omega = g_t dt' = g_{t'}(dt'/dt)dt$, azaz $g_t = g_{t'}(dt'/dt)$.

Így $\text{ord}_P(\omega/dt') = \text{ord}_P(g_{t'}) = \text{ord}_P(g_{t'}) + \text{ord}_P(dt'/dt) = \text{ord}_P(g_{t'}(dt'/dt)) = \text{ord}_P(g) = \text{ord}_P(\omega/dt)$.
 4, Írjuk fel x -et $x = ut^n$ alakban, ahol $n = \text{ord}_P(x) \geq 1$, és így $\text{ord}_P(u) = 0$. $\text{ord}_P(x) \geq 1$, mivel, ha $p|n$, akkor $t^{n/p} = (x/u)^{1/p} := \alpha \in \overline{K}(C)$, másfelől ez azt jelenti, hogy α gyöke $\xi^p - (x/u) \in \overline{K}(x, u)[\xi]$ -nek, azonban ennek α p -szeres gyöke ($(\xi^p - (x/u))' \equiv 0$), így $\xi^p - (x/u) = (\xi - \alpha)^p$, viszont $\overline{K}(C)$ szeparábilis $\overline{K}(x, u)$ felett, azaz α minimálpolinomja $\xi - \alpha$, $\alpha \in \overline{K}(x, u)$, $\alpha = f(x, u)/g(x, u)$ valamely $f, g \in K[\xi, \zeta]$ -ra, $x/u = f(x, u)^p/g(x, u)^p = F(x^p, u^p)/G(x^p, u^p)$, ami ellentmondás.

A differenciálási szabályok alapján $dx = du \cdot t^n + u \cdot dt^n = du \cdot t^n + u \cdot nt^{n-1} \cdot dt = [(du/dt)t^n + nut^{n-1}]dt$.
 A 2, rész alapján du/dt reguláris P -ben, így ha $n \neq 0$, akkor $\text{ord}_P(dx) = \text{ord}_P([(du/dt)t^n + nut^{n-1}]dt) = \text{ord}_P(nut^{n-1}dt) = n - 1$. Így $\text{ord}_P(fdx) = \text{ord}_P(f \cdot nut^{n-1}dt) = \text{ord}_P(f) + n - 1$.

5, Ezt az állítást csak elliptikus görbékre látjuk be (később ezekre fogjuk használni), azaz felteszzük, hogy $C = V(\langle y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \rangle)$

A 2.2.2 Megjegyzés alapján $x - x_0$ prímelem $P = (x_0, y_0)$ -ban, ugyanis generálja M_P -t: $M_P = \langle x - x_0, y - y_0 \rangle$ generálja, másrészt most $y^2 + a_1xy + a_3y - (y_0^2 + a_1xy_0 + a_3y_0) = x^3 + a_2x^2 + a_4x + a_6 - (x_0^3 + a_2x_0^2 + a_4x_0 + a_6)$, ahonnan $(y - y_0)(y + y_0 + a_1x + a_3) = (x - x_0)(x^2 + xx_0 + x_0^2 + a_2(x + x_0) + a_4)$, véges sok pont kivételével $y + y_0 + a_1x + a_3$ egység $K[C]_P$ -ben, így $y - y_0 = (x - x_0) \frac{x^2 + xx_0 + x_0^2 + a_2(x + x_0) + a_4}{y + y_0 + a_1x + a_3}$, azaz $y - y_0$ kifejezhető $x - x_0$ többszöröseként, így $x - x_0$ generálja M_P -t.

A 4, rész alapján pedig $\text{ord}_P(\omega) = \text{ord}_P(fd(x - x_0)) = \text{ord}_P(f) + \text{ord}_P(x - x_0) - 1 = 0 + 1 - 1 = 0$. $\square$

5.2.1 Megjegyzés. A 4, pont speciálisan azt mondja $f \equiv 1$ -gyel, hogy $\text{ord}_P(dx) = \text{ord}_P(x) - 1$ minden $x \in \overline{K}(C)$ -re.

5.2 Differenciálformák divizorjai

5.3 Definíció. Legyen $\omega \in \Omega_C$. Az ω -hoz asszociált divizor $\text{div}(\omega) = \sum_{P \in C} \text{ord}_P(\omega)(P) \in \text{Div}(C)$.

5.4 Definíció. C kanonikus divizor osztálya $\text{div}(\omega)$ osztálya $\text{Pic}(C)$ -ben tetszőleges $0 \neq \omega \in \Omega_C$ -re. Ezen osztály bármely elemét kanonikus divizornak nevezzük.

5.4.1 Megjegyzés. A definíció értelmes, hiszen ha $\omega_1, \omega_2 \in \Omega_C$ nem 0 differenciálformák, akkor 5.1 Állítás miatt $\omega_1 = f\omega_2$ valamely $f \in \overline{K}(C)$ -ra. Így $\text{ord}_P(\omega_1) = \text{ord}_P(f\omega_2) = \text{ord}_P(f) + \text{ord}_P(\omega_2)$ minden $P \in C$ -re, azaz $\text{div}(\omega_1) = \text{div}(f) + \text{div}(\omega_2)$. Tehát $\text{div}(\omega_1) \sim \text{div}(\omega_2)$.

5.1 Tétel. Riemann-Roch tétel

Legyen C egy sima görbe, K_C kanonikus divizor C -n. Ekkor létezik $g \in \mathbb{Z}_{\geq 0}$, amit C génuszának nevezünk, hogy minden $D \in \text{Div}(C)$ -re $\ell(D) - \ell(K_C - D) = \deg D - g + 1$

Bizonyítás. Nem bizonyítjuk (ld. [5] Lang: Introduction to Algebraic and Abelian Functions, Ch. I, §2).

5.1.1 Következmény. Ha $\deg D > 2g - 2$, akkor $\ell(D) = \deg D - g + 1$.

Bizonyítás. A Riemann-Roch tételt fogjuk használni.

1, 0-ra: $-g + 1 = \deg 0 - g + 1 = \ell(0) - \ell(K_C - 0) = \dim_{\overline{K}} \overline{K} - \ell(K_C) = 1 - \ell(K_C)$, így $\ell(K_C) = g$.
($\mathcal{L}(0) = \overline{K}$, mivel a 4.2 Állításból tudjuk, hogy $\deg \operatorname{div}(f) = 0$ minden $f \in \overline{K}(C)$ -re, így $\operatorname{div}(f) \geq 0$ csakis úgy lehet, ha $\operatorname{div}(f) = 0$, azaz ha f nem 0 konstans.)

2, K_C -re: $\deg K_C - g + 1 = \ell(K_C) - \ell(0) = g - 1$, így $\deg K_C = 2g - 2$.

Tehát $\deg(K_C - D) < 0$, így a Riemann-Roch tételt, illetve a 4.3 Állítás 1, részét használva

$\deg(K_C - D) - g + 1 = \ell(K_C - D) - \ell(D) = 0 - \ell(D)$, azaz $\ell(D) = g - 1 - \deg K_C + \deg D = g - 1 - 2g + 2 + \deg D = \deg D - g + 1$. $\square$

5.5 Definíció. Az $\omega \in \Omega_C$ differenciálformát is regulárisnak hívjuk $P \in C$ -ben, ha $\operatorname{ord}_P(\omega) \geq 0$, és **regulárisnak**, ha C minden pontban az.

5.4 Állítás. A $\mathbb{P}^1$ görbe génusza 0.

Bizonyítás. Először megmutatjuk, hogy $\mathbb{P}^1$ -en nincsen reguláris differenciál forma. Legyen t koordináta függvény $\mathbb{P}^1$ -en (azaz $\mathbb{P}^1 = \{[t, 1] : t \in \overline{K}\} \cup \infty$, ha X, Y a homogén koordináták, akkor $t = X/Y$). Ekkor tetszőleges $\omega \in \Omega_{\mathbb{P}^1}$ -re az 5.3 Állítás 1, része alapján létezik $g \in \overline{K}(\mathbb{P}^1)$, hogy $\omega = gdt$. Ekkor tehát $P = [t_0, 1]$ -ben $\operatorname{ord}_P(\omega) = \operatorname{ord}_P(g)$ (mivel $dt = d(t - t_0)$, és $t - t_0$ prímelem P -ben). ∞ -ben pedig $1/t$ lesz a prímelem, a deriválási szabályokból $d(1/t) = -dt/t^2$, így $\omega = gdt = -t^2g(-dt/t^2) = -t^2gd(1/t)$. Vagyis $\operatorname{ord}_{\infty}(\omega) = \operatorname{ord}_{\infty}(-t^2g) = \operatorname{ord}_{\infty}(g) - 2$. Tehát $\deg \operatorname{div}(\omega) = \deg \operatorname{div}(g) - 2 = -2$ a 4.2 Állítást felhasználva.

Azt is észre vehetjük, hogy egy C görbére és a $K_C = \operatorname{div}(\omega)$ kanonikus osztóra (ω -t válasszuk bázisnak) $\mathcal{L}(K_C) \cong \{\Omega_C \text{ reguláris elemei}\}$, ugyanis a $\varphi : \mathcal{L}(K_C) \rightarrow \{\Omega_C \text{ reguláris elemei}\}$, $f \mapsto f\omega$ egy izomorfizmus:

1. értelmes, mivel ha $f \in \mathcal{L}(K_C)$, akkor $\operatorname{div}(f) \geq \operatorname{div}(\omega)$, így $\operatorname{div}(f\omega) \geq 0$, ami éppen azt jelenti, hogy $f\omega$ reguláris
2. ez triviálisan egy injektív homomorfizmus
3. szürjektivitás: minden $\{\text{reguláris } \omega \in \Omega_C\}$ előáll $f\omega$ aakban, ahol $f \in \overline{K}(C)$, az hogy reguláris, éppen azt jelenti, hogy $\operatorname{div}(f\omega) \geq 0$, vagyis $\operatorname{div}(f) \geq -\operatorname{div}(\omega)$, azaz $f \in \mathcal{L}(K_C)$.

Így $\ell(K_C) = \dim_{\overline{K}}\{\Omega_C \text{ reguláris elemei}\}$. Ez most a mi esetünkre nézve $\ell(K_{\mathbb{P}^1}) = \dim_{\overline{K}}\{\Omega_{\mathbb{P}^1} \text{ reguláris elemei}\} = \dim_{\overline{K}}\{0\} = 0$.

Az 5.1.1 Következmény bizonyításának 1. pontjában belátottak szerint pedig $\ell(K_{\mathbb{P}^1}) = g$, tehát $\mathbb{P}^1$ génusza 0. $\square$

6 Az elliptikus görbék

6.1 A Weierstrass-egyenletek és elliptikus görbék

Bevezetjük az algebrailag jól megfogható Weierstrass-egyenletek-, illetve a geometriailag jobban leírható elliptikus görbék fogalmát, majd megmutatjuk, hogy (legalábbis a mi céljaink szempontjából) a kettő lényegében ugyanazt jelenti.

6.1 Definíció. Weierstrass-egyenletnek nevezzük az $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ alakú homogén egyenletet, ahol $a_1, \dots, a_6 \in \overline{K}$. Ha $a_1, \dots, a_6 \in K$, akkor az általa megadott görbe definiált K felett.

Ennek egyetlen ideális pontja a $[0, 1, 0] := \infty$. A továbbiakban az egyszerűség kedvéért az egyenlet inhomogén $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ alakját fogjuk használni, nem megfelelően a ∞ pontjáról.

6.1.1 Megjegyzés. Ha f egy Weierstrass-egyenlet, akkor valóban görbét ad meg: ha V jelöli az általa megadott varietást, akkor $\text{trdeg}(\overline{K}(V)|\overline{K}) = \text{trdeg}(\text{Quot}(\overline{K}[x, y]/\langle f \rangle)|\overline{K}) = 1$, ugyanis $\{y\}$ egy transzcendencia bázis, hiszen x kifejezhető y -nal, mivel f x -re egy harmadfokú egyenlet y paraméterrel.

6.2 Definíció. Definiálunk néhány jellemző értéket:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \quad b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$\Delta := -b_2^2b_8 - 3b_4^3 - 27b_6^2 + 9b_2b_4b_6 \text{ az egyenlet \textbf{diszkriminánsa}},$$

$\omega := dx/(2y + a_1x + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1y)$ az egyenlet **invariáns differenciálja** (a két alakot a deriválási szabályoknak az egyenlet mindkét oldalára való alkalmazásából kapjuk).

6.2.1 Megjegyzés. Definícióból kiszámolható, hogy $\Delta \neq 0$ pontosan akkor, ha a Weierstrass-egyenlettel megadott görbe sima.

6.1 Állítás. Az ω invariáns differenciál reguláris ($\text{ord}_P(\omega) \geq 0$) és nincs gyöke E -n ($\text{ord}_P(\omega) \leq 0$), azaz $\text{div}(\omega) = 0$.

Bizonyítás. Legyen $P = (x_0, y_0) \in E$, $F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$. Ekkor $\omega = d(x - x_0)/\partial_y F(x, y) = d(y - y_0)/\partial_x F(x, y)$. P nem lehet ω pólusa, különben $\partial_x F(P) = \partial_y F(x, y) = 0$ lenne, azaz P nem lenne sima, ami ellentmondás.

Legyen $\phi : E \rightarrow \mathbb{P}^1$, $\phi([x, y, 1]) := [x, 1]$, $\deg \phi = [\overline{K}(E) : \phi^*\overline{K}(\mathbb{P}^1)] = 2$ (mivel $\overline{K}(E) = \phi^*\overline{K}(\mathbb{P}^1)(y)$ és $\dim_{\overline{K}(\mathbb{P}^1)} \phi^*\overline{K}(\mathbb{P}^1)(y) = \deg y = 2$, ugyanis $1, y, y^2$ összefügg az E -t megadó egyenlet mentén), így a 3.4. Állítás 1. része alapján $\text{ord}_P(x - x_0) \leq 2$ ($x - x_0$ vehető prímelemnek az elágazási index definíciójában) és $\text{ord}_P(x - x_0) = 2$ pontosan akkor, ha $F(x_0, y)$ -nak 2-szeres gyöke van. Tehát

$\text{ord}_P(x - x_0) = 1$ vagy $\text{ord}_P(x - x_0) = 2$ és $\partial_y F(x_0, y) = 0$. Mindkét esetben az 5.3 Állítás 4. része miatt $\text{ord}_P(\omega) = \text{ord}_P(x - x_0) - \text{ord}_P(\partial_y F) - 1 = 0$.

Egy eset maradt: $P = \infty$. Ekkor pedig legyen t_∞ egy prímelem ∞ -ban. Mivel a 2.1.2 és 2.1.3 Példák alapján $\text{ord}_\infty(x) = -2$ és $\text{ord}_\infty(y) = -3$, így $x = t_\infty^{-2}f$, $y = t_\infty^{-3}g$ valamely $f, g \in \overline{K}(E)$ -re, amelyekre $f(\infty), g(\infty) \neq 0, \infty$.

Ezek alapján $\omega = dx/\partial_y F(x, y) = d(t^{-2}f)/\partial_y F(x, y) = ((-2t^{-3}f + t^{-2}f')/(2t^{-3}g + a_1t^{-2}f + a_3))dt = ((-2f + tf')/(2g + a_1tf + a_3t^3))dt$. (Vegyük észre, hogy $f' = df/dt$ 5.3 Állítás 2. része miatt reguláris ∞ -ban).

Tehát, ha $\text{char}(K) \neq 2$, akkor $((-2f + tf')/(2g + a_1tf + a_3t^3))dt$ ∞ -ban reguláris, nem 0. $\text{char}(K) = 2$ esetén hasonló gondolatmenetet alkalmazhatunk $\omega = dy/\partial_x(x, y)$ -ra. $\square$

6.1.1 Következmény. Egy sima, Weierstrass egyenlettel megadott görbe génusza 1.

Bizonyítás. Tekintsük az ω invariáns differenciált. Az 5.1.1 Következmény bizonyítása során beláttuk, hogy $\deg K_C = 2g - 2$, így ez alapján $2g - 2 = \deg \text{div}(\omega) = \deg 0 = 0$, ahonnan $g = 1$. $\square$

6.3 Definíció. Az **elliptikus görbe** egy (E, O) pár, ahol E egy 1 génuszú sima görbe $\mathbb{P}^2$ -ben és $O \in E$ egy kijelölt bázispont. Ha a bázispont egyértelmű (általában $O = \infty$), egyszerűen E -vel jelöljük.

6.2 Állítás. 1, Minden sima, Weierstrass egyenlettel megadott görbe elliptikus görbe.

2, Fordítva, ha $E|K$ egy K felett definiált elliptikus görbe, akkor létezik $x, y \in K(E)$ úgy, hogy $\phi : E \rightarrow \mathbb{P}^2, \phi = [x, y, 1]$ egy izomorfizmus $E|K$ -ről egy $C \subseteq \mathbb{P}^2$ $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \in K[X, Y]$ Weierstrass egyenlettel megadott sima görbére és $\phi(O) = [0, 1, 0]$.

Bizonyítás. 1, Ezt az előzőek során már beláttuk (6.1.1 Megjegyzés és 6.1.1 Következmény).

2, Az 5.1.1 Következmény miatt $\ell(n(O)) = \deg n(O) - g + 1 = n - 1 + 1 = n$ minden $n = 1, 2, \dots$ -re. Belátható (ld. [2] Silverman: The Arithmetic of Elliptic Curves, Ch. II, Prop. 5.8), hogy ha $C|K$ -nak D egy K felett definiált divizorja, akkor $\mathcal{L}(D)$ -nek van $K(C)$ -beli bázisa. Tehát létezik $x, y \in K(E)$ úgy, hogy $\overline{K}$ felett $\{1, x\}$ bázisa $\mathcal{L}(2(O))$ -nak és $\{1, x, y\}$ pedig bázisa $\mathcal{L}(3(O))$ -nak. Ekkor szükségképpen $\text{ord}_O(x) = -2$ és $\text{ord}_O(y) = -3$, hiszen $\mathcal{L}(n(O)) = \{f \in K(E) - \{0\} : \text{div} f \geq -n(O)\}$.

Mivel $\mathcal{L}(2(O)), \mathcal{L}(3(O)) \subseteq \mathcal{L}(6(O))$, így $1, x, y, x^2, xy, y^2, x^3 \in \mathcal{L}(6(O))$, másrészt viszont $\ell(6(O)) = 6$. Így létezik $\lambda_1, \dots, \lambda_7 \in K$, amire $\lambda_1 + \lambda_2x + \lambda_3y + \lambda_4x^2 + \lambda_5xy + \lambda_6y^2 + \lambda_7x^3 = 0$ ($\lambda_1, \dots, \lambda_7$ azért választható K -belinek, mert a bázist kereshetjük $K(E)$ -ben az előzőleg hivatkozott állítás szerint).

Ekkor $\lambda_6 \neq 0, \lambda_7 \neq 0$, különben a kifejezés minden tagjának más lenne O -ban a rendje, azaz a rendek minimuma lenne a kifejezés rendje, holott ∞ -nek kellene lennie, hiszen 0-val egyenlő.

Az $(x, y) \mapsto (-\lambda_6\lambda_7x, \lambda_6\lambda_7^2y)$ cserével, majd $\lambda_6^3\lambda_7^4$ -nel lenormálva a $\phi = [x, y, 1]$ egy Weierstrass egyenlet görbéjére képez.

$\phi(O) = [0, 1, 0]$, mivel $\text{ord}_O(y) > \text{ord}_O(x)$, így a projektív koordinátákat beszorozhatjuk az y nevezőjével, amitől az első és a harmadik koordinátában gyök lesz.

ϕ morfizmus a 3.1 Állítás miatt és szürjektív a 3.2 Állítás miatt.

Most a 3.3.1 Következmenyt szeretnénk használni, ahhoz, hogy megmutassuk, hogy ϕ izomorfizmus.

Ehhez az kell, hogy $\deg \phi = 1$ legyen, azaz $1 = \deg \phi = [K(E) : \phi^* K(\mathbb{P}^2)] = [K(E) : K(x, y)]$, ami azzal ekvivalens, hogy $K(E) = K(x, y)$.

Ehhez tekintsük a $[x, 1] : E \rightarrow \mathbb{P}^1$ leképezést. x -nek O -ban van 2-szeres pólusa (2.2.2 Megjegyzés), más pontokban pedig nincs pólusa. Így a 3.4 Állítás 1. része miatt $2 = \deg[x, 1] = [K(E) : K(x)]$.

Teljesen hasonlóan, mivel y -nak O -ban 3-szoros pólusa van (2.2.3 Megjegyzés), más pontban pedig nincs pólusa, az $[y, 1] : E \rightarrow \mathbb{P}^1$ leképezés foka 3, így $[K(E) : K(y)] = 3$.

Ezek alapján, mivel $2 = [K(E) : K(x)] = [K(E) : K(x, y)][K(x, y) : K(x)]$, illetve $3 = [K(E) : K(y)] = [K(E) : K(x, y)][K(x, y) : K(y)]$, így $[K(E) : K(x, y)] \mid 2, 3$, amiből $[K(E) : K(x, y)] = 1$.

Az maradt hátra, hogy C sima (ami kell a 3.3.1 Következmeny használhatóságához is). Indirekt tegyük fel, hogy nem az. $(x, y) \mapsto (x - x_0, y - y_0)$ cserével feltehetjük, hogy az $(x_0, y_0) = (0, 0)$ pontban nem sima (ekkor a_6 szükségképpen 0), azaz

$$0 = \partial_x(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6)|_{(0,0)} = a_1y - 3x^2 - 2a_2x - a_4|_{(0,0)} = -a_4, \text{ és}$$

$$0 = \partial_y(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6)|_{(0,0)} = 2y + a_1x + a_3|_{(0,0)} = a_3.$$

Így a Weierstrass-egyenlet $y^2 + a_1xy = x^3 + a_2x^2$ alakú, vagyis a $\varphi : C \rightarrow \mathbb{P}^1$, $(x, y) \mapsto [x, y]$ -ra $\deg \varphi = 1$, mivel létezik inverze: $\varphi^{-1} : \mathbb{P}^1 \rightarrow E$ $[1, t] \mapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t)$.

Így $\varphi \circ \phi : E \rightarrow \mathbb{P}^1$ egy 1 fokú leképezés két sima görbe között, így a 3.3.1 Következmeny alapján $E \cong \mathbb{P}^1$, ami viszont ellent mond annak, hogy E génusza 1, $\mathbb{P}^1$ -é viszont 0 az 5.4 Állítás alapján. (A génusz izomorfizmus-invariáns, hiszen ha két görbe között van egy izomorfizmus, akkor az a divizorcsoportok között is indukál egy izomorfizmust, az 5.1 Tétel alapján pedig a génuszt a divizorcsoportok alapján származtatjuk).

Tehát C sima és innen pedig már azt is kapjuk, hogy ϕ izomorfizmus. $\square$

6.2 Csoportstruktúra az elliptikus görbéken

6.4 Definíció. L_{AB} -vel jelöljük az A, B pontokon átmenő egyenest, ami $A = B$ esetén az A -beli érintő.

Gyakran lesz szükségünk $A, B \in E$ esetén $L_{AB} \cap E$ harmadik metszéspontjára, így erre bevezetjük az $L_{AB} \cap^3 E$ jelölést. (A metszéspontokat multiplicitással számoljuk, így $L_{AB} \cap^3 E \in \{A, B\}$, illetve $A = B$ esetén $L_{AB} \cap^3 E = A$ előfordulhat.)

6.4.1 Megjegyzés. A Bézout-tétel (ld. [4] Shafarevich: Basic Algebraic Geometry 1, Ch. 3, §2.2) alapján, ha L egy egyenes, akkor $\#(L \cap E) = 3$ multiplicitással számolva.

6.5 Definíció. Legyen $E \subseteq \mathbb{P}^2$ egy Weierstrass-egyenlettel megadott görbe, $O = [0, 1, 0]$ a kijelölt pontja (ún. bázispontja). E -n megadunk egy $(E, \oplus)$ csoport struktúrát: $P, Q \in E$, és legyen $R := L_{PQ} \cap^3 E$. Ekkor $P \oplus Q$ -t $L_{RO} \cap^3 E$ -ként definiáljuk.

6.1 Lemma. Ha L egy egyenes és $L \cap E = \{A, B, C\}$ nem feltétlen különböző pontok, akkor $(A \oplus B) \oplus C = O$.

Bizonyítás. $L_{AB} \cap^3 E = C$, mivel $L \cap E = \{A, B, C\}$. Így $A \oplus B = L_{CO} \cap^3 E$.

$L_{(A \oplus B)C} \cap^3 E = O$, mivel az előzőek alapján $L_{CO} \cap E = \{C, O, A \oplus B\}$. Így $(A \oplus B) \oplus C = L_{OO} \cap^3 E = O$, mivel az O -beli érintő 3 multiplicitással metszi E -t. Ugyamis, ha egy $S \neq O$ pontban metszené, akkor, mivel O ideális pont, az O -beli érintő szükségszerűen az ideális egyenes, azaz ekkor S -nek is ideális pontnak kellene lennie, de korábban már láttuk, hogy a Weierstrass-egyenlet egyetlen ideális megoldása az O pont. $\square$

6.3 Állítás. $(E, \oplus)$ valóban (Abel-)csoport: $P, Q, R \in E$ tetszőleges, nem feltétlen különböző pontok.

1, $P \oplus O = P$

2, $P \oplus Q = Q \oplus P$

3, Létezik $\ominus P \in E$, hogy $P \oplus (\ominus P) = O$.

4, $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$

Bizonyítás. 1, $L_{PO} \cap^3 E =: S$, $P \oplus O = L_{SO} \cap^3 E = P$, hiszen $L_{PO} \cap E = \{P, O, S\}$.

2, $L_{PQ} \cap^3 E =: S$, $P \oplus Q = L_{SO} \cap^3 E = Q \oplus P$, hiszen $L_{PQ} = L_{QP}$.

3, Az előző lemma alapján könnyen látszik, hogy $L_{PO} \cap^3 E =: S$ esetén S jó lesz $\ominus P$ -nek hiszen ekkor $O = (P \oplus O) \oplus S = P \oplus S$.

4, A 6.5 Állítás 5, részéből azonnal következni fog. $\square$

6.6 Definíció. Legyen $P \in E$, $m \in \mathbb{Z}$ ekkor $[m]P := \bigoplus^m P$ $m > 0$ -ra, $[m]P := [-m](\ominus P)$ $m < 0$ -ra, és $[0]P := O$.

Mostantól, ha egyértelmű, elhagyjuk az $\oplus, \ominus$ jeleket és egyszerűen a $+$, $-$ jelölést használjuk helyettük.

6.4 Állítás. Legyen E az $F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ Weierstrass-egyenlettel megadott elliptikus görbe. Ekkor

1, Ha $P_0 = (x_0, y_0) \in E$, akkor $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.

2, $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3) \in E$ úgy, hogy $P_1 + P_2 = P_3$.

i, Ha $x_1 = x_2$ és $y_1 + y_2 + a_1x_2 + a_3 = 0$, akkor $P_3 = O$.

ii, Ha $x_1 \neq x_2$, akkor legyen $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ és $v = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$

Ha $x_1 = x_2$, akkor pedig legyen $\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$ és $v = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$.

Ekkor $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$, és $y_3 = -(\lambda + a_1)x_3 - v - a_3$.

Bizonyítás. 1, Ahogyan az előző állításban láttuk, $-P_0$ -at L_{P_0O} E -vel vett harmadik metszéspontja adja, ez alapján fogjuk tudni a koordinátákat is kiszámolni: $L_{P_0O} : x - x_0$, ezt $F(x, y)$ -ba helyettesítve egy y -ban 2.-fokú egyenletet kapunk: $F(x_0, y) = y^2 + a_1x_0y + a_3y - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 = 0$
 Ennek az egyik megoldása nyilván y_0 , a másik, y'_0 , pedig $-P_0$ második koordinátája lesz (tudjuk, hogy az egyenes $P_0, O, -P_0$ pontokban metszi E -t és az inhomogén egyenlet $O = \infty$ -t "nem látja", így ennek az egyenletnek a megoldásai P_0 és $-P_0$). A gyökök összegére vonatkozó Viéte-formulák szerint $y'_0 = -y_0 - a_1x_0 - a_3$.

2, Az összeadásra vonatkozó formulát is az összegzési szabály egyenletrendszerre alakításából nyerjük:

i , Ha $x_1 = x_2$ és $y_1 + y_2 + a_1x_2 + a_+ = 0$, akkor a $-P_0$ -ra vonatkozó formulából világos, hogy $P_1 + P_2 = O$

ii , Különben $L_{P_1P_2} : y = \lambda x + v$ alakú, ahol $\lambda, v \in \overline{K}$ az állításban leírt értékek. Ezt $F(x, y)$ -ba írva $F(x, \lambda x + v) = (\lambda x + v)^2 + a_1x(\lambda x + v) + a_3(\lambda x + v) - x^3 - a_2x^2 - a_4x - a_6$ x -ben 3.-fokú polinomot kapunk, melynek két gyöke persze x_1 és x_2 , a harmadik pedig $-P_3$ első koordinátája lesz (az előző állításban láttuk, hogy ha S a harmadik metszéspont, akkor $P_1 + P_2 + S = O$, azaz $P_1 + P_2 = -S$, tehát $S = -P_3$). Ismét a gyökök összegére vonatkozó Viéte formulák szerint, illetve az előbb $-P_0$ -ra levezetett formula alapján

$$x_3 = \lambda^2 + \lambda a_1 - a_2 - x_1 - x_2 \text{ és}$$

$$-y_3 - a_1x_3 - a_3 = \lambda x_3 + v, \text{ azaz } y_3 = -(\lambda + a_1)x_3 - v - a_3. \quad \square$$

6.3 Elliptikus görbék divizor csoportja

Azt fogjuk megmutatni, hogy egy E elliptikus görbe izomorf a $\text{Pic}^0(E) = \text{Div}^0(E)/\sim$ -vel, mégpedig csoportstruktúra-tartó módon.

6.2 Lemma. Legyen C egy 1 génuszú görbe, $P, Q \in C$. Ekkor $(P) \sim (Q)$ pontosan akkor, ha $P = Q$

Bizonyítás. Ha $(P) \sim (Q)$, akkor létezik egy $f \in \overline{K}(C)$ úgy, hogy $\text{div}(f) = (P) - (Q)$. Ekkor $f \in \mathcal{L}((Q))$, így az 5.1.1 Következmény alapján $\dim_{\overline{K}} \mathcal{L}((Q)) = \ell((Q)) = \deg(Q) - g + 1 = 1 - 1 + 1 = 1$. Másfelől, ha g egy nem 0 konstans függvény $\overline{K}(C)$ -ben, akkor $\text{ord}_P(g) = 0$ minden $P \in C$ -re, azaz $g \in \mathcal{L}((Q))$. Így $\overline{K} \subseteq \mathcal{L}(D)$.

Ezek alapján $\overline{K} = \mathcal{L}(D)$. Így $0 = \text{div}(f) = (P) - (Q)$, ami csakis úgy lehetséges, ha $P = Q$.

A visszafele irány triviális. $\square$

6.5 Állítás. Legyen (E, O) egy elliptikus görbe. Ekkor

1, minden $D \in \text{Div}^0(E)$ -hez létezik egyértelműen egy $P \in E$, hogy $D \sim (P) - (O)$.

Legyen $\sigma : \text{Div}^0(E) \rightarrow E$ az a leképezés, ami minden D -hez ezt a P pontot rendeli.

2, $\sigma : \text{Div}^0(E) \rightarrow E$ szürjektív leképezés.

3, ha $D_1, D_2 \in \text{Div}^0(E)$, akkor $\sigma(D_1) = \sigma(D_2)$ pontosan akkor, ha $D_1 \sim D_2$.

Azaz σ indukál egy $\hat{\sigma} : \text{Pic}^0(E) \rightarrow E$ bijekciót.

4, $\hat{\sigma}$ inverze $\kappa : E \rightarrow \text{Pic}^0(E)$, $P \mapsto [(P) - (O)]$.

5, ha E -t egy Weierstrass-egyenlőtlenség adja meg, akkor a már bevezetett $(E, \oplus)$ csoportstruktúra megegyezik a $\hat{\sigma}$ által $\text{Pic}^0(E)$ -ből átörökölt csoportstruktúrával.

Bizonyítás. 1, E 1 génuszú, így az 5.1.1 Következmény miatt $\ell(D + (O)) = \deg(D + (O)) - g + 1 = \deg D + \deg(O) - g + 1 = 0 + 1 - 1 + 1 = 1$.

Legyen $f \in \overline{K}(E) \setminus \mathcal{L}(D + (O))$ egy generátora. Így nyilván $\text{div}(f) \geq -D - (O)$, másrészt a 4.2 Állítás miatt $\deg \text{div}(f) = 0$, és $\deg(-D - (O)) = -1$, így ez csakis úgy lehetséges, hogy van egy olyan $P \in E$, hogy $\text{div}(f) = -D - (O) + (P)$.

Az is világos, hogy ez a P egyértelmű, ugyanis ha $P, P' \in E$ olyan, hogy $-D - (O) + (P) = \text{div}(f) = -D - (O) + (P')$, akkor $(P) = D + (O) + \text{div}(f) = (P')$, azaz $(P) \sim D + (O) \sim (P')$. Az előző lemma miatt ekkor $P = P'$.

2, Legyen $P \in E$ tetszőleges. $\sigma((P) - (O)) = P$, hiszen $-((P) - (O)) - (O) + (P) = 0$.

3, $P_1 := \sigma(D_1)$, $P_2 := \sigma(D_2)$. Ekkor σ definíciója alapján $D_1 \sim (P_1) - (O)$, és $D_2 \sim (P_2) - (O)$, azaz $D_1 - D_2 \sim (P_1) - (O) - (P_2) + (O) = (P_1) - (P_2)$.

Ha $P_1 = P_2$, akkor $D_1 \sim D_2$ (hiszen létezik $f \in \overline{K}(E)$ úgy, hogy $D_1 - D_2 = \text{div}(f) + 0$, vagyis $D_1 = D_2 + \text{div}(f)$).

Ha pedig $D_1 \sim D_2$, akkor $(P_1) \sim (P_2)$ (hiszen létezik $f, g \in \overline{K}(E)$ úgy, hogy $D_1 = D_2 + \text{div}(f)$ és $D_1 - D_2 = (P_1) - (P_2) + \text{div}(g)$, így $(P_2) = -(D_1 - D_2) + (P_1) + \text{div}(g) = (P_1) - \text{div}(f) + \text{div}(g) = (P_1) + \text{div}(g/f)$), azaz az előző lemma alapján $P_1 = P_2$.

Tehát $\sigma(D_1) = \sigma(D_2)$ pontosan akkor, ha $D_1 \sim D_2$, azaz $\hat{\sigma}$ injektív, és σ szürjektivitása miatt szürjektív is, tehát bijektív.

4, Az előzőekből triviális.

5, Legyen $P, Q \in E$. Azt szeretnénk tehát belátni, hogy $P \oplus Q = \hat{\sigma}(\kappa(P) + \kappa(Q))$, mindkét oldalra alkalmazva κ -t az ezzel ekvivalens állítás, hogy $\kappa(P \oplus Q) = \kappa(P) + \kappa(Q)$.

$L_{PQ} : f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$ a P, Q -n átmenő egyenes egyenlete $\mathbb{P}^2$ -ben. Legyen $S = L_{PQ} \cap^3 E$, ekkor $L_{SO} : \tilde{f}(X, Y, Z) = \alpha' X + \beta' Y + \gamma' Z = 0$ pedig az S, O -n átmenő egyenes egyenlete $\mathbb{P}^2$ -ben.

$\text{div}(f/Z) = \text{div}(f) - \text{div}(Z) = (P) + (Q) + (S) - 3(O)$, mivel $Z = 0$ -nak O -ban 3 a multiplicitása a 2.1.1 Példa alapján.

$\text{div}(\tilde{f}/Z) = \text{div}(\tilde{f}) - \text{div}(Z) = (S) + (P \oplus Q) + (O) - 3(O)$.

A két egyenletet kivonva egymásból $(P \oplus Q) + (O) - (P) - (Q) = \text{div}(\tilde{f}/f) \sim 0$, átrendezve $(P \oplus Q) -$

$(O) - ((P) - (O)) - ((Q) - (O)) \sim 0$, vagyis $\kappa(P \oplus Q) - \kappa(P) - \kappa(Q) = 0$. $\square$

6.6 Állítás. Legyen (E, O) elliptikus görbe, $D = \sum_{P \in E} n_P(P) \in \text{Div}(E)$. Ekkor D fődivizor pontosan akkor, ha $\deg D = 0$ és $\bigoplus_{P \in E} [n_P]P = O$.

Bizonyítás. A 6.4 Állításban leírtak alapján $D \sim 0$ pontosan akkor, ha $O = \sigma(D) = \sigma(D - \deg D(O)) = \sigma(\sum_{P \in E} n_P[(P) - (O)]) = \bigoplus_{P \in E} [n_P]\sigma((P) - (O)) = \bigoplus_{P \in E} [n_P]P$.
Másképp a 4.2 Állítás alapján ha D fődivizor, akkor $\deg D = 0$. $\square$

7 Az izogéniák

Ahogy láttuk, az elliptikus görbénél fontos szerepet játszik a kitüntetett bázispont. Ezért olyan morfizmusokat érdemes vizsgálni az elliptikus görbék között, amelyek bázispontot bázispontba visznek.

7.1 Definíció. Legyen $(E_1, O), (E_2, O)$ két elliptikus görbe. A $\phi : E_1 \rightarrow E_2$ morfizmus **izogénia**, ha $\phi(O) = O$.

7.1.1 Megjegyzés. A 3.2 Állítás alapján egy $\phi : E_1 \rightarrow E_2$ izogéniára vagy $\phi(E_1) = \{O\}$ vagy $\phi(E_1) = E_2$. Az előbbi esetet null-izogéniának nevezzük és $[0]$ -val jelöljük.

7.1.2 Megjegyzés. A nem konstans izogéniák véges leképezések.

7.2 Definíció. Ha $\phi : E_1 \rightarrow E_2$ egy nem konstans izogénia, akkor indukál egy $\phi^* : \overline{K}(E_2) \rightarrow \overline{K}(E_1)$ injekciót a korábban már megadott módon.

7.3 Definíció. A ϕ nem konstans izogénia **fokát, szeparábilis-, inszeparábilis fokát** ($\deg, \deg_s, \deg_i$), illetve **szeparábilisát, inszeparábilisát, tisztán szeparábilisát** is hasonlóan a $\overline{K}(E_1) | \phi^* \overline{K}(E_2)$ megfelelő jellemzője adja.

A $\deg[0]$ -t 0-nak definiáljuk.

7.1 Az izogéniák és az elliptikus görbe csoportstruktúrája

Látni fogjuk, hogy az izogéniák a csoportstruktúrát megőrzik illetve a később sokat használt állítást, ami szerint a "szorzás leképezés" morfizmus.

7.4 Definíció. Legyen $E|K$ egy elliptikus görbe és $Q \in E$. Ekkor a Q -val való eltolás leképezése $\tau_Q : E \rightarrow E, P \mapsto P + Q$.

7.4.1 Megjegyzés. τ_Q izomorfizmus, hiszen τ_{-Q} inverze lesz.

τ_Q persze nem izogénia, ha $Q \neq O$.

7.1 Állítás. Legyen $\psi : E_1 \rightarrow E_2$ egy morfizmus. Ekkor $\tau_{-\psi(O)} \circ \psi$ egy $E_1 \rightarrow E_2$ izogénia.

Bizonyítás. $(\tau_{-\psi(O)} \circ \psi)(O) = \tau_{-\psi(O)}(\psi(O)) = O$. □

7.1.1 Következmény. Ezek szerint minden morfizmus előáll egy izogénia és egy eltolás kompozíciójaként.

7.2 Állítás. Legyen E_1, E_2 két elliptikus görbe, $\phi : E_1 \rightarrow E_2$ izogénia közöttük. Ekkor ϕ homomorfizmus a csoportstruktúráik között, azaz $\phi(P + Q) = \phi(P) + \phi(Q)$ minden $P, Q \in E_1$ esetén.

Bizonyítás. Ha ϕ a konstans izogénia ($\phi(P) = O$ minden P -re), akkor az állítás triviális.

Különben ϕ egy véges leképezés, ami indukál egy $\phi_* : \text{Pic}^0(E_1) \rightarrow \text{Pic}^0(E_2)$ homomorfizmust: $[\sum_{P \in E_1} n_P(P)] \mapsto [\sum_{P \in E_1} n_P(\phi(P))]$.

Másrészt tekintsük a 6.4 Állításból kapott $\kappa_i : E_i \rightarrow \text{Pic}^0(E_i)$, $P \mapsto [(P) - (O)]$ $i = 1, 2$ izomorfizmusokat.

Tehát az alábbi kommutatív diagramot kapjuk:

$$\begin{array}{ccc} E_1 & \xrightarrow{\kappa_1} & \text{Pic}^0(E_1) \\ \phi \downarrow & & \downarrow \phi_* \\ E_2 & \xrightarrow{\kappa_2} & \text{Pic}^0(E_2) \end{array}$$

$\kappa_1, \kappa_2, \phi_*$ csoporthomomorfizmusok és κ_2 injektív, így ϕ is csoporthomomorfizmus lesz: $\kappa_2(\phi(P+Q)) = \phi_*(\kappa_1(P+Q)) = \phi_*(\kappa_1(P)) + \phi_*(\kappa_1(Q)) = \kappa_2(\phi(P)) + \kappa_2(\phi(Q)) = \kappa_2(\phi(P) + \phi(Q))$, ami κ_2 injektivitása miatt ekvivalens azzal, hogy $\phi(P + Q) = \phi(P) + \phi(Q)$. □

7.2.1 Megjegyzés. $\phi_*, \kappa : E \rightarrow \text{Pic}^0(E)$ tényleg homomorfizmusok:

$$\begin{aligned} 1, \phi_*([\sum_{P \in E_1} n_P(P)] + [\sum_{P \in E_1} n'_P(P)]) &= \phi_*([\sum_{P \in E_1} (n_P + n'_P)(P)]) = [\sum_{P \in E_1} (n_P + n'_P)(\phi(P))] = [\sum_{P \in E_1} n_P(\phi(P)) + \\ &+ [\sum_{P \in E_1} n'_P(\phi(P))] = \phi_*[\sum_{P \in E_1} n_P(P)] + \phi_*[\sum_{P \in E_1} n'_P(P)] \end{aligned}$$

2, Az, hogy κ homomorfizmus, éppen a 6.5 Állítás 5. része.

7.2.1 Következmény. Ha E_1, E_2 elliptikus görbék, akkor Abel-csoportként tekintve rájuk $\{\phi \mid \phi : E_1 \rightarrow E_2 \text{ izogénia}\} = \text{Hom}(E_1, E_2)$, ami szintén Abel-csoport $(\phi + \psi)(P) := \phi(P) + \psi(P)$ csoportművelettel.

Továbbá $E_1 = E_2 = E$ esetén $\text{Hom}(E, E) = \text{End}(E)$ gyűrű is a kompozícióval, mint szorzással. Ez valóban disztributív az összeadásra nézve az előző állítás miatt: $((\phi + \psi) \circ \lambda)(P) = (\phi + \psi)(\lambda(P)) = (\phi \circ \lambda)(P) + (\psi \circ \lambda)(P) = (\phi \circ \lambda + \psi \circ \lambda)(P)$, és $(\lambda \circ (\phi + \psi))(P) = \lambda(\phi(P) + \psi(P)) = (\lambda \circ \phi)(P) + (\lambda \circ \psi)(P) = (\lambda \circ \phi + \lambda \circ \psi)(P)$.

7.3 Állítás. $+: E \times E \rightarrow E$, $(P_1, P_2) \mapsto P_1 + P_2$,

$- : E \rightarrow E$, $P \mapsto -P$ morfizmusok.

Bizonyítás. A $-$ leképezés $(x, y) \mapsto (x, -y - a_1x - a_3)$ alakú, azaz racionális. Tudjuk, hogy E sima, így a 3.1 Állítás miatt morfizmus is.

A $+$ leképezéshez, először rögzítsünk le egy $O \neq Q \in E$ pontot és tekintsük a τ_Q eltolást. A 6.3 Állítás 2, részében megadott formulák alapján ez is egy racionális leképezés, és hasonlóan E simasága miatt így morfizmus. Sőt, izomorfizmus is, hiszen van inverze: τ_{-Q} .

A 6.3 Állítás formulái alapján látható, hogy $+: E \times E \rightarrow E$ a $(P, P), (P - P), (O, P), (P, O)$ morfizmus (ugyanis ezek kivételével λ és v biztosan értelmesek).

A kivételek esetén legyen $Q_1, Q_2 \in E$ tetszőleges és legyen $\phi: E \times E \xrightarrow{\tau_{Q_1} \times \tau_{Q_2}} E \times E \xrightarrow{+} E \xrightarrow{\tau_{Q_1}^{-1}} E \xrightarrow{\tau_{Q_2}^{-1}} E$. $+$ asszociativitása és kommutativitása miatt ϕ a következőt csinálja: $(P_1, P_2) \mapsto (P_1 + Q_1, P_2 + Q_2) \mapsto P_1 + Q_1 + P_2 + Q_2 \mapsto P_1 + P_2 + Q_2 \mapsto P_1 + P_2$, tehát $\phi = +$ azokban a pontokban, ahol mindkettő értelmes. τ_{Q_1}, τ_{Q_2} izomorfizmusok, így az előbbi gondolatmenetet használva ϕ morfizmus, kivéve esetleg $(P - Q_1, P - Q_2), (P - Q_1, -P - Q_2), (P - Q_1, -Q_2), (-Q_1, P - Q_2)$. Mivel azonban Q_1, Q_2 tetszőleges, így találhatunk $\phi_1, \dots, \phi_n: E \times E \rightarrow E$ leképezéseket, amelyekre $\phi_i = +$ azokban a pontokban, ahol értelmesek, valamint minden $(P_1, P_2) \in E \times E$ -re van olyan i , hogy ϕ_i értelmes (P_1, P_2) -ben. $\square$

7.5 Definíció. $[m]: E \rightarrow E, P \mapsto [m]P$ az m -mel való "szorzás leképezés".

7.5.1 Megjegyzés. $[m]$ izogénia (a 7.3 állítás többszöri alkalmazásából adódik, hogy morfizmus, és persze $[m]O = O$).

7.5.2 Megjegyzés. Ha ϕ egy izogénia, akkor $[m] \circ \phi = \phi \circ [m]$, ugyanis a 7.2 Állítás miatt $[m](\phi(P)) = \bigoplus_{i=1}^m \phi(P) = \phi(\bigoplus_{i=1}^m P) = \phi([m](P))$.

7.2 Kapcsolat az izogéniák tulajdonságai és a görbék algebrai struktúrája között

Ebben az alfejezetben három fontos állítást látunk be arról, hogy az izogéniák tulajdonságaiból milyen információt nyerhetünk az elliptikus görbék struktúrájáról.

7.5.3 Megjegyzés. A következő állításban a Galois-bővítés azon definícióját fogjuk használni, hogy $E|F$ Galois bővítés, ha $\text{Fix}[\text{Aut}(E|F)] = F$.

Ezzel ekvivalens, hogy $\#\text{Aut}(E|F) = [E : F]$ (ha $\text{Fix}[\text{Aut}(E|F)] = F$, akkor $[E : F] = \#\text{Gal}(E|F) = \#\text{Aut}(E|F)$, másrészt ha $\#\text{Aut}(E|F) = [E : F] = \#\text{Gal}(E|F) \leq \#\text{Aut}(E|F)$, mivel $\text{Gal}(E|F) < \text{Aut}(E|F)$, így $\text{Gal}(E|F) = \text{Aut}(E|F)$, $\text{Fix}[\text{Aut}(E|F)] = F$).

7.4 Állítás. Legyen E_1, E_2 két elliptikus görbe, $\phi: E_1 \rightarrow E_2$ nem konstans izogénia közöttük. Ekkor 1, minden $Q \in E_2$ -re $\#\phi^{-1}(Q) = \deg_s \phi$ és minden $P \in E_1$ -re $e_\phi(P) = \deg_i \phi$.

2, $\ker \phi \rightarrow \text{Aut}[\overline{K}(E_1)|\phi^*\overline{K}(E_2)]$, $P \mapsto \tau_P^*$ izomorfizmus.

3, ha ϕ szeparábilis, akkor nem elágazó, $\# \ker \phi = \deg \phi$ és $\overline{K}(E_1)$ Galois bővítése $\phi^*\overline{K}(E_2)$ -nek.

Bizonyítás. 1, A 3.4 állítás 2, része alapján már tudjuk, hogy $\#\phi^{-1}(Q) = \deg_s \phi$ véges sok Q kivételével.

Tetszőleges $Q, Q' \in E_2$ esetén legyen $R \in E_1$ olyan, hogy $\phi(R) = Q - Q'$. Mivel ϕ homomorfizmus, így $\phi^{-1}(Q) \rightarrow \phi^{-1}(Q')$, $P \mapsto R + P$ egy bijekció. Tehát $\#\phi^{-1}(Q) = \#\phi^{-1}(Q')$.

Legyen $P, P' \in E_1$ olyan, hogy $\phi(P) = \phi(P') = Q$ és legyen $R := P - P'$. Ekkor $\phi(R) = O$, vagyis $\phi \circ \tau_R = \phi$ ($\phi(Q) = \phi(Q) + \phi(R) = \phi(Q + R) = (\phi \circ \tau_R)(Q)$ minden $Q \in E_1$ -re).

A 3.4 Állítás 3, része miatt $e_\phi(P) = e_{\phi \circ \tau_R}(P) = e_\phi(\tau_R(P))e_{\tau_R}(P) = e_\phi(P')$ (mivel τ_R izomorfizmus, $e_{\tau_R}(S) = \text{ord}_S(\tau_R^*t_{\tau_R}(S)) = \text{ord}_{S+R}(t_{\tau_R}(S)) = \text{ord}_{S+R}(t_{S+R}) = 1$). Tehát $\phi^{-1}(Q)$ minden elemének azonos a elágazási indexe. Így a 3.4 Állítás 1, része alapján $\deg_s \phi \deg_i \phi = \deg \phi = \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = (\#\phi^{-1}(Q))e_\phi(P) \deg_s \phi \cdot e_\phi(P)$, $\deg_s \phi$ -vel leosztva $\deg_i \phi = e_\phi(P)$.

2, Legyen $P \in \ker \phi$, $f \in \overline{K}(E_2)$. Ahogy az előző részben is láttuk, $\phi = \phi \circ \tau_P$, így $\phi^*f = (\phi \circ \tau_P)^*f = \tau_P^*(\phi^*f)$, tehát τ_P^* valóban fixen hagyja $\phi^*\overline{K}(E_2)$ -t, vagyis $\tau_P^* \in \text{Aut}[\overline{K}(E_1)|\overline{K}(E_2)]$.

$\tau_P \circ \tau_P' = \tau_{P+P'} = \tau_P' \circ \tau_P$, $\tau_O = \text{id}$ tehát a leképezés homomorfizmus.

Az 1, részből $\#\ker \phi = \deg_s \phi$. Azt is tudjuk a 3.6.4 Megjegyzésből ($N = F = \overline{K}(E_1)$, $K = \phi^*\overline{K}(E_2)$ választással), hogy $\#\text{Aut}[\overline{K}(E_1)|\phi^*\overline{K}(E_2)] \leq \deg_s \phi = \#\ker \phi$.

Így az izomorfizmushoz elég belátni az injektivitást. Ha $\tau_P^* = \text{id}_{\overline{K}(E_1)}$, akkor $f(O) = (\tau_P^*f)(O) = f(P + O) = f(P)$ minden $f \in \overline{K}(E_1)$ -re, azaz speciálisan $f = \text{id}$ esetén $P = O$.

3, Mivel ϕ szeparábilis, így $\deg \phi = \deg_s \phi$. Így az 1, részből minden $Q \in E_2$ -re $\#\phi^{-1}(Q) = \deg_s \phi$, így a 3.5 Állítás alapján ez azt jelenti, hogy ϕ unramified.

$Q = O$ választással $\#\ker \phi = \#\phi^{-1}(Q) = \deg_s \phi$. A 2, részből $\#\text{Aut}[\overline{K}(E_1)|\phi^*\overline{K}(E_2)] = \#\ker \phi = \deg \phi = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)]$, így $\overline{K}(E_1)|\phi^*\overline{K}(E_2)$ Galois bővítés. $\square$

7.3 Az invariáns differenciál alkalmazása

Az invariáns differenciál az elliptikus görbe differenciálformáinak kitüntetett eleme, aminek segítségével beláthatjuk a duális morfizmusok linearitását és az abból következő szeparabilitásra vonatkozó feltételt.

7.5 Állítás. Legyen E a $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ Weierstrass-egyenlettel megadott elliptikus görbe, $\omega \in \Omega_E$ pedig a 6.2 Definícióban már megadott invariáns differenciálja. Ekkor minden $Q \in E$ -re $\tau_Q^*\omega = \omega$.

Bizonyítás. Az 5.1 Állítás alapján Ω_E 1-dimenziós vektortér $\overline{K}(E)$ felett, így létezik $a_Q \in \overline{K}(E) - \{0\}$ úgy, hogy $\tau_Q^*\omega = a_Q\omega$ ($q_Q \neq 0$, mivel τ_Q izomorfizmus).

Ekkor a 4.1 Állítás 2, részét használva $\text{div}(a_Q) = \text{div}(\tau_Q^*\omega/\omega) = \text{div}(\tau_Q^*\omega) - \text{div}(\omega) = \tau_Q^*\text{div}(\omega) -$

$\text{div}(\omega) = 0$ a 6.1 Állítás alapján. Így $a_Q \in \overline{K}(E)$ -nak nincs pólusa, se gyöke, vagyis a 2.3 Állítás miatt konstans, $a_Q \in \overline{K} - \{0\}$.

Legyen $\phi : E \rightarrow \mathbb{P}^1$, $Q \mapsto [a_Q, 1]$. a_Q kifejezhető $x(Q), y(Q)$ racionális függvényeként, ugyanis a 6.3 Állításban bebizonyított formula szerint tetszőleges $P \in E$ -re $x(P+Q)$ -t és $y(P+Q)$ -t ki tudjuk fejezni $x(P), y(P), x(Q), y(Q)$ -val, majd Q -t lefixálva $(x(Q), y(Q))$ -t konstansként kezelve $dx(P+Q)$ -t $dx(P)g_1, dy(P+Q)$ -t $dy(P)g_2$ alakba írhatjuk, ahol g_1, g_2 racionális függvények, azaz $a_Q = \tau_Q^* \omega / \omega(x(Q), y(Q))$ racionális függvényeként felírható.

Tehát ϕ egy racionális leképezés, ami nem szürjektív (pl. a ∞ -t nem veszi fel), így a 3.1 és 3.2 Állítások alapján ϕ -mek konstansnak kell lennie, így $a_Q = a_O = 1$ minden $Q \in E$ -re. $\square$

7.5.4 Megjegyzés. Tehát ω eltolás-invariáns, innen a neve: invariáns differenciál.

7.6 Állítás. Legyen E, E' két elliptikus görbe, ω E invariáns differenciálja, $\phi, \psi : E' \rightarrow E$ pedig két izogénia. Ekkor $(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$.

Bizonyítás. Ha $\phi = [0]$ vagy $\psi = [0]$, akkor triviálisan igaz az állítás ($\omega(O) = 0$).

Ha $\phi + \psi = [0]$, akkor $\psi^* = (-\phi)^* = \phi^* \circ [-1]^*$ miatt elég azt belátni, hogy $[-1]^* \omega = -\omega$. $[-1](x, y) = (x, -y - a_1x - a_3)$ a 6.3 Állítás alapján. Így, $[-1]^* \omega = [-1]^* \left(\frac{dx}{2y + a_1x + a_3} \right) = \frac{dx}{2(-y - a_1x - a_3) + a_1x + a_3} = \frac{-dx}{2y + a_1x + a_3} = -\omega$.

Mostantól tehát feltehető, hogy $\phi, \psi, \phi + \psi \neq [0]$:

Legyen $(x_1, y_1), (x_2, y_2)$ független Weierstrass-koordináták, azaz kielégítik a Weierstrass-egyenletet, és más algebrai reláció nem áll fenn közöttük (vagyis $([x_1, y_1, 1], [x_2, y_2, 1]) \in E \times E \subseteq \mathbb{P}^2 \times \mathbb{P}^2$ -et koordinátázza).

Legyen $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$, így, ahogyan az előző állítás bizonyításában is láttuk, x_1, y_1, x_2, y_2 racionális kombinációiként kifejezhető x_3, y_3 . $\omega(x, y)$ -nak $\frac{dx}{2y + a_1x + a_3}$ alakját fogjuk használni. Ezek alapján tehát $\omega(x_3, y_3) = f(x_1, y_1, x_2, y_2)\omega(x_1, y_1) + g(x_1, y_1, x_2, y_2)\omega(x_2, y_2)$, ahol f, g racionális függvények.

Továbbá, mivel $i = 1, 2$ -re $y_i^2 + a_1x_iy_i + a_3y_i = x_i^3 + a_2x_i^2 + a_4x_i + a_6$, így

$$d(y_i^2 + a_1x_iy_i + a_3y_i) = d(x_i^3 + a_2x_i^2 + a_4x_i + a_6), \text{ azaz}$$

$$2y_i dy_i + a_1x_i dy_i + a_1y_i dx_i + a_3 dy_i = 3x_i^2 dx_i + 2a_2x_i dx_i + a_4 dx_i, \text{ azaz}$$

$(2y_i + a_1x_i + a_3)dx_i = (3x_i^2 + 2a_2x_i + a_4 - a_1y_i)dx_i$. Ezzel együtt azt kapjuk, hogy $\omega(x_3, y_3)$ kifejezhető dx_1, dx_2 $\overline{K}(x_1, y_1, x_2, y_2)$ -lineáris kombinációjaként.

Következő lépésként megmutatjuk, hogy $f, g \equiv 1$: Fixáljuk le x_2, y_2 -t, azaz valamilyen $Q \in E$ -re $x_2 = x(Q), y_2 = y(Q)$. Ekkor persze $dx_2 = 0$, így $\omega(x_2, y_2) = 0$ is. A 7.5 állításból pedig $\omega(x_3, y_3) = \tau_Q^* \omega(x_1, y_1) = \omega(x_1, y_1)$, így $\omega(x_1, y_1) = \omega(x_3, y_3) = f(x_1, y_1, x(Q), y(Q))\omega(x_1, y_1) + g(x_1, y_1, x(Q), y(Q))\omega(x_2, y_2) = f(x_1, y_1, x(Q), y(Q))\omega(x_1, y_1)$. Tehát $f(x_1, y_1, x(Q), y(Q)) \equiv 1$ mint $\overline{K}(x_1, y_1)$ -beli függvény. Ez azonban minden $Q \in E$ -re igaz, így $f(x_1, y_1, x_2, y_2) \equiv 1$ mint $\overline{K}(x_1, y_1, x_2, y_2)$ -

beli függvény is.

Hasonlóan kapjuk, hogy $g \equiv 1$.

Tehát, ha $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$, akkor $\omega(x_3, y_3) = \omega(x_1, y_1) + \omega(x_2, y_2)$.

Legyen (x', y') Weierstrass-koordináták E' -n és legyen $(x_1, y_1) = \phi(x', y')$, valamint $(x_2, y_2) = \psi(x', y')$.

Ekkor $(x_3, y_3) = (\phi + \psi)(x', y')$, ezt az eddigiekbe írva $\omega \circ (\phi + \psi)(x', y') = (\omega \circ \phi)(x', y') + (\omega \circ \psi)(x', y')$, vagyis $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$. $\square$

7.6.1 Következmény. Legyen E elliptikus görbe, ω pedig az invariáns differenciálja, valamint $m \in \mathbb{Z}$. Ekkor $[m]^*\omega = m\omega$.

Bizonyítás. $m = 0$ -ra triviális, a 7.6 Állítást felhasználva pedig indukcióval láthatjuk be tetszőleges m -re: $[m+1]^*\omega = [m]^*\omega + [1]^*\omega = [m]^*\omega + \omega$ $\square$

7.6.2 Következmény. Legyen $\text{char}(K) = p > 0$, $q = p^r$ legyen $E|\mathbb{F}_q$ elliptikus görbe, $\phi : E \rightarrow E$ a q -adik Frobenius endomorfizmus, végül legyen $m, n \in \mathbb{Z}$. Ekkor $m + n\phi : E \rightarrow E$ szeparábilis pontosan akkor, ha $p \nmid m$. Speciálisan $1 - \phi$ szeparábilis.

Bizonyítás. Legyen ω invariáns differenciál E -n. az 5.2 Állítás miatt $\psi : E \rightarrow E$ inszeparábilis pontosan akkor, ha ψ^* nem injektív, azaz, ha $\psi^*\omega = 0$. (Ω_E 1-dimenziós $\overline{K}(E)$ -vektortér.)

A 7.5 és 7.6 Állítások alapján $(m + n\phi)^*\omega = m\omega + n\phi^*\omega$. $\phi^*\omega = 0$, mivel ϕ tisztán insze parábilis (mivel $K(E)|\phi^*K(E^{(q)}) = K(E)^q$ a 3.6 Állítás 1, része alapján, azaz minden $f \in K(E)$ -re $f^q \in \phi^*K(E^{(q)})$, vagyis a minimálpolinom $(x - f)^q$ osztója). Így $(m + n\phi)^*\omega = m\omega$. $m\omega$ pedig pontosan $p|m$ esetén lesz 0, azaz pontosan ekkor lesz $(m + n\phi)^*$ inszeparábilis. $\square$

7.4 A duális izogénia

A duális izogénia kapcsolatot teremt az izogénia és a fokával való "szorzás leképezés" között.

7.1 Lemma. Legyenek $\phi : E_1 \rightarrow E_2$, $\psi : E_1 \rightarrow E_3$ nem konstans izogéniák, és legyen ϕ szeparábilis. Ha $\ker \phi \subseteq \ker \psi$, akkor létezik $\lambda : E_2 \rightarrow E_3$ izogénia úgy, hogy $\psi = \lambda \circ \phi$.

Bizonyítás. A 7.4 Állítás 3, része miatt $\overline{K}(E_1)$ Galois bővítése $\phi^*\overline{K}(E_2)$ -nek.

Mivel $\ker \phi \subseteq \ker \psi$, így a 7.4 Állítás 2, részében leírt izomorfizmus alapján $\text{Gal}(\overline{K}(E_1)|\phi^*\overline{K}(E_2))$ fixálja $\psi^*\overline{K}(E_3)$ -at $[\text{Gal}(\overline{K}(E_1)|\phi^*\overline{K}(E_2)) \leftarrow \ker \phi \subseteq \ker \psi \rightarrow \text{Gal}(\overline{K}(E_1)|\psi^*\overline{K}(E_3))]$ izomorfizmusok, azaz $\text{Gal}(\overline{K}(E_1)|\phi^*\overline{K}(E_2)) \subseteq \text{Gal}(\overline{K}(E_1)|\psi^*\overline{K}(E_3))$. Emiatt $\psi^*\overline{K}(E_3) \subseteq \phi^*\overline{K}(E_2) \subseteq \overline{K}(E_1)$.

Tehát, kaptunk egy $\iota : \overline{K}(E_3) \rightarrow \overline{K}(E_2)$ injekciót ($\iota := (\phi^*)^{-1} \circ \text{id}_{\phi^*\overline{K}(E_2)} \circ \psi^*$), amire $\psi^* = \phi^* \circ \iota$.

Mivel ez K -t fixen hagyja, így a 3.3 Állítás 2, része alapján létezik egy $\lambda : E_2 \rightarrow E_3$, amire $\lambda^* = \iota$, azaz $\psi^* = \phi^* \circ \lambda^* = (\lambda \circ \phi)^*$, azaz $\psi = \lambda \circ \phi$. λ izogénia, mivel $\lambda(O) = \lambda(\phi(O)) = \psi(O) = O$. $\square$

7.7 Állítás. Legyen $\phi : E_1 \rightarrow E_2$ nem konstans izogénia, $\deg \phi = m$.

1, Létezik egyértelműen egy $\hat{\phi} : E_2 \rightarrow E_1$ izogénia, amire $\hat{\phi} \circ \phi = [m]$.

2, Mint csoporthomomorfizmus, $\hat{\phi}$ a következő kompozícióval egyezik meg: $E_2 \xrightarrow{\psi_1} \text{Div}^0(E_2) \xrightarrow{\phi^*} \text{Div}^0(E_1) \xrightarrow{\psi_2} E_1$, ahol $\psi_1(Q) := (Q) - (O)$ és $\psi_2(\sum_{P \in E_1} n_P P) := \bigoplus_{P \in E_1} [n_P]P$.

Bizonyítás. 1, Egyértelműség: tegyük fel, hogy $\hat{\phi}, \hat{\phi}'$ két ilyen izogénia. Ekkor $(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = [0]$. Mivel ϕ nem konstans, így a 3.2 Állítás alapján szürjektív, vagyis $(\hat{\phi} - \hat{\phi}')$ -nek kell konstansnak lennie, azaz $\hat{\phi} - \hat{\phi}' = O$, $\hat{\phi} = \hat{\phi}'$.

Létezés: tegyük fel, hogy $\psi : E_2 \rightarrow E_1$ egy másik nem konstans izogénia, $\deg \psi = n$ és tegyük fel, hogy $\hat{\psi}, \hat{\phi}$ létezik. Ekkor $(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [m] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [n] \circ [m] = [nm]$. tehát $\hat{\phi} \circ \hat{\psi}$ alkalmas jelölt $\widehat{\psi \circ \phi}$ -re. A 3.7 állítás alapján így elég $\hat{\phi}$ -t megtalálnunk szeperábilis, illetve Frobenius homomorfizmus esetén (ugyanis minden leképezés felbontható ezek kompozíciójára).

1. eset: ϕ szeperábilis.

Ekkor a 7.4 Állítás miatt $m = \deg \phi = \deg_s \phi = \# \ker \phi$, így $\ker \phi \subseteq \ker [m]$ (hiszen $\ker \phi < E_1$ -ben részcsoport, így elemeinek rendje osztja $\# \ker \phi = m$ -et, vagyis $[m]$ -szeresük biztosan 0).

A lemma szerint van egy $\hat{\phi} : E_2 \rightarrow E_1$ leképezés úgy, hogy $\hat{\phi} \circ \phi = [m]$.

2. eset: ϕ a q -adik Frobenius homomorfizmus ($q = p^r$).

Ekkor ϕ -re úgy tekinthetünk, mint a p . Frobenius homomorfizmus r -szer komponálva önmagával. Emiatt az is elég, hogy $\hat{\phi}$ -t a p . frobenius homomorfizmushoz megtaláljuk. (Tehát feltehetjük, hogy $r = 1$.)

$\deg \phi = p$ a 3.6 állítás 2. része szerint.

Legyen ω inavriáns differenciálja E_1 -nek. A 7.6.1 Következmenyből tudjuk, hogy $[p]^* \omega = p\omega = 0$ (mivel $\text{char}(K) = p$). Az 5.2 állítás miatt így $[p]$ inszeperábilis. Így, a 3.7 Állításban leírtak szerint, illetve a 3.6.2 Megjegyzés állítását használva $[p]$ -t felbonthatjuk a $\deg_i [p] = \deg [p] = p^t$. Frobenius homomorfizmus ($\phi_1 = \phi^t$) és egy szeperábilis leképezés (ϕ_2) kompozíciójára: $[p] = \phi_2 \circ \phi^t$, ahol $t \geq 1$, hiszen $[p]$ inszeperábilis. Ekkor $\hat{\phi} = \phi_2 \circ \phi^{t-1}$ jó lesz.

2, Legyen $Q \in E_2$.

$$\text{Ekkor } \psi_2[\phi^*(\psi_1(Q))] = \psi_2[\phi^*((Q) - (O))] = \psi_2\left[\sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) - \sum_{P \in \phi^{-1}(O)} e_\phi(P)(P)\right] = \\ \bigoplus_{P \in \phi^{-1}(Q)} [e_\phi(P)]P \ominus \bigoplus_{R \in \phi^{-1}(O)} [e_\phi(R)]P.$$

A 7.4 Állítás 1. része alapján ez $[\deg_i \phi](\bigoplus_{P \in \phi^{-1}(Q)} P \ominus \bigoplus_{R \in \phi^{-1}(O)} R)$ -rel egyenlő.

$$\text{Rögzítsünk le egy } P_0 \in \phi^{-1}(Q)\text{-t. Ekkor } \bigoplus_{P \in \phi^{-1}(Q)} P = \bigoplus_{P \in \phi^{-1}(Q)} P_0 + (P - P_0) =$$

$$\bigoplus_{P \in \phi^{-1}(Q)} P_0 \oplus \bigoplus_{P \in \phi^{-1}(Q)} (P - P_0) = \bigoplus_{P \in \phi^{-1}(Q)} P_0 \oplus \bigoplus_{R \in \phi^{-1}(O)} R =$$

$$[\# \phi^{-1}(Q)]P_0 \oplus \bigoplus_{R \in \phi^{-1}(O)} R, \text{ vagyis } \bigoplus_{P \in \phi^{-1}(Q)} P \ominus \bigoplus_{R \in \phi^{-1}(O)} R = [\# \phi^{-1}(Q)]P_0.$$

$$\text{Így } [\deg_i \phi](\bigoplus_{P \in \phi^{-1}(Q)} P \ominus \bigoplus_{R \in \phi^{-1}(O)} R) = [\deg_i \phi][\# \phi^{-1}(Q)]P_0 = [\deg_i \phi][\deg_s \phi]P_0 = [\deg \phi]P_0.$$

Mivel $\hat{\phi}(Q) = \hat{\phi} \circ \phi(P_0) = [\deg \phi]P_0$, így $\psi_2 \circ \phi^* \circ \psi_1$. □

7.6 Definíció. $\hat{\phi} : E_2 \rightarrow E_1$ izogéniát $[0] \neq \phi : E_1 \rightarrow E_2$ **duális izogéniájának** nevezzük (konstans izogénia esetén $\widehat{[0]}$ -t $[0]$ -nak értelmezzük).

7.8 Állítás. Legyen $\phi : E_1 \rightarrow E_2$ egy izogénia, $m := \deg \phi$. Ekkor

- 1, $\hat{\phi} \circ \phi = [m]$ E_1 -en, $\phi \circ \hat{\phi} = [m]$ E_2 -n.
- 2, ha $\psi : E_2 \rightarrow E_3$ ($n := \deg \psi$) egy másik izogénia, akkor $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$.
- 3, ha $\lambda : E_1 \rightarrow E_2$ szintén izogénia, akkor $\widehat{\phi + \lambda} = \hat{\phi} + \hat{\lambda}$.

Bizonyítás. Ha ϕ, ψ, λ valamelyike konstans, akkor triviális az állítás, így innentől feltehető, hogy nem konstansok.

1, $\hat{\phi} \circ \phi = [m]$ $\hat{\phi}$ definíciója alapján.

Másrészt $(\phi \circ \hat{\phi}) \circ \phi = \phi \circ (\hat{\phi} \circ \phi) = \phi \circ [m] = [m] \circ \phi$, azaz $((\phi \circ \hat{\phi}) - [m]) \circ \phi = [0]$, és mivel ϕ nem konstans, így $\phi \circ \hat{\phi} - [m]$ -nek kell annak lennie, vagyis $\phi \circ \hat{\phi} = [m]$.

2, $(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [n] \circ [m] = [nm]$. A 7.7 Állítás 1. része alapján az egyértelműség miatt $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$.

3, Legyenek $(x_1, y_1) \in K(E_1)$, $(x_2, y_2) \in K(E_2)$ Weierstrass koordináták. Tekintsünk E_2 -re, mint $K(E_1) = K(x_1, y_1)$ felett definiált elliptikus görbére. Ekkor $\phi(x_1, y_1), \lambda(x_1, y_1), (\phi + \lambda)(x_1, y_1) \in E_2 \cap K(x_1, y_1)$.

Legyen $D = ((\phi + \lambda)(x_1, y_1)) - (\phi(x_1, y_1)) - (\lambda(x_1, y_1)) + (O) \in \text{Div}_{K(x_1, y_1)}^0(E_2)$.

A 6.5 Állítás alapján $D \sim 0$, azaz létezik olyan $f \in K(x_1, y_1)(E_2) = K(x_1, y_1, x_2, y_2)$, amire x_2, y_2 -beli függvényként tekintve $\text{div}(f) = D$.

Most tekintsünk f -re x_1, y_1 -beli függvényként, azaz $K(x_2, y_2)(E_1)$ -beliként. Legyen $P \in E_1 \cap \overline{K(x_2, y_2)}$ olyan, hogy $\phi(P) = (x_2, y_2)$. Ekkor $\sum_P \text{ord}_P f \cdot (P) = \text{div}(f) = D = ((\phi + \lambda)(x_1, y_1)) - (\phi(x_1, y_1)) - (\lambda(x_1, y_1)) + (O)$. A kétféle felírást összehasonlítva, f -nek pólusa van $P = (x_1, y_1)$ -ben, azaz $f(x_1, y_1, x_2, y_2)$ -nek pólusa van, ha $(x_2, y_2) = \phi(x_1, y_1)$. Hasonlóan f -nek pólusa van P -ben, ha $\lambda(P) = (x_2, y_2)$ és gyöke, ha $(\phi + \lambda)(P) = (x_2, y_2)$ ($\phi, \lambda, \phi + \lambda$ nem konstansok, azaz szürjektívek, így minden (x_2, y_2) ponthoz van olyan P , ami rá képződik).

Így, mint x_1, y_1 -beli függvény,

$\text{div}(f) = ((\phi + \lambda)^*(x_2, y_2)) - (\phi^*(x_2, y_2)) - (\lambda^*(x_2, y_2)) + \sum_{P_i \in E_1(\overline{K})} n_i(P_i) =$
 $\sum_{P \in (\phi + \lambda)^{-1}} e_{\phi + \lambda}(P)(P) - \sum_{P \in \phi^{-1}} e_{\phi}(P)(P) - \sum_{P \in \lambda^{-1}} e_{\lambda}(P)(P) + \sum_{P_i \in E_1(\overline{K})} n_i(P_i)$ alakba írható
 $(\sum_{P_i \in E_1(\overline{K})} n_i(P_i) \in \text{Div}_{\overline{K}}(E_1))$. Itt tehát azt írtuk fel, hogy x_2, y_2 -re paraméterként tekintve $P = (x_1, y_1)$ -bne f -nek pontosan akkor van gyöke vagy pólusa, ha az (x_2, y_2) -re képződik ϕ, λ vagy $\phi + \lambda$ szerint. Az utolsó tagot onnan kapjuk, hogy lehetnek $\phi, \lambda, \phi + \lambda$ szerint (O) -ba képződő pontok, amelyek nem függenek x_2, y_2 -től, mivel $O \in E_2(\overline{K})$. Az együtthatók is működni fognak, hiszen az

elágazási index éppen azt mutatja, hogy hányszor képződik $P(x_2, y_2)$ -re, azaz f -nek mint x_1, y_1 -beli függvénynek P hányszoros pólusa (ϕ, λ esetén) / gyöke ($\phi + \lambda$ esetén) .

Mivel ez f divizorja, így $((\phi + \lambda)^*(x_2, y_2)) - (\phi^*(x_2, y_2)) - (\lambda^*(x_2, y_2))$ (x_2, y_2) -től független, vagyis a 7.7 Állítás 2, részében leírt felbontás szerint $\widehat{\phi + \lambda}(x_2, y_2) - \hat{\phi}(x_2, y_2) - \hat{\lambda}(x_2, y_2)$ is független (x_2, y_2) -től, vagyis $E_1(\bar{K})$ -beli.

$(x_2, y_2) = O$ választással ez $\widehat{\phi + \lambda}(O) - \hat{\phi}(O) - \hat{\lambda}(O) = O - O - O = O$, vagyis $\widehat{\phi + \lambda} = \hat{\phi} + \hat{\lambda}$. $\square$

8 Hasse becslése

Hasse becslése egy $\mathbb{F}_q$ feletti elliptikus görbe racionális pontjainak számáról szól. Intuitívan, ha a Weierstrass egyenletben lerögzítjük x -et, amit q féleképpen tehetünk meg, akkor kapunk egy y -ban másodfokú egyenletet, aminek $\sim 1/2$ eséllyel létezik két megoldása, vagyis (még a ∞ pontot nem elfelejtve) azt várhatnánk, hogy $\sim q + 1$ racionális pontja van a görbének.

A tételből kiderül, hogy a heurisztika valójában egészen jó közelítést ad.

8.1 Definíció. Legyen A egy Abel-csoport. Azt mondjuk, hogy $d : A \rightarrow \mathbb{R}$ **kvadratikus forma**, ha

- i. minden $s \in A$ -ra $d(-a) = d(a)$.
- ii. $A \times A \rightarrow \mathbb{R}$, $(a, b) \mapsto d(a + b) - d(a) - d(b)$ bilineáris.

Ezen felül pozitív definit, ha

- iii. minden $a \in A$ -ra $d(a) \geq 0$ és $d(a) = 0$ pontosan akkor, ha $a = 0$.

8.1 Állítás. E_1, E_2 elliptikus görbék. $\deg : \text{hom}(E_1, E_2) \rightarrow \mathbb{Z}$ egy pozitív definit kvadratikus forma.

Bizonyítás. i. $\deg(\phi) = \deg(-\phi)$, mivel $\phi^* \bar{K}(E_2) \cong (-\phi)^* \bar{K}(E_2)$

ii. $\langle \phi, \psi \rangle := \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ bilineáris:

$[] : \mathbb{Z} \rightarrow \text{End}(E_1)$ homomorfizmus injektív (itt $\mathbb{Z}$ a szorzásra nézve csoport), emiatt elég $[] \circ \langle \rangle$ -re belátni a bilinearitást. $[\langle \phi, \psi \rangle] = [\deg(\phi + \psi)] - [\deg \phi] - [\deg \psi] = \widehat{\phi + \psi} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi = (\hat{\phi} + \hat{\psi}) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi = \hat{\phi} \circ \psi + \hat{\psi} \circ \phi$. A 7.8 Állítás 3, része miatt ez lineáris ϕ -ben és ψ -ben is.

iii. $\deg$ definíciója alapján teljesül. $\square$

8.1 Lemma. Cauchy-Schwarz

Ha A Abel-csoport, $d : A \rightarrow \mathbb{R}$ pozitív definit kvadratikus alak. Ekkor tetszőleges $a, b \in A$ -ra $|d(a - b) - d(a) - d(b)| \leq 2\sqrt{d(a)d(b)}$.

Bizonyítás. Legyen $L(a, b) := d(a - b) - d(a) - d(b)$. L bilineáris a kvadratikus alak definíciójának

i., ii. pontja miatt. Mivel d pozitív definit, így minden $m, n \in \mathbb{Z}$ -re $0 \leq d(ma - nb) = m^2 d(a) +$

$mnL(a, b) + n^2d(b)$. Speciálisan, válasszunk $m = -L(a, b)$, $n = 2d(a)$ -t.

Ekkor $0 \leq L(a, b)^2d(a) - 2L(a, b)^2d(a) + 4d(a)^2d(b) = d(a)[L(a, b)^2 - 2L(a, b)^2 + 4d(a)d(b)]$.

Ha $a \neq 0$, akkor $d(a)$ -val leosztva és gyököt vonva a bizonyítandó egyenlőtlenséget kapjuk, $a = 0$ -ra pedig triviálisan teljesül az állítás. $\square$

8.1 Tétel. Legyen $K = \mathbb{F}_q$ ($q = p^r$, p prím), $E|K$ elliptikus görbe. Ekkor $|\#E(K) - q - 1| \leq 2\sqrt{q}$.

Bizonyítás. Tekintsük E -nek egy Weierstrass-egyenletét K -beli együtthatókkal és legyen ϕ a q -adik Frobenius homomorfizmus. Tudjuk, hogy $G_{\bar{K}|K}$ Galois-csoportot ϕ generálja és $P \in E(K)$ pontosan akkor, ha $\phi(P) = P$. Így $E(K) = \ker(\text{id} - \phi)$, és ezzel együtt $\#E(K) = \#\ker(\text{id} - \phi) = \deg(\text{id} - \phi)$ (a 7.6.2 Következmény miatt $\text{id} - \phi$ szeparábilis, és így a 7.4 Állítás 3, része alapján $\#\ker(1 - \phi) = \deg(1 - \phi)$).

A 7.9 Állítás miatt a $\deg \text{End}(E)$ -n pozitív definit kvadratikus alak. A 3.6 Állítás 2, része miatt pedig $\deg \phi = q$. Így az előző lemmában kapott Cauchy-Schwarz egyenlőtlenséget használva $|\#E(K) - q - 1| = |\deg(\text{id} - \phi) - \deg \phi - \deg \text{id}| \leq 2\sqrt{\deg \phi \deg \text{id}} = 2\sqrt{q}$. $\square$

Hasse becslését bizonyos karakter-összegek becslésére használhatjuk véges testek felett:

8.1.1 Alkalmazás. Legyen $K = \mathbb{F}_q$, $2 \nmid q$ és legyen $f(x) = ax^3 + bx^2 + cx + d \in K[x]$ különböző $\bar{K}$ -beli gyökökkel. Legyen a karakter $\chi : K \rightarrow \{1, 0, -1\}$, $\chi(t) = \begin{cases} 1 & \text{ha létezik } t_0 \in K - \{0\}, \text{ hogy } t = t_0^2 \\ 0 & \text{ha } t = 0 \\ -1 & \text{különben} \end{cases}$

(mint a Legendre-szimbólum $q = p$ esetén).

Tekintsük az $E : y^2 = f(x)$ elliptikus görbét. Ekkor egy rögzített $x \in K$ -ra

1. nulla darab (x, y) alakú pontja van $E(K)$ -nak, ha $f(x)$ nem négyzet
2. egy darab (x, y) alakú pontja van $E(K)$ -nak, ha $f(x) = 0$
3. kettő darab (x, y) alakú pontja van $E(K)$ -nak, ha $f(x)$ nem nulla négyzet.

Ezt χ alapján felírva $\#E(K) = 1 + \sum_{x \in K} (\chi(f(x)) + 1) = 1 + q + \sum_{x \in K} \chi(f(x))$.

így Hasse becslése szerint $|\sum_{x \in K} \chi(f(x))| \leq 2\sqrt{q}$.

$q = p$ -re (p prím) ez éppen azt jelenti, hogy $|\sum_{x=0}^{p-1} (\frac{f(x)}{p})| \leq 2\sqrt{p}$, ahol $(\frac{a}{p})$ a Legendre-szimbólum.

9 Kitekintés: a Weil-sejtések

Hasse 1933-ban belátott becslése nyomán Weil 1949-ben fogalmazta meg projektív varietásokra vonatkozó sejtéseit. Ezek a 20. század második felében nagyban előrelendítették a az algebrai geometria fejlődését.

A sejtések egy, a Riemann-féle zeta függvény algebrai geometriai analógiának tekinthető generátorfüggvényről szólnak:

9.1 Definíció. Ha K egy q elemű test, K_n pedig ennek n -edfokú bővítése (azaz $|K_n| = q^n$), akkor $Z : \mathbb{C} \rightarrow \mathbb{C}$, $Z(V|K; T) = \exp\{\sum_{n=1}^{\infty} \#V(K_n) \frac{T^n}{n}\}$ a V **varietás zeta függvénye**, ahol $\exp\{F(T)\} = \sum_{j=0}^{\infty} \frac{F(T)^j}{j!}$.

Azért hasznos ez a függvény, mert $\#V(K_n)$ leolvasható belőle a következő formulával:

$$\frac{1}{(n-1)!} \frac{d^n}{(dT)^n} \log Z(V|K; T) \Big|_{T=0}.$$

9.1 Tétel. Weil sejtései

1, Racionalitás: $Z(V|K; T) \in \mathbb{Q}(T)$

2, Kielégíti a következő függvényegyenletet: $Z(V|K; 1/q^n T) = \pm q^{\varepsilon n/2} T^{\varepsilon} Z(V|K; T)$ alkalmas ε -ra (V Euler-karakterisztikája).

3, "Riemann-hipotézis": $Z(V|K; T)$ -nak létezik $\frac{P_1(T)P_3(T)\dots P_{2n-1}(T)}{P_0(T)P_2(T)\dots P_{2n}(T)}$ faktorizációja, ahol minden i -re $P_i(T) \in \mathbb{Z}[T]$, $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$, és minden $1 \leq i \leq 2n - 1$ -re $P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T)$ -re bomlik $\mathbb{C}$ felett, úgy, hogy $|\alpha_{ij}| = q^{i/2}$.

Weil a sejtéseit görbékre és Abel-varietásokra (projektív varietás csoport struktúrával) látta be. 1960-ban Dwork a racionalitásra, 1965-ben Grothendieck a függvényegyenletre, és végül 1973-ban Deligne a "Riemann-hipotézisre" vonatkozó állítást bizonyította be, többek között, amiért később megkapta a Fields-érmet, az Abel-díjat és a Wolf-díjat, a három legrangosabb kitüntetést a matematikában.

9.1 A varietás zeta függvénye és a Riemann féle zeta függvény

A függvény elnevezése nem véletlen, ugyanis sok hasonlóság van közte és a Riemann-féle zeta függvény között:

9.2 Definíció. A Riemann-féle zeta függvény

$$\zeta : \mathbb{C} \rightarrow \mathbb{C}, \zeta(s) = \begin{cases} \sum_{n=1}^{\infty} \frac{1}{n^s} & \text{ha } \operatorname{Re}(s) > 1 \\ \text{ennek meromorf kiterjesztése} & \text{ha } \operatorname{Re}(s) \leq 1 \end{cases}$$

Könnyen meggondolható, hogy $\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prím}} \left(\frac{1}{1-p^{-s}}\right)$ (minden $n \in \mathbb{N}$ -et felbonthatjuk prímtényezőik szorzatára, így $\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prím}} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots) = \prod_{p \text{ prím}} \frac{1}{1-p^{-s}}$).

Ezzel párhuzamosan belátható, hogy egy $V|K$ varietás zeta függvénye $Z(V|K, T) = \exp \sum_{n=1}^{\infty} \#V(K_n) \frac{T^n}{n} =$

$$\prod_{\substack{I \subseteq K(V) \text{ maximális} \\ \deg I = [\mathbb{F}_p[X]/I : \mathbb{F}_p]}} (1 - T^{\deg I})^{-1} \stackrel{s := -\log_p T}{=} \prod_{I \subseteq K(V) \text{ maximális}} \frac{1}{1 - (p^{\deg I})^{-s}} \text{ alakba írható (itt } p = \operatorname{char}(K) \text{ és}$$

A Riemann hipotézis alapján a zeta függvénynek $\text{Re}(s) = 1/2$ egyenesen vannak a nemtriviális gyökei, ami $Z(V|K, T)$ -re nézve annak felel meg, hogy az α_i gyökeire $|\alpha_i| = q^{1/2}$. Erről Hasse belátta, hogy ekvivalens a $|\#V(K_n) - 1 - q^n| \leq 2gq^{n/2}$ egyenlőtlenséggel, ahol g a varietás génusza. Ez $g = 1$ -re éppen az általunk belátott Hasse-bebecslés.

9.2 Véges testek feletti varietások kohomológiája

Egy sokaság kohomológiáját hasonlóan származtatjuk, mint a homológiáját, csak itt a lánckomplexusok és határleképezések duálisát kell vennünk.

Ha ϕ jelöli a q -adik Frobenius homomorfizmust, akkor $\#V(K_n) = \#Fix(\phi^n)$, azaz a varietás zeta függvénye $Z(V|K, T) = \exp \sum_{n=1}^{\infty} \#Fix(\phi^n) \frac{T^n}{n}$ alakba is írható.

Ha X egy komplex sokaság, $\phi : X \rightarrow X$ pedig egy megfelelően megválasztott endomorfizmus, akkor Lefschetz fixpont tétele nyomán $\exp\{\sum_{n=1}^{\infty} \#Fix(\phi^n) \frac{T^n}{n}\} = \prod_{i=0}^{2n} \det(1 - T\phi|H^i(X, \mathbb{C}))^{(-1)^{i+1}}$, ahol $H^i(X, \mathbb{C})$ X i . kohomológia csoportja, ϕ -re pedig most mátrixként gondolunk és $\det(1 - T\phi|H^i(X, \mathbb{C}))$ pedig a "karakterisztikus polinomja". Tehát X kohomológiája meghatározza a "zeta függvényét".

Ennek nyomán merült fel a véges testek feletti varietások kohomológiájának ötlete, melynek kidolgozása és következményei az algebrai geometriai fejlődésének mozgatórugói lettek a 20. század második felében.

Több sikertelen próbálkozás után végül M. Artin és Grothendieck vezette be az ún. Étale-kohomológiát 1962-ben.

9.3 Alkalmazások

Weil (mára már belátott) sejtéseinek fontos alkalmazási területe az analitikus számelmélet, azon belül is többek között az exponenciális összegek vizsgálata. Az exponenciális összegek $\sum_{n=0}^{\infty} a_n \exp(2\pi i x_n)$ alakú összegek valamely $(x_n)_{n \in \mathbb{N}} \subseteq \mathbb{C}^{\mathbb{N}}$ -re, amik az egészek eloszlásának vizsgálatára alkalmasak.

Egy ilyen összeg becslését láttuk a 8.1.1 Alkalmazásban.

Irodalomjegyzék

- [1] Jean-Pier Serre. *A Course in Arithmetic*. Springer, 1996.
- [2] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.
- [3] Robin Hartshorne. *Algebraic Geomtetry*. Springer, 1997.
- [4] Igor R. Shafarevich. *Basic Algebraic Geomtetry 1*. Springer, 2013.
- [5] Serge Lang. *Introduction to Algebraic and Abelian Functions*. Springer, 1995.
- [6] Thomas W. Hungerford. *Algebra*. Springer, 1974.
- [7] Zábrádi Gergely. *Algebrai számelmélet jegyzet*. 2020.
- [8] Nicholas M. Katz. “An Overview of Deligne’s Proof of the Riemann Hypothesis for Varieties Over Finite Fields”. In: *Proceeding of Symposia in Pure Mathematics* 28 (1976).

Nyilatkozat MI alapú eszközök használatáról

Alulírott *Somogyi Dalma* nyilatkozom, hogy szakdolgozatom elkészítése során nem használtam MI alapú eszközt.