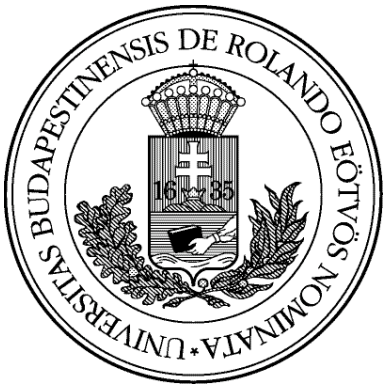
Eötvös Loránd Tudományegyetem
Természettudományi Kar

Bodor Bertalan
Matematika BSc
Matematikus szakirány

Elliptikus görbék torziópontjai

Szakdolgozat

Témavezető: Zábrádi Gergely egyetemi adjunktus



Budapest, 2013.

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Zábrádi Gergelynek a dolgozat igen alapos ellenőrzését, a konzultációkat és a kiváló szakirodalom ajánlását.

Tartalomjegyzék

Bevezetés

A diofantoszi egyenletek (azaz az egész vagy racionális számokra vonatkozó polinomegyenletek) tanulmányozásának története az ókori görögökig nyúlik vissza. Ha F egy kétváltozós egész vagy racionális együtthatós egyenlet, akkor az $F(x, y) = = 0$ egyenlet egész vagy racionális megoldásai megfelelnek az F polinomhoz tartozó algebrai görbe egész vagy racionális pontjainak.

A legegyszerűbb eset az, amikor F lineáris. Ekkor az egyenlet $ax + by = c$ alakú, ahol a, b, c egészek (és $ab \neq 0$). Egy ilyen egyenletnek mindig van racionális megoldása, és pontosan akkor van egész megoldása, ha $(a, b)|c$, és ekkor ezek a megoldások az euklideszi algoritmus segítségével megtalálhatóak.

Amennyiben F másodfokú, akkor F felírható valamilyen

$$F(X, Y) = aX^2 + bXY + cY^2 + dX + eY + f$$

alakban, ahol $a, b, c, d, e, f \in \mathbb{Q}$ (és $abc \neq 0$). Ekkor az F által definiált algebrai görbe egy megfelelő lineáris transzformációval átvihető egy $AX^2 \pm BY^2 = 0$ egyenletű ellipszisbe illetve hiperbolába, vagy egy $AX + BY^2 = 0$ egyenletű parabolába. Az ilyen típusú egyenletek racionális megoldásait a Hasse–Minkowsi-tétel ([7] IV. 8.) segítségével lehet meghatározni.

A következő eset, amikor $\deg F = 3$. Tegyük fel, hogy az F-hez tartozó (harmadfokú) algebrai görbe nem szinguláris (azaz nincs olyan pontja, ahol mindegyik parciális derivált eltűnik). Az ilyen tulajdonsági görbéket nevezzük elliptikus görbének. Jelöljük $E(\mathbb{Q})$-val az előbbi görbe racionális pontjait. Ha $E(\mathbb{Q})$ nem üres, akkor - amint ezt a 2. fejezetben látni fogjuk - $E(\mathbb{Q})$-n megadható egy természetes kommutatív csoportstruktúra. Mordell híres tétele ([5] IV.) szerint ez a csoport mindig végesen generált. Ezen csoport rangjával kapcsolatos a Birch–Swinnerton-Dyer-sejtés, ami a matematika egyik legfontosabb megoldatlan problémája. A sejtés teljesülése esetén ez a rang algoritmikusan kiszámítható. Ebben a dolgozatban az $E(\mathbb{Q})$ csoport torziórészcsoportjával fogunk foglalkozni, amint látni fogjuk a 4. fejezetben, ez könnyen kiszámítható. A dolgozatban leírt állítások és bizonyítások elsősorban az [5] könyv II. fejezetében leírtakon alapulnak.

1. Algebrai görbék

Ebben a fejezetben áttekintünk néhány alapvető algebrai geometriai fogalmat és tételt, amelyekre a dolgozat során szükségünk lesz.

1.1. Affin görbék

Legyen k tetszőleges test. Tekintsünk ekkor egy $f \in k[X,Y]$ (nem konstans) polinomot. Tegyük fel, hogy tetszőleges $k \subset K$ testre f-nek a K feletti irreducibilis felbontásában mindegyik tényező pontosan egyszer szerepel. Ekkor f definiál egy C_f *affin algebrai görbét* k felett, amelynek pontjai $K \times K$-ban valamilyen $k \subset K$ testre a

$$C_f(K) = \{(x,y) \in K \times K | f(x,y) = 0\}$$

halmaz. Ha $c \in k^\times$, akkor a $C_f(K)$ és $C_{cf}(K)$ görbéknek ugyanazok a pontjai minden $k \subset K$ testre, így az f és cf polinomokhoz tartozó affin görbéket a továbbiakban nem különböztetjük meg. A C_f görbe *foka* f foka. Ha $f, g \in k[X,Y]$, akkor néha $C : f = g$-vel fogjuk jelölni azt, hogy a C görbe megegyezik a C_{f-g} görbével.

A C_f görbét *irreduciblis*nek nevezzük, ha f irreducibilis k felett, és *geometriailag irreducibilis*nek nevezzük, ha f irreducibilis k^{al} felett. Legyen f irreducibilisekre való felbontása k felett $f = f_1 f_2 f_3 ... f_n$. Ekkor tehát az f_i polinomok páronként különbözőek. Ekkor tetszőleges $k \subset K$-ra

$$C_f(K) = \bigcup_{i=1}^{n} C_{f_i}(K)$$

ahol a C_{f_i} görbék irreducibilisek. Ezen C_{f_i} görbéket hívjuk a C_f algebrai görbe *irreducibilis komponens*einek.

Ha $f \in k[X,Y]$, akkor definiálhatjuk a $\frac{\partial f}{\partial X}$, $\frac{\partial f}{\partial Y}$ formális parciális deriváltakat a szokásos formulákkal. Ha valamilyen $P = (a,b) \in C_f(K)$ pontban mindkét parciális derivált eltűnik, akkor a P pontot *szinguláris pont*nak hívjuk. Ha a P pont nem szinguláris, akkor definiálhatjuk a C_f görbe P pont beli *érintő*jét a szokásos módon:

$$T_P(C_f) : \frac{\partial f}{\partial X}(a,b)(X-a) + \frac{\partial f}{\partial Y}(a,b)(Y-b) = 0$$

Ha $P = (a,b) \in C_f(K)$, akkor az f polinom egyértelműen felírható

$$f(X,Y) = f_1(X-a, Y-b) + f_2(X-a, Y-b) + ... + f_n(X-a, Y-b)$$

alakban, ahol minden i-re f_i egy homogén i-ed fokú polinom. Azt mondjuk, hogy a P pont *multiplicitás*a a C_f görbén m, ha $f_m \neq 0$, de $\forall i < m\,(f_i = 0)$. Könnyen

látható, hogy ekkor a P pont pontosan akkor szinguláris, ha $m \geq 2$. $m = 2$ esetén a P pontot *duplapont*nak nevezzük.

Az $f_m(X, Y)$ polinom egyértelműen felírható

$$f_m(X, Y) = \prod_{i=1}^{m} L_i$$

alakban, ahol az L_i polinomomok mind $L_i(X, Y) = c_i(X-a)+d_i(Y-b)$ alakúak, ahol $c_i, d_i \in K^{\mathrm{al}}$. Ekkor az $L_i = 0$ egyeneseket a C_f görbe P pont beli *érintő egyenes*einek hívjuk. Ha ezek az érintő egyenesek mind különbözőek (azaz az L_i polinomok mind különbözőek), akkor a P pontot *közönséges szinguláris pont*nak nevezzük. Egy C_f affin görbe *szinguláris*, ha $C_f(k^{\mathrm{al}})$-nak van szinguláris pontja.

1.2. Metszetmultiplicitás

Legyen $\mathcal{F}(k)$ az olyan $f, g \in K[X, Y]$ párok halmaza, amelyeknek nincs olyan h közös irreducibilis faktora, melyre $h(0,0) = 0$. Ekkor a következő tétel igaz:

1.2.1. Tétel. *Egyértelműen létezik olyan $I : \mathcal{F}(k) \to \mathbf{N}$ függvény, amire a következők teljesülnek:*
(a) $I(X, Y) = 1$;
(b) $I(f, g) = I(g, f)$ minden $(f, g) \in \mathcal{F}(k)$-ra;
(c) $I(f, gh) = I(f, g) + I(f, h)$ minden $(f, g), (f, h) \in \mathcal{F}(k)$-ra;
(d) $I(f, g + hf) = I(f, g)$ minden $(f, g) \in \mathcal{F}(k)$ és $h \in k[X, Y]$-ra;
(e) $g(0,0) \neq 0 \Rightarrow I(f, g) = 0$.

A bizonyítás megtalálható például [5] I. 1. fejezetében. Ha $(f, g) \in \mathcal{F}(k)$, akkor a C_f és C_g görbék origó beli *metszetmultiplicitás*án az $I(f, g)$ számot értjük a tételben szereplő I függvényre. Jelöljük $k[[X, Y]]$-nal a k feletti formális hatványsorok gyűrűjét (az X, Y változókkal). Ekkor $k[[X, Y]]$ egy k-algebra is. Belátható, hogy minden $(f, g) \in \mathcal{F}(k)$-ra $k[[X, Y]]/(f, g)$, mint k-vektortér véges dimenziós, és az $I(f, g) = \dim(k[[X, Y]]/(f, g))$ függvény kielégíti a tétel feltételeit ([1] III. 3.). Hasonlóképpen tetszőleges $f, g \in k[X, Y]$-re a $C_f(K)$ és $C_g(K)$ görbéknek a $P = (a, b) \in C_f(K) \cap C_g(K)$ pont beli metszetmultiplcititásán az

$$I(P, C_f \cap C_g) := I(f(X + a, Y + b), g(X + a, Y + b))$$

számot értjük. Belátható, hogy ez a szám mindig legalább akkora, mint a P pontnak a C_f és a C_g görbéken vett multiplicitásainak a szorzata.

Tekintsünk egy C tetszőleges affin görbét, és annak egy P nem szinguláris pont-

ját. Könnyen meggondolható, hogy ekkor egy P-n átmenő L egyenesre

$$I(P, C \cap L) \geq 2$$

pontosan akkor teljesül, ha L a görbe P pont beli érintője. Ha $I(P, C \cap T_P C) \geq 3$, akkor a P pontot a C görbe *inflexiós pontjá*nak nevezzük.

1.3. Projektív görbék

Tekintsük a k feletti projektív síkot:

$$\mathbf{P}^2(k) = \{(x, y, z) \in k^3 | (x, y, z) \neq (0,0,0)\} / \sim,$$

ahol

$$(x, y, z) \sim (x', y', z') \Leftrightarrow \exists c \in k^\times (x' = cx, y' = cy, z' = cz).$$

Az $(x, y, z) \in k^3$ vektornak megfelelő ekvivalenciaosztályát $(x : y : z)$-vel fogjuk jelölni. Legyen $U_2 = \{(x : y : z) \in \mathbf{P}^2(k) | z \neq 0\}$. Ekkor az

$$(x, y) \mapsto (x : y : 1) : k \times k \to \mathbf{P}^2(k)$$

hozzárendelés egy bijekció az $\mathbf{A}^2(k) = k \times k$ affin sík és U_2 között, ezért U_2 azonosítható egy k feletti affin síkkal. Tekintsünk most egy $F \in k[X, Y, Z]$ (nem konstans) homogén polinomot, és tegyük fel, hogy tetszőleges $k \subset K$ testre F-nek a K feletti irreducibilis felbontásában mindegyik tényező pontosan egyszer szerepel. Ekkor F definiál egy C_F *projektív algebrai görbé*t k felett, amelynek pontjai $\mathbf{P}^2(K)$-ban valamilyen $k \subset K$ testre a

$$C_F(K) = \{(x : y : z) \in \mathbf{P}^2(K) | F(x, y, z) = 0\}$$

halmaz. (Mivel F homogén, ezért $F(cx, cy, cz) = c^{\deg F} F(x, y, z)$, így mindegy, hogy egy $(x : y : z) \in \mathbf{P}^2(k)$ pontnak melyik reprezentánsát tekintjük.) Az affin esethez hasonlóan a C_F, és C_G görbéket nem fogjuk megkülönböztetni, ha $G = cF$ valamilyen $c \in k^\times$-ra. A C_F görbe *foka* F foka. Legyenek $U_0 = \{(x : y : z) \in \mathbf{P}^2(k) | x \neq 0\}$, $U_1 = \{(x : y : z) \in \mathbf{P}^2(k) | y \neq 0\}$. Ekkor az U_2-höz hasonlóan U_0 és U_1 is természetes módon azonosítható az $\mathbf{A}^2(k) = k \times k$ affin síkkal. Ekkor $\mathbf{P}^2(k) = U_0 \cup U_1 \cup U_2$. Tekintsünk most egy $C = C_F$ projektív görbét. Legyen $C_i = C \cap U_i$, ekkor $C = C_0 \cup C_1 \cup C_2$, és ha minden U_i-t a természetes módon azonosítjuk az $\mathbf{A}^2(k)$ affin síkkal, akkor C_0-at, C_1-et és C_2-t rendre azonosíthatjuk az $F(1, Y, Z)$, $F(X,1, Z)$ és $F(X, Y,1)$ polinomok által definiált affin görbékkel.

A projektív görbékre is kiterjeszthetőek a *szinguláris pont, érintő, multiplicitás, metszetmultiplicitás*, stb. fogalmak felhasználva, hogy egy C projektív görbe tetszőleges P pontja rajta van a C_0, C_1, C_2 affin görbék valamelyikén.

A későbbiekben szükségünk lesz az alábbi algebrai geometriai tételre.

1.3.1. Tétel (Bézout)**.** *Legyenek C, D projektív algebrai görbék valamilyen k test felett, melyeknek foka rendre m és n. Tegyük fel, hogy C-nek és D-nek nincs közös irreduciblis komponense. Ekkor C és D közös pontjainak száma k^{al} felett (multiplicitással számolva) mn, azaz*

$$\sum_{P \in C(k^{\mathrm{al}}) \cap D(k^{\mathrm{al}})} I(P, C \cap D) = mn$$

A tétel bizonyítása megtalálható [1] 5. fejezetében.

2. Harmadfokú görbék

Ebben a fejezetben definiálunk egy csoportstruktúrát a harmadfokú projektív algebrai görbéken, majd definiáljuk az elliptikus görbe fogalmát, és megvizsgáljuk az elliptikus görbék néhány alapvető tulajdonságát. A fejezet végén belátunk néhány egyszerű állítást szinguláris harmadfokú görbékkel kapcsolatban.

2.1. Csoportstruktúra egy harmadfokú görbén

Legyen C egy harmadfokú nem szinguláris projektív görbe k felett. Ekkor C szükségképpen geometriailag irreducibilis. Tegyük fel ugyanis, hogy $C = C_{fg}$ valamilyen $f, g \in k^{\mathrm{al}}[X, Y, Z]$ nem konstans polinomokra. Ekkor $C_f(k^{\mathrm{al}}) \cap C_g(k^{\mathrm{al}})$ nem üres a Bézout-tétel (1.3.1 tétel) szerint, és ekkor egy $P \in C_f(k^{\mathrm{al}}) \cap C_g(k^{\mathrm{al}}) \subset C(k^{\mathrm{al}})$ pontra

$$\frac{\partial(fg)}{\partial X}(P) = f(P)\frac{\partial g}{\partial X}(P) + g(P)\frac{\partial f}{\partial X}(P) = 0,$$

és hasonlóan a többi parciális derivált is 0, tehát a P pont szinguláris, ami lehetetlen, hiszen a C görbe nem szinguláris.

Az egyszerűség kedvéért a k testről mindig feltesszük, hogy tökéletes (általában $\operatorname{char} k = 0$ lesz). Tegyük fel, hogy $C(k)$ nem üres, rögzítsünk ekkor egy tetszőleges $O \in C(k)$ pontot. Ekkor $C(k)$ pontjain megadható természetes módon egy csoportstuktúra, amint ezt látni fogjuk.

Tekintsünk most valamilyen $P_1, P_2 \in C(k)$ pontokat, amik közül egyik sincs rajta a görbének a másik pont beli érintőjén. Ekkor a P_1 és P_2 pontokat összekötő egyenes egyenlete

$$l(P_1P_2) : aX + bY + cZ = 0$$

alakú, ahol $a, b, c \in k$. Mivel ez az egyenes nem érinti a P_1 és P_2 pontok egyikében sem $C(k)$-t, ezért $I(P_1, C(k) \cap l(P_1P_2)) = I(P_2, C(k) \cap l(P_1P_2)) = 1$, és így a Bézout-tétel (1.3.1 tétel) szerint létezik pontosan egy olyan $P_3 \in C(k^{\mathrm{al}})$ pont, ami rajta van $l(P_1P_2)(k^{\mathrm{al}})$-en, és különbözik a P_1 és P_2 pontoktól. Azt állítjuk, hogy $P_3 \in C(k)$. Legyen $\sigma \in \mathrm{Gal}(k^{\mathrm{al}}/k)$. Valamilyen $P = (x : y : z) \in \mathbf{P}^2(k^{\mathrm{al}})$ pontra jelöljük σP-vel a $(\sigma(x) : \sigma(y) : \sigma(z))$ pontot. Ekkor

$$P \in l(P_1P_2) \Leftrightarrow ax + by + cz = 0 \Leftrightarrow \sigma(ax + by + cz) = 0 \Leftrightarrow$$
$$\Leftrightarrow a\sigma(x) + b\sigma(y) + c\sigma(z) = 0 \Leftrightarrow \sigma(P) \in l(P_1P_2)$$

Minden $\sigma \in \mathrm{Gal}(k^{\mathrm{al}}/k)$-ra $\sigma(P_1) = P_1$, $\sigma(P_2) = P_2$ (hiszen $P_1, P_2 \in \mathbf{P}^2(k)$), ezért minden $\sigma \in \mathrm{Gal}(k^{\mathrm{al}}/k)$-ra $\sigma(P_3) = P_3$. Mivel k tökéletes, ezért a k^{al}/k bővítés normális és szeparábilis, és ekkor $\forall \sigma \in \mathrm{Gal}(k^{\mathrm{al}}/k)(\sigma(t) = t) \Leftrightarrow t \in k$. Ebből következik,

hogy a P_3 pont koordinátáinak aránya is k-ban van, és ekkor $P_3 \in \mathbf{P}^2(k) \Rightarrow$
$\Rightarrow P_3 \in C(k)$.

Legyen most $P_1 \in C(k)$ egy tetszőleges pont, és tegyük fel, hogy P_1 nem inflexiós pontja C-nek, azaz $I(P_1, C \cap T_{P_1}(C)) = 2$. Ekkor a Bézout-tétel (1.3.1 tétel) szerint létezik pontosan egy, a P_1-től különböző $P_2 \in C(k^{\mathrm{al}})$ pont, ami rajta van $T_{P_1}(C)(k^{\mathrm{al}})$-on. Ekkor az előbbi esethez hasonlóan látható, hogy $P_2 \in C(k)$.

Ha $P, Q \in C(k)$, $P \neq Q$, és $l(PQ)$ nem érinti $C(k)$-t a P és Q pontokban, akkor jelöljük PQ-val $l(PQ)$ és $C(k)$ harmadik metszéspontját. Ha $P \neq Q$, és $l(PQ)$ érinti $C(k)$ P-ban vagy Q-ban, akkor jelölje PQ a P, Q pontok közül azt, amelyikben érinti (a Bézout-tétel szerint nem érintheti mindkét pontban). PP jelölje P-t, ha P inflexiós pont, és jelölje a $T_P(C)(k)$ érintő és $C(k)$ másik metszéspontját, ha P nem inflexiós pont.

2.1.1. Tétel. *Az előbbi jelölések mellett $C(k)$ pontjai egy kommutatív csoportot alkotnak a $P + Q := O(PQ)$ műveletre, amelynek egységeleme az O pont.*

Bizonyítás (vázlat). Ha P, Q tetszőlegesek pontjai $C(k)$-nak, akkor nyilván $PQ =$
$= QP$, és így $P + Q = O(PQ) = O(QO) = Q + P$. $O + P = O(OP) = P$ a definícióból. Legyen $P' = P(OO)$. Ekkor a P, OO és P' pontok egy egyenesen vannak. (Pontosabban valamilyen L egyenesre ezek a pontok éppen az L és a $C(k)$ görbe metszéspontjai multiplicitással számolva.) Ekkor tehát $PP' = OO$, és ekkor $P + P' = O(PP') = O(OO) = O + O = O$.

Az asszociativitás bizonyításához vezessük be a következő jelölést: ha C_1, C_2 harmadfokú projektív görbék k felett, amiknek nincs közös irreducibilis komponense, akkor jelölje $C_1 \cdot C_2$ a

$$\sum_{P \in C_1(k) \cap C_2(k)} I(P, C_1 \cap C_2)[P_i]$$

elemet a C_1 görbe $\mathbf{P}^2(k)$-beli pontjai által generált szabad Abel-csoportban. Azt állítjuk, hogy ekkor ha valamilyen C_1, C_2, C_3 harmadfokú görbékre, ha C_1-nek és C_2-nek, valamint C_1-nek és C_3-nak nincs közös irreducibilis komponense, és $C_1 \cdot C_2 =$
$= \sum_{i=1}^{9} [P_i]$, akkor $C_1 \cdot C_3 = \sum_{i=1}^{8} [P_i] + [Q]$ esetén $Q = P_9$.

Ezt abban az esetben bizonyítjuk, amikor a $P_1, P_2, ..., P_9$ pontok mind különbözőek, és általános helyzetűek abban az értelemben, hogy a $P_i = (x_i : y_i, z_i)$ jelölés mellett a

$$v_i := (x_i^3, x_i^2 y_i, x_i^2 z_i, x_i y_i^2, x_i y_i z_i, x_i z_i^2, y_i^3, y_i^2 z_i, y_i z_i^2, z_i^3)$$

vektorok lineárisan függetlenek. Legyen

$$F(X, Y, Z) =$$
$$= a_1 X^3 + a_2 X^2 Y + a_3 X^2 Z + a_4 X Y^2 + a_5 X Y Z + a_6 X Z^2 + a_7 Y^3 + a_8 Y^2 Z + a_9 Y Z^2 + a_{10} Z^3.$$

Ekkor a $P_i\,(i = 1{,}2{,}...{,}8)$ pontok pontosan akkor vannak rajta a C_F görbén, ha $\langle a, v_i\rangle = 0$ minden $i = 1{,}2{,}...{,}8$-ra $(a = (a_1, a_2, ..., a_{10}))$. Ez 8 lineáris egyenlet az a_i együtthatókra, ami a v_i vektorok lineáris függetlensége miatt azt jelenti, hogy ennek megoldásai egy 2 dimenziós alteret alkotnak k^{10}-ben. Ebből következik, hogy a $C_j = = C_{F_j}$ $(j = 1{,}2{,}3)$ jelölés mellett F_1 és F_2 együtthatóiból álló vektorok generálják ezt az alteret, és ekkor létezik olyan $\lambda, \mu \in k$, hogy $F_3 = \lambda F_1 + \mu F_2$, amiből

$$P_9 \in C_1(k) \cap C_2(k) \Rightarrow P_9 \in C_{\lambda F_1 + \mu F_2} = C_3.$$

Ez csak $P_9 = Q$ esetén lehetséges a Bézout-tétel (1.3.1 tétel) szerint. Az általános eset bizonyításához ld. [1], 124. o.

Legyenek most P, Q, R tetszőleges pontjai $C(k)$-nak, és legyenek ekkor

$$S := (P + Q)R, \quad T := P(Q + R).$$

Ekkor $(P+Q)+R = OS$ és $P+(Q+R) = OT$, ezért az asszociativitáshoz elég lenne belátni, hogy $S = T$. Jelöljük általában $l(P_1P_2)$-vel a P_1 és P_2 pontokat összekötő egyenest, ha $P_1 \neq P_2$, és $T_{P_1}(C)$-t, ha $P_1 = P_2$, és tekintsük ekkor a

$$\begin{aligned} C_1 &:= C \\ C_2 &:= l(P, Q) \cup l(R, P + Q) \cup l(QR, O) \\ C_3 &:= l(P, Q + R) \cup l(Q, R) \cup l(PQ, O) \end{aligned}$$

harmadfokú görbéket. Könnyen ellenőrizhető, hogy ekkor

$$\begin{aligned} C_1 \cdot C_2 &= [P] + [Q] + [PQ] + [R] + [P + Q] + [S] + [QR] + [O] + [Q + R] \\ C_1 \cdot C_3 &= [P] + [Q + R] + [T] + [Q] + [R] + [QR] + [PQ] + [O] + [P + Q] \end{aligned}$$

Mint láttuk a $C_1 = C$ görbe geometriailag irreducibilis, ezért használható az előbbi állítás, ami ezesetben éppen azt mondja, hogy $S = T$. □

2.1.2. Megjegyzés. *Az előbbi csoport elegánsabban is definiálható a divizorok és a görbe Picard-csoportjának segítségével, ld. [5] I. 4. vagy [8] III. 3.*

2.2. Elliptikus görbék

2.2.1. Definíció. *Legyen k egy tökéletes test. Ekkor egy (E, O) pár egy* elliptikus görbe *k felett, ha E egy harmadfokú nem szinguláris görbe k felett, és O egy inflexiós pontja $E(k)$-nak.*

2.2.2. Állítás. *(a) Legyen (E, O) egy elliptikus görbe k felett. Ekkor létezik olyan invertálható k-lineáris transzformáció, ami (E, O)-t egy olyan (E', O') elliptikus görbébe viszi, amire $O' = (0 : 1 : 0)$, és E'-nek az O'-beli érintőjének az egyenlete $Z = 0$.*

(b) Ha (E,O) egy elliptikus görbe, amire $O=(0:1:0)$, és E-nek az O-beli érintőjének az egyenlete $Z=0$, akkor E egyenlete a következő alakban írható:

$$E: a_0Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \quad (a_0\neq 0)$$

Bizonyítás. (a) Könnyen ellenőrizhető, hogy $\mathrm{GL}_3(k)$ tranzitívan hat a $0<V_1<<V_2<k^3$ altérpárokon, így $\mathrm{PGL}_3(k)$ is tranzitívan hat az $L_0<L_1<\mathbf{P}^2(k)$ projektív altérpárokon. Ezt használva könnyen adódik az állítás.

(b) Legyen (E,O) egy elliptikus görbe, ami teljesíti az állításban szereplő feltételeket, és legyen

$$F(X,Y,Z)=$$
$$=c_1X^3+c_2X^2Y+c_3X^2Z+c_4XY^2+c_5XYZ+c_6XZ^2+c_7Y^3+c_8Y^2Z+c_9YZ^2+c_{10}Z^2$$

az a polinom, ami az E görbét definiálja. Ekkor mivel $O=(0:1:0)\in E(k)$, ezért $c_7=0$. Legyen $U_1=\{(x:y:z)\in\mathbf{P}^2(k)|y\neq 0\}$, ekkor mint láttuk U_1 azonosítható az $\mathbf{A}^2(k)=k\times k$ affin síkkal, és az $E\cap U_1$ görbe azonosítható az

$$E_1: c_1X^3+c_2X^2+c_3X^2Z+c_4X+c_5XZ+c_6XZ^2+c_8Z+c_9Z^2+c_{10}Z^3$$

affin görbével az $(x:1:z)\mapsto(x,z):\mathbf{P}^2(k)\to\mathbf{A}^2(k)$ bijekción keresztül. Ekkor az E görbének az origó beli érintőjének egyenlete $c_4X+c_8Z=0$. Ez azonban a feltétel szerint megegyezik a $L_\infty: Z=0$ egyenessel, így $c_4=0$ és $c_8\neq 0$. Mivel O inflexiós pontja E-nek, ezért

$$3\leq I(O,L_\infty\cap E)=I(Z,F(X,1,Z))=I(Z,c_1X^3+c_2X^2),$$

amiből következik, hogy $c_2=0$. Azt kaptuk tehát, hogy az F polinom a következő alakban írható:

$$F(X,Y,Z)=c_1X^3+c_3X^2Z+c_5XYZ+c_6XZ^2+c_8Y^2Z+c_9YZ^2+c_{10}Z^2.$$

$c_1\neq 0$, hiszen $c_1=0$ esetén $F(X,Y,Z)$ osztható lenne Z-vel. Ekkor ezt az egyenletet c_1-gyel elosztva, majd átrendezve megkapjuk a kívánt alakot. □

Az előbbi egyenletben $a_0=1$ is elérhető az $(X,Y,Z)\mapsto(X,Y,\frac{Z}{a_0})$ lineáris transzformáción keresztül. Egy (E,O) elliptikus görbének az előbbi formában felírt egyenletét hívjuk az elliptikus görbe Weierstrass-egyenletének.

Amennyiben $\operatorname{char}k\neq 2,3$, akkor az előbbi egyenletben az

$$(X,Y,Z)\mapsto(X+\frac{a_0}{3}Z,Y+\frac{a_1}{2}X+\frac{a_3}{2}Z,Z)$$

lineáris transzformáción keresztül $a_1 = a_2 = 0$ is elérhető, és ekkor egy

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

alakú egyenletet kapunk. A későbbiekben mindig feltesszük, hogy egy elliptikus egyenlete ilyen alakú.

2.3. Szinguláris harmadfokú görbék

Legyen $C = C_f$ egy tetszőleges harmadfokú görbe, ahol

$$f(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3 \quad a, b \in k$$

alakú. Megvizsgáljuk, hogy ekkor C milyen feltételek mellett szinguláris, és hogy milyen típusú szingularitásai lehetnek.

Tegyük fel, hogy S egy szinguláris pontja a $C(k^{\mathrm{al}})$ görbének. Ekkor $S \neq O$, hiszen $\frac{\partial f}{\partial Z}(O) = 1 \neq 0$. Az $l(SO)$ egyenes tehát legalább két különböző pontban metszi $C(k^{\mathrm{al}})$-t, így $I(S, C \cap l(SO)) < 3$, ami azt jelenti, hogy az S pont multiplicitása pontosan 2 a $C(k^{\mathrm{al}})$ görbén. Azt állítjuk, hogy a $C(k^{\mathrm{al}})$ görbének az S ponton kívül nem lehet szinguláris pontja. Tegyük fel ugyanis, hogy egy $T \neq S$ pont szinguláris pontja $C(k^{\mathrm{al}})$-nak. Ekkor $4 \leq I(S, C \cap l(ST)) + I(T, C \cap l(ST))$, ami ellentmond a Bézout-tételnek (1.3.1 tétel). Ebből az is következik, hogy szükségképpen $S \in$ $\in C(k)$. Legyen ugyanis $\sigma \in \mathrm{Gal}(k^{\mathrm{al}}/k)$ tetszőleges. Ekkor minden $P \in C(k^{\mathrm{al}})$ pontra $\frac{\partial f}{\partial X}(P) = 0 \Leftrightarrow \frac{\partial f}{\partial X}(\sigma(P)) = 0$, és hasonlóan a többi parciális deriváltra, ami azt jelenti, hogy $\sigma(S) = S$ minden $\sigma \in \mathrm{Gal}(k^{\mathrm{al}}/k)$-ra. Ebből a korábbiakhoz hasonlóan következik, hogy $S \in C(k)$.

Jelölje $C^{\mathrm{ns}}(k)$ a $C(k)$ görbe nem szinguláris pontjainak halmazát (azaz $C(k) \setminus$ $\setminus \{S\}$-et). Tetszőleges $P, Q \in C^{\mathrm{ns}}(k)$ pontokra definiáljuk a PQ pontot a nem szinguláris esethez hasonlóan. Ekkor $PQ \neq S$, hiszen ekkor a P és Q pontokat összekötő $l(PQ)$ egyenesnek (vagy $P = Q$ esetén a görbe P pont beli érintőjének) és a görbének a metszéspontjai (multiplicitással számolva) P, Q és PQ. Ha $PQ = P$ vagy $PQ = Q$, akkor készen vagyunk, egyébként pedig $I(PQ, l(PQ) \cap C) = 1$, ami nem lehetséges $PQ = S$ esetén. Ezen jelölések mellett a nem szinguláris esethez hasonlóan igazolható, hogy $C^{\mathrm{ns}}(k)$ pontjai egy kommutatív csoportot alkotnak a $P + Q := O(PQ)$ műveletre, ahol $O = (0 : 1 : 0)$ a csoport egységeleme.

2.3.1. Állítás. *Ha* $\mathrm{char}\, k \neq 2$*, akkor a* $C : Y^2Z = X^3 + aXZ^2 + bZ^3$ *görbe pontosan akkor szinguláris, ha* $\Delta := 4a^3 + 27b^2 = 0$.
Ha $\mathrm{char}\, k = 2$*, akkor az előbbi görbe mindig szinguláris.*

Bizonyítás. Mint láttuk az O pont soha nem szinguláris pontja C-nek, és ez az egyetlen pont a $Z = 0$ egyenesen, így a C görbe pontosan akkor szinguláris, ha a

$C_2 : Y^2 = X^3 + aX + b$ affin görbe szinguláris. Egy $(x, y) \in \mathbf{A}^2(k)$ pont pontosan akkor szinguláris pontja $C_2(k)$-nak, ha az alábbi egyenletek teljesülnek:

$$2y = 0, \quad 3x^2 + a = 0, \quad y^2 = x^3 + ax + b.$$

Ha $\operatorname{char} k \neq 2$, akkor ez pontosan akkor teljesül, ha $y = 0$, és x gyöke a

$$g(X) = X^3 + aX + b$$

polinomnak és $g(X)$ deriváltjának. Ez pedig pontosan akkor lehetséges, ha $g(X)$-nek van többszörös gyöke, ami pontosan akkor teljesül, ha a diszkriminánsa $\Delta = 4a^3 + + 27b^2 = 0$.

Ha $\operatorname{char} k = 2$, akkor legyenek $\alpha, \beta \in k$ olyanok, hogy $\alpha^2 + a = 0$ és $\beta^2 = \alpha^3 + + a\alpha + \beta$ teljesüljenek. Ilyen α és β létezik, hiszen k tökéletes, így a $x \mapsto x^2 : k \to k$ Frobenius-endomorfizmus szürjektív. Könnyen látható, hogy ekkor (α, β) szinguláris pontja C-nek. □

Tegyük fel most, hogy $\operatorname{char} k \neq 2{,}3$, és legyen

$$C : Y^2Z = X^3 + aXZ^2 + bZ^3$$

egy szinguláris projektív görbe, és

$$C_2 : Y^2 = X^3 + aX + b$$

a megfelelő affin görbe. Ekkor tehát $4a^3 + 27b^2 = 0$. Ha $a \neq 0$, akkor legyen $t := -\frac{3}{2}\frac{b}{a}$. Ha $a = 0$ (azaz $a = b = 0$), akkor legyen $t := 0$. Könnyen ellenőrizhető, hogy ekkor $t^2 = -\frac{a}{3}$, és $t^3 = -\frac{b}{2}$, és ekkor a C_2 görbe egyenlete

$$Y^2 = X^3 + aX + b \Leftrightarrow Y^2 = X^3 - 3t^2X + 2t^3 \Leftrightarrow Y^2 = (X - t)^2(X + 2t) \Leftrightarrow$$
$$\Leftrightarrow Y^2 = (X - t)^3 + 3t(X - t)^2$$

alakban is írható. Ekkor tehát az

$$(X, Y, Z) \mapsto (X - tZ, Y, Z)$$

lineáris transzformáció $C(k)$-t a

$$C'(k) : Y^2Z = X^3 + 3tX^2Z$$

görbébe viszi.

Tegyük fel először, hogy $t = 0$. Ekkor $C = C'$. Legyenek

$$C_0 : Y^2Z = 1,\ C_1 : Z = X^3 \text{ és } C_2 : Y^2 = X^3$$

a C görbének megfelelő affin görbék. A $C_2(k)$ görbe (egyetlen) szinguláris pontja az origó, ami ekkor egy duplapont, és a C_2 görbének az egyetlen origóbeli érintő egyenese az $L : Y = 0$ egyenes. Továbbá

$$I((0,0), L \cap C_2) = I(Y^2 - X^3, Y) = I(X^3, Y) = 3$$

is teljesül, az ilyen tulajdonságú szingularitásokat *cusp*nak hívjuk. Könnyen látható, hogy a $C(k)$ görbének az $Y = 0$ egyenesen az $S = (0 : 0 : 1)$ szinguláris pontján kívül nincs más pontja, így $C^{\text{ns}}(k)$ pontjai megfeleltethetőek a C_1 affin görbe pontjainak, a továbbiakban ezeket a természetes módon azonosítjuk egymással. Tegyük fel, hogy a $P_1 = (x_1, z_1), P_2 = (x_2, z_2), P_3 = (x_3, z_3) \in C_1(k)$ pontokra $P_1 + P_2 + P_3 = O$. Ez pontosan akkor teljesül, ha ezek a pontok egy egyenesen vannak, pontosabban ha ezek a pontok valamilyen L egyenes és a C_1 görbe metszéspontjai multiplicitással számolva. Ennek az L egyenesnek az egyenlete legyen

$$L : Z = \alpha X + \beta.$$

Ekkor az

$$X^3 - \alpha X - \beta = 0$$

egyenlet gyökei (multiplicitással számolva) éppen x_1, x_2 és x_3, amiből következik, hogy $x_1 + x_2 + x_3 = 0$. Könnyen látható továbbá, hogy $P = (x.z) \in C_1(k)$ esetén $-P = (-x, -z)$. Ebből következik, hogy tetszőleges $P_1, P_2 \in C_1$ pontok esetén

$$x(P_1 + P_2) = x(P_1) + x(P_2) + x(-P_1 - P_2) + x(P_1 + P_2) = x(P_1) + x(P_2),$$

ahol $x(P)$ jelöli egy $P \in C_1$ pont X koordinátáját. Ez éppen azt jelenti, hogy a

$$P \mapsto x(P) : C_1(k) \to k^+$$

vagy az eredeti jelölésekkel az

$$(x : y : z) \mapsto x/y : C^{\text{ns}}(k) \to k^+$$

leképezés egy homomorfizmus. Könnyen látható, hogy ez a leképezés valójában izomorfizmus, tehát $C^{\text{ns}}(k) \simeq k^+$.

Tegyük fel most, hogy $t \neq 0$. Ekkor a

$$C_2'(k) : Y^2 = X^3 + 3tX^3$$

görbe (egyetlen) szinguláris pontja az origó. Ez egy közönséges duplapont, hiszen a görbének az origóbeli érintő egyeneseinek az egyenlete

$$L_1 : Y + \sqrt{3t}X = 0,\ L_2 : Y - \sqrt{3t}X = 0,$$

amik különbözőek. Az ilyen tulajdonságú szingularitásokat *node*-nak nevezzük. Ebben az esetben az előbbi számoláshoz hasonlóan ellenőrizhető, hogy az

$$(x : y : z) \mapsto \frac{y + \sqrt{3t}(x - tz)}{y - \sqrt{3t}(x - tz)} : C^{\mathrm{ns}}(k) \to (k[\sqrt{3t}])^{\times}$$

leképezés egy injektív homomorfizmus. Amennyiben $\sqrt{3t} \in k$, akkor ez a homomorfizmus szürjektív is, amiből következik, hogy ekkor $C^{\mathrm{ns}}(k) \simeq k^{\times}$. Amennyiben $\sqrt{3t} \notin k$, akkor az előbbi homomorfizmus képe

$$\mathbb{G}_m[\sqrt{3t}](k) := \{\gamma \in (k[\sqrt{3t}])^{\times} \,|\, \mathrm{Nm}\,\gamma = 1\},$$

ahol $\mathrm{Nm}(x + \sqrt{3t}y) = x^2 - 3ty^2$ tetszőleges $x, y \in k$ esetén. Ebben az esetben tehát $C^{\mathrm{ns}}(k) \simeq \mathbb{G}_m[\sqrt{3t}](k)$.

3. p-adikus számok

Ebben a fejezetben bevezetjük a p-adikus számok fogalmát, és ezekkel kapcsolatban belátunk néhány egyszerű tételt, amikre a 4. fejezetben szükségünk lesz.

3.1. Értékelések

3.1.1. Definíció. *Legyen K egy tetszőleges test. Ekkor egy $x \mapsto |x| : K \to \mathbb{R}$ függvényt* értékelés*nek nevezünk, ha a következő feltételek teljesülnek:*
(a) $|0| = 0$ *és* $|x| > 0$ *minden* $x \in K^\times$*-ra*
(b) $|xy| = |x||y|$
(c) $|x + y| \leq |x| + |y|$.
Amennyiben a (c)-nél erősebb
(c') $|x + y| \leq \max\{|x|, |y|\}$
feltétel is teljesül, akkor az értékelést nemarkhimédeszi*nek (egyébként pedig* arkhimédeszi*nek) hívjuk.*

Egy $|\ |$ értékelést *triviális*nak hívunk, ha minden $x \in K^\times$-ra $|x| = 1$. Az (a) és (b) tulajdonságokból következik, hogy egy $|\ |$ értékelés homomorfizmus $K^\times$-ból a pozitív valós számok multiplikatív csoportjába. Mivel ez a csoport torziómentes, ezért K minden egységgyökének 1 az értékelése. Speciálisan $|-1| = 1$, és így a (b) tulajdonság szerint $|x| = |-x|$ minden $x \in K$-ra.

Minden $|\ |$ értékelés definiál egy metrikán (és így egy topológiát is) K-n a $d(x, y) = |x - y| = |y - x|$ távolsággal. A $|\ |_1$ és $|\ |_2$ értékeléseket ekvivalensnek nevezzük, ha $|\ |_1$ és $|\ |_2$ ugyanazt a topológiát definiálja K-n.

3.1.2. Állítás. *A $|\ |_1$ és $|\ |_2$ nem triviális értékelések pontosan akkor ekvivalensek, ha $|\ |_2 = |\ |_1^a$ valamilyen $a > 0$-ra.*

Bizonyítás. Ha $|\ |_2 = |\ |_1^a$ valamilyen $|\ |_1$ és $|\ |_2$ értékelésekre és $a > 0$-ra, akkor $|\ |_1$ és $|\ |_2$ nyilván ekvivalensek.

A másik irányhoz tekintsünk valamilyen $|\ |_1$ és $|\ |_2$ ekvivalens nem triviális értékeléseket. Mivel $|\ |_1$ nem triviális, ezért létezik olyan $y \in K$, amire $|y|_1 > 1$. Legyen ekkor $a = \log |y|_2 / \log |y|_1$. Ekkor $|y|_2 = |y|_1^a$. Legyen most $x \in K^\times$ tetszőleges. Ekkor $|x|_1 = |y|_1^b$ valamilyen b valós számra. Azt állítjuk, hogy $|x|_2 = |y|_2^b$.

Ehhez tekintsünk egy tetszőlges $m/n > b$ racionális számot (m, n egészek, $n > 0$). Ekkor $|x|_1 = |y|_1^b < |y|_1^{\frac{m}{n}}$, és így $|x^n/y^m|_1 < 1$, amiből következik, hogy $k \to \infty$ esetén $|(x^n/y^m)^k|_1 \to 0$. De ekkor $|\ |_1$ és $|\ |_2$ ekvivalenciája miatt $|(x^n/y^m)^k|_2 \to 0$ is teljesül, amiből viszont következik, hogy $|x^n/y^m|_2 < 1$, és így $|x|_2 < |y|_2^{\frac{m}{n}}$. Mivel ez minden $m/n > b$ racionális szám esetén teljesül, ezért $|x|_2 \leq |y|_2^b$. Hasonlóképpen látható a másik irányú egyenlőtlenség is.

Ebből következik, hogy $|x|_2 = |y|_2^b = |y|_1^{ab} = |x|_1^a$, és ezt kellett bizonyítanunk. □

Legyen p egy tetszőleges prím. Jelölje ekkor valamilyen $a \in \mathbb{Q}^\times$ számra $\mathrm{ord}_p(a)$ a legnagyobb olyan m egész számot, amelyre $a \in p^m\mathbb{Z}_{(p)}$, ahol

$$\mathbb{Z}_{(p)} = \{m/n \in \mathbb{Q} | m, n \in \mathbb{Z}, p \nmid n\}.$$

Könnyen ellenőrizhető, hogy ekkor az $|r|_p = p^{-\mathrm{ord}_p(r)}$ függvény egy nemarkhimédeszi értékelés $\mathbb{Q}$-n. Ez az értékelést hívjuk *p-adikus értékelés*nek. A következő tétel szerint lényegében az összes nemarkhimédeszi értékelés $\mathbb{Q}$-n ilyen alakú.

3.1.3. Tétel (Ostrowski)**.** *Legyen $||$ egy tetszőleges nem triviális értékelés $\mathbb{Q}$-n. Ekkor*
(a) ha $||$ arkhimédeszi, akkor $||$ ekvivalens a szokásos abszolútértékkel,
(b) ha $||$ nemarkhimédeszi, akkor $||$ ekvivalens $|\,|_p$-vel valamelyik p prímre, és ez a p egyértelmű.

Bizonyítás. [4] 7.12. □

3.2. Telítések

3.2.1. Definíció. *Legyen K egy test és $||$ egy nem triviális értékelés K-n. A K testet* teljes*nek nevezzük, ha a $||$ értékelésből definiált metrika teljes K-n.*

3.2.2. Tétel. *Legyen K egy test és $||$ egy nem triviális értékelés K-n. Ekkor létezik olyan $(\hat{K}, ||)$ test, ami teljes és egy $K \to \hat{K}$ homomorfizmus, ami megőrzi az értékelést, és tetszőleges $(L, ||)$ teljes testre minden $K \to L$ homomorfizmus, ami megőrzi az értékelést kiterjed egyértelműen egy $\hat{K} \to L$ homomorfizmussá.*

Bizonyítás (vázlat).

A $\hat{K}$ test elemeit a szokásos módon a K elemeiből álló Cauchy-sorozatok ekvivalenciaosztályaiként definiálhatjuk, ahol az (a_n) és (b_n) sorozatok pontosan akkor ekvivalensek, ha $\lim_{n\to\infty} |a_n - b_n| = 0$. A műveleteket a természetes módon definiáljuk $\hat{K}$-n, és ekkor könnyen ellenőrizhető, hogy $\hat{K}$ valóban test lesz ezen műveletekkel. A K testből természetes módon adódik egy egy homomorfizmus $\hat{K}$-ba, ami minden $a \in K$ elemhez az $(a, a, a, ...)$ sorozatnak megfelelő elemet rendeli. Ha (a_n) egy K elemeiből álló Cauchy-sorozat, akkor a $||$ értékelésnek az ennek megfelelő $\hat{K}$-beli elemen felvett értékét $\lim_{n\to\infty} |a_n|$-nek definiáljuk. Könnyen látható, hogy ez jól definiált, $\hat{K}$-n valóban értékelés, és az előbbi homomorfizmus megőrzi az értékelést. Legyen most $(L, ||)$ egy tetszőleges teljes test, és egy $K \to L$ homomorfizmus, ami megőrzi az értékelést. Ekkor ez egyértelműen kiterjed egy $\hat{K} \to L$ olyan módon, hogy minden $\hat{K}$-beli elemhez hozzárendeljük egy őt reprezentáló (a_n) Cauchy-sorozat L-beli képének a határértékét L-ben. □

Az előbbi $\hat{K}$ testet a K testnek a $||$ értékelés szerinti *telítés*ének nevezzük. Jelöljük $\mathbb{Q}_p$-vel $\mathbb{Q}$-nak a p-adikus értékelés szerinti telítését. Ekkor tetszőleges $a \in \mathbb{Q}_p$ elemre $|a|_p = 0$ vagy $|a|_p = p^k$ alakú, ahol k valamilyen egész. Tegyük fel ugyanis, hogy $a \in \mathbb{Q}_p$-t reprezentálja az (a_n) sorozat. Ekkor $|a_n|_p \to |a|_p$, és így

$$|a|_p \in \mathrm{cl}(\{p^k | k \in \mathbb{Z}\} \cup \{0\}) = \{p^k | k \in \mathbb{Z}\} \cup \{0\}.$$

Legyen $\mathbb{Z}_p = \{a \in \mathbb{Q}_p | \, |a| \leq 1\}$. Ekkor $\mathbb{Z}_p$ elemei gyűrűt alkotnak, és $\mathbb{Z} \subset \mathbb{Z}_p$.

3.2.3. Állítás. *Legyen p prím, és legyen $S = \{0,1,...,p-1\}$. Ekkor minden $a_{-n}, a_{-n+1}, ... \in S$-re az*

$$s_m = \sum_{k=-n}^{m} a_k p^k$$

sorozat Cauchy-konvergens, és minden $\mathbb{Q}_p$-beli elem egyértelműen előáll egy ilyen sorozat határértékeként (azaz reprezentálja egy ilyen sorozat).

Bizonyítás. Legyen $s_m = \sum_{k=-n}^{m} a_k p^k$ ($a_i \in S$). Ekkor ha $m_1 > m_2 \geq N$, akkor $\mathrm{ord}_p(s_{m_2} - s_{m_1}) \geq m_2 \geq N$, így $|s_{m_2} - s_{m_1}|_p \leq p^{-N}$, ami bizonyítja, hogy az s_m sorozat Cauchy-konvergens.

Legyen most $\alpha \in \mathbb{Q}_p$ tetszőleges. Ha $\alpha = 0$, akkor készen vagyunk, ha $\alpha \neq 0$, akkor α előáll $\alpha = p^{-n}\alpha_0$ alakban, ahol $\alpha_0 \in \mathbb{Z}_p$. $\mathbb{Q}_p$ definíciója miatt létezik olyan $a_0' \in \mathbb{Q}$, hogy $|\alpha_0 - a_0'|_p \leq 1/p$, azaz $\alpha_0 - a_0' \in p\mathbb{Z}_p$. Ekkor $a_0' \in \mathbb{Z}_p$, azaz $\mathrm{ord}_p(a_0') \geq$ ≥ 0, amiből következik, hogy a_0' felírható $a_0' = \frac{x_0}{y_0}$ alakban, ahol $x_0, y_0 \in \mathbb{Z}$ és y_0 nem osztható p-vel. Válasszuk ekkor $a_0 \in S$-et úgy, hogy $x_0 - a_0 y_0$ osztható legyen p-vel, ekkor

$$\alpha_0 - a_0 = (\alpha_0 - a_0') + (a_0' - a_0) = (\alpha_0 - a_0') + \frac{x_0 - a_0 y_0}{y_0} \in p\mathbb{Z}_p \Rightarrow \frac{\alpha_0 - a_0}{p} \in \mathbb{Z}_p.$$

Ehhez hasonlóan válasszuk $a_1 \in S$-et úgy, hogy $\frac{\alpha_0 - a_0}{p} - a_1 \in p\mathbb{Z}_p$ teljesüljön, és így tovább az $a_2, a_3, ... \in S$ számokat definiáljuk úgy, hogy

$$\frac{\alpha_0 - a_0 - a_1 p - a_1 p^2 - ... - a_m p^m}{p^{m+1}} \in \mathbb{Z}_p$$

teljesüljön. Ekkor $|\alpha_0 - a_0 - a_1 p - a_2 p^2 - ... - a_m p^m|_p \leq p^{-m-1}$, és így az $s_m' =$ $= \sum_{k=0}^{m} a_k p^k$ sorozat tart α_0-hoz, és ekkor az s_m/p^n sorozat tart α-hoz.

Az egyértelműséghez elég belátni, hogy ha valamilyen $a_{-n}, a_{-n+1}, ... \in S$-re a $s_m = \sum_{k=-n}^{m} a_k p^k$ sorozat tart 0-hoz, akkor $a_i = 0$ minden $i = -n, -n+1, ...$-re. Ez pedig teljesül, hiszen ha a_j nem lenne 0 valamilyen j-ra, akkor $m > j$ esetén $|s_m|_p = p^{-j}$ állna, és ekkor s_m nem tarthatna 0-hoz. □

A 3.2.3 állítás szerint $\mathbb{Q}_p$ elemeire gondolhatunk úgy, mint valamilyen $\sum_{k=-n}^{\infty} a_k p^k$

alakú formális összegekre, ahol $a_i \in \{0,1,2,...,p-1\}$. Egy ilyen összeg pontosan akkor lesz benne $\mathbb{Z}_p$-ben, ha a negatív indexű tagok együtthatói mind 0-k.

3.3. $\mathbb{Z}_p$ kompaktsága

3.3.1. Definíció (Inverz limesz gyűrűkre)**.** *Legyenek R_i gyűrűk és $\varphi_i : R_{i+1} \to R_i$ gyűrűhomomorfizmusok minden $i = 1,2,...$-re. Tekintsük most azon*

$$r = (r_1, r_2, ...) \in \prod_{i=1}^{\infty} R_i$$

elemeket, amikre $\varphi_i(r_{i+1}) = r_i$ minden i-re. Ezen elemek részgyűrűt alkotnak $\prod_{i=1}^{\infty} R_i$-ben. Ezt a részgyűrűt az R_i gyűrűk inverz limesz*ének nevezzük, és $\varprojlim R_i$-vel jelöljük.*

Tekintsük most valamilyen p prímre a $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z}$, $\mathbb{Z}/p^3\mathbb{Z}$, ... gyűrűket a természetes módon adódó $\varphi_i : \mathbb{Z}/p^{i+1}\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ homomorfizmusokkal. Ekkor ezen gyűrűk inverz limesze azon $a \in \prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$ elemekből áll, amik felírhatóak

$$a = (a_0 + (p), a_0 + a_1p + (p^2), a_0 + a_1p + a_2p^2 + (p^3), ...)$$

alakban, ahol $a_i \in \{0,1,2,...,p-1\}$ minden i-re. Tekintsük azt a megfeleltetést, ami egy, az előbbi alakban felírt a elemhez az $a_0 + a_1p + a_2p^2 + ... \in \mathbb{Z}_p$ elemet rendeli. Könnyen látható, hogy ez a megfeleltetés egy izomorfizmus az $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ és a $\mathbb{Z}_p$ gyűrűk között. A továbbiakban ezeket a gyűrűket azonosítjuk egymással. Mint ahogyan azt már láttuk $\mathbb{Z}_p$ ellátható egy természetes topológiával (amit a p-adik értékelés definiál rajta). Ennek a topológiának egy bázisa a

$$\mathcal{B} = \{B \subset \mathbb{Z}_p | \exists b_0, b_1, ..., b_n \in \{0,1,2,...,p-1\} (B = \{\sum_{i=0}^{\infty} a_i p^i | \forall i \leq n (a_i = b_i)\})\}$$

halmaz. Azonban $\mathbb{Z}_p$-n egy topológiát máshogy is definiálhatunk az inverz limeszes definíció segítségével. Tekintsük ugyanis a $\mathbb{Z}/p^i\mathbb{Z}$ gyűrűkön a diszkrét topológiát minden i-re, és tekintsük ekkor a $\prod_{i=1}^{\infty}(\mathbb{Z}/p^i\mathbb{Z})$ szorzattéren a szorzattopológiát, és ennek a $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ részhalmazán a megfelelő altértopológiát. Könnyen látható, hogy ennek a topológiának is bázisa az előbbi $\mathcal{B}$ halmaz, ami azt jelenti, hogy a két topológia megegyezik $\mathbb{Z}_p$-n. Ezt a topológiát *p-adikus topológiá*nak nevezzük.

3.3.2. Tétel. *Tetszőleges p prímre $\mathbb{Z}_p$ kompakt (az előbbi topológia szerint).*

Bizonyítás. $\mathbb{Z}/p^i\mathbb{Z}$ kompakt minden $i = 1,2,...$-re, mert véges, így a Tyihonov-tétel szerint $\prod_{i=1}^{\infty}(\mathbb{Z}/p^i\mathbb{Z})$ is kompakt. Ezért elég belátni, hogy $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ zárt altere ennek a szorzattérnek.

Tegyük fel, hogy $r_n = (r_{n1}, r_{n2}, r_{n3}, ...) \in \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ minden n-re és $\lim_{n\to\infty} r_n = r = (r_1, r_2, r_3, ...)$. Ekkor minden i-re r_{ni} is tart r_i-hez, ami ezesetben azt jelenti, hogy $r_{ni} = r_i$, ha n nagyobb, mint valamilyen $N(i)$ szám. Ebből következik, hogy tetszőleges i-re ha $n > \max(N(i), N(i+1))$, akkor $\varphi(r_{i+1}) = \varphi(r_{n(i+1)}) = r_{ni} = r_i$, ami éppen azt jelenti, hogy $r \in \varprojlim \mathbb{Z}/p^i\mathbb{Z}$. Tehát $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ valóban zárt altere a szorzattérnek. □

3.4. Hensel-lemma

3.4.1. Lemma. *Legyen $f(X_1, X_2, ...X_n) \in \mathbb{Z}_p[X_1, X_2, ..., X_n]$, és tegyük fel, hogy az $a_1, a_2, ..., a_n \in \mathbb{Z}$ számokra, és valamilyen m nemnegatív és r pozitív egész számra*

$$f(a_1, a_2, ..., a_n) \equiv 0 \mod p^{2m+r},$$

de valamilyen i-re

$$\frac{\partial f}{\partial X_i}(a_1, a_2, ..., a_n) \not\equiv 0 \mod p^{m+r}.$$

Ekkor léteznek olyan $b_1, b_2, b_3, ..., b_n \in \mathbb{Z}$ számok, amikre $b_i \equiv a_i \mod p^{m+r}$ teljesül minden i-re, és

$$f(b_1, b_2, ..., b_n) \equiv 0 \mod p^{2m+r+1}.$$

Bizonyítás. Nyilván feltehető, hogy $a_1 = a_2 = ... = a_n = 0$. Ekkor az f polinom felírható

$$f(X_1, X_2, X_3, ..., X_n) = f(0,0, ...,0) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(0,0, ...,0)X_i + \sum_{k=2}^{m} F_k(X_1, X_2, ..., X_n)$$

alakban, ahol $k \geq 2$-re F_k valamilyen k-adfokú homogén polinom. A b_i számokat $h_i p^{m+r}$ alakban keressük, ahol a h_i számok valamilyen alkalmas egészek lesznek. A h_i számok tetszőleges megválasztása esetén $F_k(h_1 p^{m+r}, h_2 p^{m+r}, ..., h_n p^{m+r})$ osztható p^{2m+r}-rel, ha $k \geq 2$, így az állításhoz elég olyan h_i-ket találni, hogy

$$f(0,0, ...,0) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(0,0, ...,0)h_i p^{m+r}$$

osztható legyen p^{2m+r+1}-gyel. A feltétel szerint létezik olyan $0 \leq k < m + r$, hogy $\frac{\partial f}{\partial X_i}(0,0, ...,0)$ osztható p^k-val minden i-re, de van olyan i, amire $\frac{\partial f}{\partial X_i}(0,0, ...,0)$ már nem osztható p^{k+1}-gyel. Ekkor a h_i számok választhatóak úgy, hogy

$$\frac{f(0,0, ...,0)}{p^{k+m+r}} + \sum_{i=1}^{n} \frac{\frac{\partial f}{\partial X_i}(0,0, ...,0)}{p^k} h_i$$

oszható legyen p^{m+1-k}-val, és ekkor ezt azt oszthatóságot p^{k+m+r}-rel megszorozva látható, hogy ezek a h_i-k jók lesznek. □

3.4.2. Tétel (Hensel-lemma)**.** *A 3.4.1 lemma feltételei mellett léteznek olyan* $b_1, b_2, ..., b_n \in \mathbb{Z}_p$ *számok, amikre* $b_i \equiv a_i \mod p^{m+r}$ *teljesül minden* i*-re, és*

$$f(b_1, b_2, ..., b_n) = 0.$$

Bizonyítás. A 3.4.1 lemma szerint léteznek olyan $a_{11}, a_{21}, ..., a_{n1} \in \mathbb{Z}$ számok, hogy $a_{i1} \equiv a_i \mod p^{m+r}$ minden i-re, és $f(a_{11}, a_{21}, ..., a_{n1}) \equiv 0 \mod p^{2m+r+1}$. Az első kongruenciából következik, hogy minden i-re

$$\frac{\partial f}{\partial X_i}(a_{11}, a_{21}, ..., a_{n1}) \equiv \frac{\partial f}{\partial X_i}(a_1, a_2, ..., a_n) \mod p^{m+r},$$

amiből következik, hogy valamilyen i-re

$$\frac{\partial f}{\partial X_i}(a_{11}, a_{21}, ..., a_{n1}) \not\equiv 0 \mod p^{m+r+1},$$

és így a 3.4.1 lemmát r helyett $r+1$-re alkalmazva azt kapjuk, hogy léteznek olyan $a_{12}, a_{22}, ..., a_{n2} \in \mathbb{Z}$ számok, hogy $a_{i2} \equiv a_{i1} \mod p^{m+r+1}$ minden i-re, és $f(a_{12}, a_{22}, ..., a_{n2}) \equiv 0 \mod p^{2m+r+2}$. Ezt az eljárást folytatva megadhatunk olyan $a_{i1}, a_{i2}, a_{i3}, ...$ sorozatokat minden $i = 1,2, ..., n$-re, hogy minden k-ra $a_{i(k+1)} \equiv a_{ik} \mod p^{m+r+k}$ teljesül minden i-re és

$$f(a_{1k}, a_{2k}, ..., a_{nk}) \equiv 0 \mod p^{2m+r+k}.$$

Ekkor minden i-re, ha $k_1 > k_2 \geq k$, akkor $p^{m+r+k} | a_{ik_1} - a_{ik_2} \Rightarrow |a_{ik_1} - a_{ik_2}|_p \leq$ $\leq p^{-(m+r+k)}$. Ebből következik, hogy az a_{ik} sorozat Cauchy-konvergens, tehát konvergens $\mathbb{Z}_p$-ben. Legyen $\lim_{k\to\infty} a_{ik} = b_i$ minden i-re. Azt állítjuk, hogy ezek a b_i-k jók lesznek. Könnyen látható, hogy $b_i \equiv a_i \mod p^{m+r}$ teljesül minden i-re. Mivel az $f : \mathbb{Z}_p^n \to \mathbb{Z}_p$ függvény folytonos (a p-adikus topológiára nézve), ezért

$$|f(b_1, b_2, ..., b_n)|_p = |f(\lim_{k\to\infty} a_{1k}, \lim_{k\to\infty} a_{2k}, ..., \lim_{k\to\infty} a_{nk})|_p =$$
$$= |\lim_{k\to\infty} f(a_{1k}, a_{2k}, ..., a_{nk})|_p = 0,$$

tehát $f(b_1, b_2, ..., b_n) = 0$. □

3.5. A p-adikus értékelések kiterjesztése $\mathbb{Q}_p$ véges bővítéseire

3.5.1. Definíció. *Legyen* K *tetszőleges test. Ekkor a* K*-n értelmezett nemarkhimédeszi* $||$ *értékelést* diszkrét*nek nevezzük, ha a* $\{|x| \, | x \in K^\times\}$ *halmaz diszkrét részhalmaza* $\mathbb{R}$*-nek (azaz minden pontja izolált pont).*

3.5.2. Definíció. *Legyen K tetszőleges test, és legyen L egy véges szeparábilis bővítése K-nak. Ekkor tetszőleges $\alpha \in L$ elemre az $x \mapsto \alpha x$ egy $L \to L$ K-lineáris transzformáció. Ennek a transzformációnak a determinánsát az $\alpha \in L$ elem* normájának *nevezzük, és $\mathrm{Nm}_{L/K}(\alpha)$-val jelöljük. (Erről tudjuk, hogy független a bázis megválasztásától.)*

A definícióból könnyen látható, hogy tetszőleges $\beta_1, \beta_2 \in L$ esetén

$$\mathrm{Nm}_{L/K}(\beta_1\beta_2) = \mathrm{Nm}_{L/K}(\beta_1)\,\mathrm{Nm}_{L/K}(\beta_2).$$

Ha $\alpha \in K$, akkor a definícióban szereplő lineáris transzformáció mátrixa αI alakú tetszőleges bázisban, ekkor tehát $\mathrm{Nm}_{L/K}(\alpha) = \alpha^n$, ahol $n = \deg(L/K)$.

3.5.3. Tétel. *Legyen p tetszőleges prím, és legyen K $\mathbb{Q}_p$ egy véges bővítése, a $K/\mathbb{Q}_p$ bővítés fokát jelöljük n-nel. Ekkor egyértelműen létezik olyan K-n értelmezett $||$ diszkrét értékelés, ami kiterjeszti $|\,|_p$-t. Erre a $||$ értékelésre nézve a K test teljes, és tetszőleges $\beta \in K$-ra*

$$|\beta| = |\,\mathrm{Nm}_{K/\mathbb{Q}_p}(\beta)|_p^{1/n}.$$

Bizonyítás. [4] 7.38. □

4. Elliptikus görbék torziópontjai

A fejezet elején definiáljuk és megvizsgáljuk egy elliptikus görbe különböző típusú redukcióit. Ezután belátunk néhány állítást $\mathbb{Q}_p$ feletti elliptikus görbékre, amiknek a felhasználásával $\mathbb{Q}$ feletti elliptikus görbék torziópontjaira vonatkozó tételeket kapunk. A fejezet végén belátjuk a Lutz–Nagell-tételt, és ennek felhasználásával vázolunk egy algoritmust, amivel egy $\mathbb{Q}$ feletti elliptikus görbe torziórészcsoportja kiszámítható.

4.1. Redukciók

Legyen K egy test, és $||$ egy nem triviális diszkrét értékelés K-n. Tekintsük ekkor az

$$A := \{x \in K | |x| \leq 1\} \text{ és } M := \{x \in K | |x| < 1\}$$

gyűrűket K-ban. Azt állítjuk, hogy A egyetlen maximális ideálja M. Az, hogy M ideál A-ben triviális. Azt állítjuk, hogy $A^\times = A \setminus M$, ebből már következik az előbbi állítás. Nyilván $A^\times \cap M = \emptyset \Rightarrow A^\times \subset A \setminus M$. Legyen most $a \in A \setminus M$ tetszőleges, ekkor $|a| = 1 \Rightarrow |a^{-1}| = 1 \Rightarrow a^{-1} \in A \Rightarrow a \in A^\times$. Tehát $A \setminus M \subset A^\times$ is teljesül. Legyen most $k := A/M$. Mivel M maximális ideál A-ben, ezért k test. Ezt a testet nevezzük a $||$ értékeléshez tartozó *maradéktest*nek. Tetszőleges $t \in A$ elemre jelöljük $\bar{t}$-sal t képét a természetes $A \to k$ homomorfizmusnál. Amennyiben $K = \mathbb{Q}$ vagy $K = \mathbb{Q}_p$, és $|| = |\,|_p$ (a p-adikus értékelés), akkor rendre $A = \mathbb{Z}$ és $M = p\mathbb{Z}$, illetve $A = \mathbb{Z}_p$ és $M = p\mathbb{Z}_p$. Mindkét esetben $k \simeq \mathbb{F}_p$, és $\bar{t} = t \bmod p$.

Tekintsük most az $E : Y^2Z = X^3 + aX^2Z + bZ^3$ görbét, ahol $a, b \in A$, és $\Delta = = 4a^3 + 27b^2 \neq 0$. Ekkor a 2.3.1 állítás szerint E nem szinguláris, és az $O = (0 : 1 : 0)$ pont inflexiós pontja E-nek, tehát (E, O) egy elliptikus görbe. Jelöljük ekkor $\bar{E}$-sal az

$$\bar{E} : Y^2Z = X^3 + \bar{a}X^2Z + \bar{b}Z^3$$

k test feletti görbét. Ezt az $\bar{E}$ görbét az E görbének a $||$ értékeléshez tartozó (vagy modulo M) *redukció*jának nevezzük. Tekintsük most a következő

$$P \mapsto \bar{P} : \mathbf{P}^2(K) \to \mathbf{P}^2(k)$$

*redukciós leképezés*t: tetszőleges $P \in \mathbf{P}^2(K)$ pontnak tekintsük egy olyan $(x : y : z)$ reprezentását, amire $\max\{|x|, |y|, |z|\} = 1$, és legyen ekkor $\bar{P} := (\bar{x} : \bar{y} : \bar{z})$. Ez a definíció értelmes, hiszen $\max\{|x|, |y|, |z|\} = 1$ miatt $x \in A^\times$, $y \in A^\times$ vagy $z \in A^\times$, és így $(x, y, z) \neq (0{,}0{,}0)$, továbbá tetszőleges $a \in A^\times$ esetén

$$(\bar{a}\bar{x} : \bar{a}\bar{y} : \bar{a}\bar{z}) = (\bar{x} : \bar{y} : \bar{z}).$$

Könnyen látható, hogy ezen jelölések mellett $P \in E(K)$ esetén $\bar{P} \in \bar{E}(k)$. A redukcióknak az alábbi típusai léteznek.

4.1.1. Definíció. *(a) Ha az előbb definiált $\bar{E}$ görbe nem szinguláris, akkor azt mondjuk, hogy E-nek* jó redukció*ja van (mod M).*
(b) Ha $\bar{E}$ szinguláris, és $\bar{E}$-nek cuspja van, akkor azt mondjuk, hogy E-nek additív redukció*ja van.*
(c) Ha $\bar{E}$ szinguláris, és $\bar{E}$-ek node-ja van, akkor azt mondjuk, hogy E-nek multiplikatív redukciója *van. Egy multiplikatív redukciót* szétes*őnek nevezünk, ha a $\bar{E}$ görbének a szinguláris pontjához tartozó érintő egyeneseinek az egyenleteinek együtthatói k-ban vannak.*

4.1.2. Állítás. *Az előbbi jelölések mellett az alábbiak teljesülnek:*
(a) Az E görbének pontosan akkor van jó redukciója (mod M), ha $\Delta \notin M$, és $\operatorname{char} k \neq 2$.
(b) $\operatorname{char} k \neq 2,3$ *esetén az E görbének akkor pontosan van additív redukciója, ha $\Delta \in M$ és $-2ab \in M$. Ebben az eseben $\bar{E}(k)^{\mathrm{ns}} \simeq k^{+}$.*
(c) $\operatorname{char} k \neq 2,3$ *esetén az E görbének pontosan akkor van szétes̋ multiplikatív redukciója, ha $\Delta \in M$, $-2ab \notin M$ és $\sqrt{-2\overline{ab}} \in k$. Ebben az esetben $\bar{E}(k)^{\mathrm{ns}} \simeq k^{\times}$.*
(d) $\operatorname{char} k \neq 2,3$ *esetén az E görbének pontosan akkor van nem szétes̋ multiplikatív redukciója, ha $\Delta \in M$, $-2ab \notin M$ és $\sqrt{-2\overline{ab}} \notin k$. Ebben az esetben $\bar{E}(k)^{\mathrm{ns}} \simeq$ $\simeq \mathbb{G}_m[\sqrt{-2\overline{ab}}](k)$.*

Bizonyítás. (a) A 2.3.1 állítás szerint az $\bar{E}$ görbe pontosan akkor nem szinguláris, ha $\operatorname{char} k \neq 2$ és $4\bar{a}^3 + 27\bar{b}^2 \neq 0$. Az utóbbi feltétel ekvivalens azzal, hogy $\Delta = 4a^3 + 27b^2 \notin M$.

(b) A 2.3 fejezetben láttuk, hogy ha $\bar{E}$ szinguláris, akkor $\bar{E}$-nek pontosan akkor van cuspja, ha $\bar{a} = 0$ vagy $\bar{b} = 0$, azaz $ab \in M$.

(c), (d) A 2.3 fejezetben láttuk, hogy ha $\bar{E}$ szinguláris, akkor $\bar{E}$-nek pontosan akkor van node-ja, ha $\bar{a}, \bar{b} \neq 0$, azaz $ab \notin M$, és ekkor $\bar{E}$ szinguláris pontjához tartozó érintő egyenesének egyenletének együtthatói pontosan akkor vannak k-ban, ha $\sqrt{-\frac{9}{2}\frac{\bar{a}}{\bar{b}}} \in k \Leftrightarrow \sqrt{-2\overline{ab}} \in k$.

Az állításban szereplő izomorfizmusok a 2.3 fejezet végén leírt izomorfizmusokból adódnak. □

Ha $K = \mathbb{Q}_p$, és E-nek jó vagy multiplikatív redukciója van, és a K testet lecseréljük K valamilyen véges bővítésére, akkor E-nek továbbra is ugyanolyan típusú redukciója lesz, ez azonban nem teljesül, ha E-nek additív redukciója van. Általánosabban a következő tétel igaz.

4.1.3. Tétel. *Legyen K $\mathbb{Q}_p$ egy véges bővítése valamilyen p prímre, és legyen (E, O) egy elliptikus a görbe az előbbi jelölések szerint. Ekkor a következők teljesülnek:*
(a) Legyen L a K test egy véges bővítése. Ekkor ha E-nek, mint K feletti elliptikus görbének jó vagy multiplikatív redukciója van, akkor ugyanolyan típusú redukciója van E-nek, mint L feletti elliptikus görbének.
(b) Létezik olyan L véges bővítése K-nak, hogy E-nek, mint L feletti elliptikus görbének jó vagy (széteső) multiplikatív redukciója van.

Az előbbi tételben a redukciókat mindig azon (a 3.5.3 tétel szerint egyértelműen létező) $||$ diszkrét értékelés szerint tekintjük, ami kiterjeszti $|\,|_p$-t.

Bizonyítás. [8] VII. 5.4. □

4.2. Elliptikus görbék $\mathbb{Q}_p$ felett

Legyen p tetszőleges prím, és tekintsük az

$$E : Y^2Z = X^3 + aX^2Z + bZ^3$$

görbét, ahol $a, b \in \mathbb{Q}_p$, és $\Delta = 4a^3 + 27b^2 \neq 0$. Ekkor (mint láttuk) (E, O) egy elliptikus görbe, ahol $O = (0 : 1 : 0)$. Legyen $c \in \mathbb{Q}_p^\times$ tetszőleges, ekkor az

$$(X, Y, Z) \mapsto (X/c^2, Y/c^3, Z)$$

lineáris transzformáció az O pontot fixen hagyja, és E-t az

$$E' : Y^2Z = X^3 + a'X^2Z + b'Z^3$$

görbébe viszi, ahol $a' = c^4a, b' = c^6b$. A c szám megfelelő választása mellett elérhető, hogy a' és b' $\mathbb{Z}_p$-ben legyenek. Ebből következik, hogy E-nek az előbbi egyenletében $a, b \in \mathbb{Z}_p$ feltehető, a továbbiakban ezt mindig feltesszük. Amennyiben az $E(\mathbb{Q})$ jelölést használjuk, akkor feltesszük, hogy $a, b \in \mathbb{Z}$ is teljesül. Legyen $\bar{E}$ az E görbe redukciója modulo p, és egy $P \in E(\mathbb{Q}_p)$ pont képét az $E(\mathbb{Q}_p) \to \bar{E}(\mathbb{F}_p)$ redukciós leképezésnél jelöljük $\bar{P}$-sal.

Legyen ekkor

$$E^0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) | \bar{P} \text{ nem szinguláris pontja } \bar{E}\text{-nek}\}.$$

Ekkor $O \in E^0(\mathbb{Q}_p)$, és ha $P, Q \in E^0(\mathbb{Q}_p)$, akkor $\bar{P}$ és $\bar{Q}$ nem szinguláris pontjai $\bar{E}(\mathbb{F}_p)$-nek, és így (a 2.1 fejezet jelöléseit használva) $\overline{PQ} = \bar{P}\bar{Q}$ sem szinguláris, amiből következik, hogy $PQ \in E^0(\mathbb{Q}_p)$. Ebből következik, hogy $E^0(\mathbb{Q}_p)$ nem üres, és $P, Q \in E^0(\mathbb{Q}_p)$ esetén $P + Q = O(PQ) \in E^0(\mathbb{Q}_p)$, és $-P = P(OO) \in E^0(\mathbb{Q}_p)$, tehát $E^0(\mathbb{Q}_p)$ részcsoportja $E(\mathbb{Q}_p)$-nek.

Jelöljük $\bar{E}^{\mathrm{ns}}(\mathbb{F}_p)$-vel $\bar{E}(\mathbb{F}_p)$ nem szinguláris pontjainak halmazát. Ekkor $\bar{E}^{\mathrm{ns}}(\mathbb{F}_p)$ pontjai is csoportot alkotnak a szokásos csoportművelettel, és a $P \mapsto \bar{P}$ redukciós leképezés egy $E^0(\mathbb{Q}_p) \to \bar{E}^{\mathrm{ns}}(\mathbb{F}_p)$ homomorfizmus. Ennek a homomorfimzusnak a magját jelöljük $E^1(\mathbb{Q}_p)$-vel. Ekkor $E^1(\mathbb{Q}_p)$ pontosan azon P pontokból áll, aminek létezik olyan $(x : y : z)$ reprezentációja, ahol $x, y, z \in \mathbb{Z}_p$, x és z osztható p-vel, és y nem osztható p-vel. Ebből speciálisan következik, hogy $(x : y : z) \in E^1(\mathbb{Q}_p)$ esetén $y \neq 0$. Definiáljuk ekkor az $E^1(\mathbb{Q}_p) \supset E^2(\mathbb{Q}_p) \supset E^3(\mathbb{Q}_p) \supset ...$ sorozatot a következőképpen.

4.2.1. Definíció. *Tetszőleges $n \geq 1$ egész esetén legyen*

$$E^n(\mathbb{Q}_p) := \{(x : y : z) \in E^1(\mathbb{Q}_p) | \, \frac{x}{y} \in p^n\mathbb{Z}_p\}.$$

Az előbbi megállapítás miatt $n = 1$ esetén visszakapjuk a korábbi definíciónkat $E^1(\mathbb{Q}_p)$-re.

Az $E(\mathbb{Q}_p)$ görbén definiálható egy topológia a következőképpen:
Tekintsük $\mathbb{Q}_p$-n a p-adikus topológiát, $\mathbb{Q}_p \times \mathbb{Q}_p \times \mathbb{Q}_p$-n a szorzattopológiát, $\mathbb{Q}_p^3 \setminus \{0\}$-n az ebből adódó altértopológiát, és $\mathbf{P}^2(\mathbb{Q}_p)$-n a természetes $\mathbb{Q}_p^3 \setminus \{0\} \to \mathbf{P}^2(\mathbb{Q}_p)$ faktorleképezésből adódó faktortopológiát. $E(\mathbb{Q}_p) \subset \mathbf{P}^2(\mathbb{Q}_p)$, és így $E(\mathbb{Q}_p)$-n tekinthetjük a megfelelő altértopológiát. Azt állítjuk, hogy $E(\mathbb{Q}_p)$ kompakt ezen topológia szerint.

$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p = \{u \in \mathbb{Z}_p | \, |u|_p = 1\}$ kompakt, mert ez $\mathbb{Z}_p$ zárt altere, és $\mathbb{Z}_p$ kompakt. Ebből következik, hogy $\mathbb{Z}_p^\times \times \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p^\times \times \mathbb{Z}_p$ és $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p^\times$ kompakt részhalmazai $\mathbb{Q}_p^3 \setminus \{0\}$-nak. Ekkor ezen halmazoknak a faktorleképezésnél vett képei is kompaktak. Ezekről a képhalmazokról azonban könnyen látható, hogy nyíltak is, és hogy lefedik $\mathbf{P}^2(\mathbb{Q}_p)$-t. Azt kaptuk tehát, hogy $\mathbf{P}^2(\mathbb{Q}_p)$ előáll véges sok kompakt, nyílt halmaz uniójaként, tehát kompakt. Az $E(\mathbb{Q}_p)$ halmaz zárt $\mathbf{P}^2(\mathbb{Q}_p)$-ben, hiszen ez egy polinom gyökeinek halmaza, tehát ez is kompakt.

4.2.2. Állítás. *$E(\mathbb{Q}_p)$ topologikus csoport az előbbi topológia szerint.*

Bizonyítás. Ehhez az állításhoz elég belátni, hogy (a 2.1 fejezet jelöléseit használva) a

$$(P, Q) \mapsto PQ : E(\mathbb{Q}_p) \times E(\mathbb{Q}_p) \to E(\mathbb{Q}_p)$$

leképezés folytonos.

Legyen $U_2 = \{(x : y : z) \in \mathbf{P}^2(\mathbb{Q}_p) | z \neq 0\}$. Könnyen látható, hogy ekkor $E(\mathbb{Q}_p) \cap$ $\cap \, U_2 = E(\mathbb{Q}_p) \setminus \{O\}$. Tekintsük most az

$$E_2 : Y^2 = X^3 + aX + b$$

affin görbét. Ekkor minden $P = (x : y : z) \in E(\mathbb{Q}_p) \setminus \{O\}$ pontot megfeleltethetünk a $P' = (x'(P), y'(P)) \in E_2(\mathbb{Q}_p)$ ponttal, ahol $x'(P) = \frac{x}{z}$ és $y'(P) = \frac{y}{z}$. Először

belátjuk, hogy a $(P,Q) \mapsto PQ$ leképezés folytonos a

$$H = \{(P,Q) \in E(\mathbb{Q}_p) \times E(\mathbb{Q}_p) | P, Q, P+Q, P-Q \neq O\}$$

halmazon.

Tegyük fel ugyanis, hogy $(P,Q) \in H$. Ekkor $x'(P) \neq x'(Q)$, így a P' és a Q' pontokat összekötő egyenes egyenlete $Y = \alpha X + \beta$ alakú, ahol $\alpha = \frac{y'(P)-y'(Q)}{x'(P)-x'(Q)}$, és ekkor az

$$(\alpha X + \beta)^2 = X^3 + aX + b \Leftrightarrow X^3 - \alpha^2 X^2 + (a - 2\alpha\beta)X + (b - \beta^2) = 0$$

egyenlet megoldásai éppen $x'(P)$, $x'(Q)$ és $x'(PQ)$. Ebből következik, hogy

$$x'(PQ) = \alpha^2 - x'(P) - x'(Q),$$

ami (P,Q)-nak folytonos függvénye. Hasonlóan $y'(PQ)$ is folytonos függvénye (P,Q)-nak, tehát PQ is folytonos függvénye.

Mivel H sűrű, és azt már tudjuk, hogy a $(P,Q) \mapsto PQ$ leképezés folytonos H-n, ezért ennek a leképezésnek a folytonosságához elég lenne látni, hogy tetszőleges $(P,Q) \in (E(\mathbb{Q}_p) \times E(\mathbb{Q}_p)) \setminus H$ pontra, ha $(P_i, Q_i) \in H$, és $P_i \to P, Q_i \to Q_i$, akkor $(P_i Q_i) \to (PQ)$.

Legyen most $P \in E(\mathbb{Q}_p)$ tetszőleges, és legyen P_i egy P-hez tartó sorozat, amire $P_i \neq P, -P, O, O-P$. Ekkor $\alpha_i = \frac{y'(P)-y'(Q_i)}{x'(P)-x'(Q_i)}$ tart az E_2 görbe P pont beli érintőjének meredekségéhez, így könnyen látható, hogy ekkor $(PP_i) \to (PP)$ is teljesül.

Meggondolható, hogy tetszőleges $P_n \in E(\mathbb{Q}_p) \setminus \{O\}$ sorozat esetén

$$\lim_{n\to\infty} P_n = O \Leftrightarrow \lim_{n\to\infty} \mathrm{ord}_p(y'(P)) = -\infty.$$

Ezt használva a többi eset is könnyen ellenőrizhető. □

4.2.3. Tétel. *Az imént definiált* $E(\mathbb{Q}_p) \supset E^0(\mathbb{Q}_p) \supset E^1(\mathbb{Q}_p) \supset E^2(\mathbb{Q}_p) \supset ... \supset E^n(\mathbb{Q}_p) \supset ...$ *sorozatra a következők teljesülnek:*
(a) $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ *véges;*
(b) A $P \mapsto \bar{P}$ *leképezés egy* $E^0(\mathbb{Q}_p)/E^1(\mathbb{Q}_p) \to \bar{E}^{\mathrm{ns}}(\mathbb{F}_p)$ *izomorfizmust definiál;*
(c) $n \geq 1$ *esetén* $E^n(\mathbb{Q}_p)$ *részcsoportja* $E(\mathbb{Q}_p)$*-nek és az* $(x:y:z) \mapsto p^{-n}\frac{x}{y} \mod p$ *leképezés egy* $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \to \mathbb{F}_p^+$ *izomorfizmus;*
(d) $\bigcap_{n=0}^{\infty} E^n(\mathbb{Q}_p) = \{O\}$.

Bizonyítás. (a) Az előbbi topológia szerint $E^0(\mathbb{Q}_p)$ nyílt részcsoportja $E(\mathbb{Q}_p)$-nek, hiszen két közeli $\mathbf{P}^2(\mathbb{Q}_p)$-beli pont redukciója megegyezik. Ebből következik $E(\mathbb{Q}_p)$ kompaktsága miatt, hogy $E^0(\mathbb{Q}_p)$-nak csak véges sok mellékosztálya lehet $E(\mathbb{Q}_p)$-ben.

(b) Legyen $\tilde{P} = (\bar{x} : \bar{y} : \bar{z}) \in \bar{E}^{\mathrm{ns}}(\mathbb{F}_p)$ tetszőleges. Ekkor $f(x, y, z) \equiv 0 \mod p$, ahol

$$f(X, Y, Z) := Y^2Z - X^3 - aX^2Z - bZ^3.$$

Mivel $\tilde{P}$ nem szinguláris pontja $\bar{E}(\mathbb{F}_p)$-nek, ezért a $\frac{\partial f}{\partial X}(x, y, z)$, $\frac{\partial f}{\partial Y}(x, y, z)$, $\frac{\partial f}{\partial Z}(x, y, z)$ parciális deriváltak valamelyike nem osztható p-vel. Ekkor a Hensel-lemmát (3.4.2 tétel) alkalmazva (az $m = 0$, $r = 1$ esetben) azt kapjuk, hogy van olyan $x', y', z' \in \in \mathbb{Z}_p$, hogy $x' \equiv x$, $y' \equiv y$, $z' \equiv z \mod p$, és $F(x', y', z') = 0$. Ekkor azonban $P' = (x' : y' : z') \in E(\mathbb{Q}_p)$, és $\bar{P'} = \tilde{P}$. $\bar{P'} \in \bar{E}^{\mathrm{ns}}(\mathbb{F}_p)$ miatt $P' \in E^0(\mathbb{Q}_p)$. Tehát a $P \mapsto \bar{P} : E^0(\mathbb{Q}_p) \to \bar{E}^{\mathrm{ns}}(\mathbb{F}_p)$ leképezés szürjektív, ami éppen azt jelenti, hogy állításban szereplő leképezés izomorfizmus.

(c) Az állítást n szerint indukcióval bizonyítjuk, tegyük fel, hogy $E^n(\mathbb{Q}_p)$-ről már tudjuk, hogy részcsoportja $E(\mathbb{Q}_p)$-nek, ekkor belátjuk, hogy $E^{n+1}(\mathbb{Q}_p)$ is részcsoportja $E(\mathbb{Q}_p)$-nek, és hogy az állításban szereplő $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \to \mathbb{F}_p^+$ leképezés izomorfizmus. Ha $(x : y : 1) \in E^1(\mathbb{Q}_p)$, akkor $y \notin \mathbb{Z}_p$. Legyenek ekkor $x = p^{-m}x_0$ és $y = p^{-m'}y_0$, ahol $x_0, y_0 \in \mathbb{Z}_p^\times$. Ekkor tehát $m' \geq 1$, és

$$p^{-2m'}y_0^2 = p^{-3m}x_0^3 + ap^{-m}x_0 + b.$$

$\mathrm{ord}_p(p^{-2m'}y_0^2) = -2m'$, és ha $m \geq 1$, akkor $\mathrm{ord}_p(p^{-3m}x_0^3 + ap^{-m}x_0 + b) = -3m$, egyébként pedig nemnegatív ez az érték. Mivel ennek a két értéknek meg kell egyeznie, ezért m szükségképpen pozitív, és ekkor $2m' = 3m$. Mivel m, m' egészek, ezért ebből következik, hogy létezik olyan $k \geq 1$ egész, hogy $m = 2k, m' = 3k$, és ekkor $\mathrm{ord}_p(\frac{x}{y}) = k$. Az előbbi megfigyelésből következik, hogy amennyiben

$$P = (x : y : z) \in E^n(\mathbb{Q}_p) \setminus E^{n+1}(\mathbb{Q}_p),$$

akkor $\mathrm{ord}_p x = \mathrm{ord}_p z - 2n$ és $\mathrm{ord}_p y = \mathrm{ord}_p z - 3n$.

Legyen most P egy tetszőleges pontja $E^n(\mathbb{Q}_p)$-nek. Ekkor az előbbiek szerint a P pont előáll valamilyen $P = (p^n x_0, y_0, p^{3n} z_0)$ alakban, ahol $x_0, z_0 \in \mathbb{Z}_p$, és $y_0 \in \mathbb{Z}_p^\times$. Mivel P az E görbe egy pontja, ezért

$$p^{3n}y_0^2 z_0 = p^{3n}x_0^3 + ap^{7n}x_0 z_0^2 + bp^{9n}z_0^3$$

teljesül, és ekkor a $P_0 := (\bar{x_0}, \bar{y_0}, \bar{z_0})$ pont rajta van az $E_0 : Y^2Z = X^3$ görbén. $y_0 \in \mathbb{Z}_p^\times$ miatt $\bar{y_0} \neq 0$, így

$$\frac{\partial(Y^2Z - X^3)}{\partial Z}(P_0) = \bar{y_0}^2 \neq 0,$$

tehát P_0 pont nem szinguláris pontja E_0-nak. Jelöljük $E_0^{\mathrm{ns}}(\mathbb{F}_p)$-vel $E_0(\mathbb{F}_p)$ nem szinguláris pontjainak a halmazát. A harmadfokú görbéken megadott csoportstruktúra definiálásából könnyen látható, hogy ekkor a $P \mapsto P_0 : E^n(\mathbb{Q}_p) \to E_0^{\mathrm{ns}}(\mathbb{F}_p)$ leképe-

zés homomorfizmus. Ennek a homomorfizmusnak a magja azon $P = (p^n x_0, y_0, p^{3n} z_0)$ pontokból áll, amikre x_0 osztható p-vel, ami definíció szerint éppen $E^{n+1}(\mathbb{Q}_p)$. Ebből következik, hogy $E^{n+1}(\mathbb{Q}_p)$ valóban részcsoportja $E(\mathbb{Q}_p)$-nek. A Hensel-lemmának (3.4.2 tétel) az előbbiekhez hasonló módon való alkalmazásával látható, hogy az előbbi $P \mapsto P_0$ leképezés szürjektív, tehát ez a leképezés egy $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \to E_0^{\mathrm{ns}}(\mathbb{F}_p)$ izomorfizmust definiál. A 2.3 fejezetben láttuk, hogy az $(x : y : z) \mapsto \frac{x}{y}$ leképezés egy $E_0^{\mathrm{ns}}(\mathbb{F}_p) \to \mathbb{F}_p^+$ izomorfizmus. Így ezen leképezések kompozíciója, azaz a

$$(p^n x_0 : y_0 : p^{3n} z_0) \mapsto \bar{x_0}/\bar{y_0} : E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \to \mathbb{F}_p^+$$

leképezés is egy izomorfizmus, és ez éppen megegyezik a tétel állításában szereplő leképezéssel.

(d) Ha $P = (x : y : z) \in \bigcap_{n=0}^{\infty} E^n(\mathbb{Q}_p)$, akkor mint láttuk $y \neq 0$, és tetszőleges n-re $\frac{x}{y} \in p^n\mathbb{Z}_p$, és $\frac{z}{y} \in p^{3n}\mathbb{Z}_p$, azaz $\frac{x}{y} = \frac{z}{y} = 0 \Rightarrow x = z = 0$, tehát $P = (0 : 1 : 0) = O$. □

4.2.4. Megjegyzés. *Az (a) részben szereplő $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ csoportról a következőket tudjuk: ha E-nek széteső multiplikatív redukciója van modulo p, akkor az $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ csoport ciklikus, és a rendje $\mathrm{ord}_p(\Delta)$ 12-es maradéka, minden más esetben pedig $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ legfeljebb 4 rendű (Kodaira, Néron [6]).*

4.2.5. Következmény. *Ha m egy p-vel nem osztható egész, akkor a*

$$P \mapsto mP : E^1(\mathbb{Q}_p) \to E^1(\mathbb{Q}_p)$$

leképezés izomorfizmus.

Bizonyítás. Ez a leképezés nyilván homomorfizmus. Tegyük fel most, hogy $P \in \in E^1(\mathbb{Q}_p)$, és $P \neq O$. Ekkor a 4.2.3 tétel (d) pontja szerint $P \in E^n(\mathbb{Q}_p) \setminus E^{n+1}(\mathbb{Q}_p)$ valamilyen $n \geq 1$-ra. A 4.2.3 tétel (c) pontja szerint azonban

$$E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \simeq \mathbb{Z}/p\mathbb{Z},$$

és a P képe nem 0 $\mathbb{Z}/p\mathbb{Z}$-ben, hiszen $P \notin E^{n+1}(\mathbb{Q}_p)$. Ebből következik $(p, m) = 1$ miatt, hogy az mP pont képe sem 0, tehát speciálisan $mP \neq O$. Tehát tetszőleges $P \in E^1(\mathbb{Q}_p)$ pontra $mP = O \Rightarrow P = O$, azaz az állításban szereplő leképezés injektív.

Most belátjuk, hogy ez a leképezés szürjektív. Legyen $P \in E^1(\mathbb{Q}_p)$ tetszőleges. Ekkor, mivel

$$E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \simeq \mathbb{Z}/p\mathbb{Z},$$

ezért $(p, m) = 1$ miatt az m-mel való szorzás egy izomorfizmus $E^1(\mathbb{Q}_p)/E^2(\mathbb{Q}_p)$-n. Ez azt jelenti, hogy létezik olyan $Q_1 \in E^1(\mathbb{Q}_p)$, hogy $P - mQ_1 \in E^2(\mathbb{Q}_p)$. Ehhez hasonlóan kapjuk, hogy létezik olyan $Q_2 \in E^2(\mathbb{Q}_p)$ pont, hogy $P - mQ_1 - mQ_2 \in E^3(\mathbb{Q}_p)$.

Az eljárást folytatva kapjuk, hogy létezik olyan $Q_1, Q_2, ... \in E(\mathbb{Q}_p)$ sorozat, hogy minden n-re $Q_n \in E^n(\mathbb{Q}_p)$, és $P - \sum_{i=1}^{n} mQ_i \in E^{n+1}(\mathbb{Q}_p)$. A fejezet elején láttuk, hogy $E(\mathbb{Q}_p)$ kompakt, amiből következik, hogy az $S_n = \sum_{i=1}^{n} Q_i$ sorozatnak van egy $S_{i_1}, S_{i_2}, ...$ konvergens részsorozata. Legyen ekkor $T_k = P - S_{i_k}$, és legyen

$$T := \lim_{k\to\infty} T_k = P - m(\lim_{k\to\infty} S_{i_k}).$$

Azt állítjuk, hogy

$$P = m(\lim_{k\to\infty} S_{i_k}) \Leftrightarrow T = O.$$

Legyen $n \geq 1$ tetszőleges. A Q_i pontok konstrukciója miatt $P - \sum_{i=1}^{n} mQ_i \in$ $\in E^{n+1}(\mathbb{Q}_p)$, és $n < j < i_n$ esetén $mQ_j \in E^{n+1}(\mathbb{Q}_p)$. Ebből következik, hogy

$$T_n = P - \sum_{i=1}^{n} mQ_i - \sum_{j=n+1}^{i_n} mQ_j \in E^{n+1}(\mathbb{Q}_p).$$

A 4.2.3 tétel (c) részének bizonyításában láttuk, hogy ekkor T_n előáll $T_n = (x_n, y_n, z_n)$ alakban, ahol $x_n, y_n, z_n \in \mathbb{Z}_p$, és $p^{n+1} | x_n, z_n$, de $p \nmid y_n$. Ekkor $\lim_{k\to\infty} x_k = \lim_{k\to\infty} z_k =$ $= 0$, és így $T = \lim_{k\to\infty} T_k = O$. □

4.3. Torziópontok

4.3.1. Tétel. *Az $E^1(\mathbb{Q}_p)$ csoport torziómentes.*

Bizonyítás. A 4.2.5 következmény miatt ehhez az állításhoz elég belátni, hogy ha $P \in E^1(\mathbb{Q}_p)$, akkor $P \neq O$ esetén $pP \neq O$. Ehhez az E görbe helyett tekintsük az

$$E_1 : Z = X^3 + aXZ^2 + bZ^3$$

affin görbét. Ekkor tetszőleges $P = (x : y : z) \in E^1(\mathbb{Q}_p)$ esetén, mivel $y \neq 0$, ezért $P' = (x'(P), z'(P)) \in E_1(\mathbb{Q}_p)$, ahol $x'(P) = \frac{x}{y}, z'(P) = \frac{z}{y}$. Ezen jelölések mellett

$$E^n(\mathbb{Q}_p) = \{P \in E^1(\mathbb{Q}_p) |\, x'(P) \in p^n\mathbb{Z}_p\}.$$

A tétel bizonyításához szükségünk lesz a következő lemmára.

4.3.2. Lemma. *Legyenek $P_1, P_2, P_3 \in E^n(\mathbb{Q}_p)$ olyan pontok, amikre $P_1 + P_2 + P_3 =$ $= O$. Ekkor az előbbi jelöléseket használva*

$$x'(P_1) + x'(P_2) + x'(P_3) \in p^{5n}\mathbb{Z}_p.$$

Bizonyítás. A 4.2.3 tétel (c) részének bizonyításában láttuk, hogy $P \in E^n(\mathbb{Q}_p)$ esetén P előáll $P = (p^n x_0 : y_0 : p^{3n} z_0)$ alakban, ahol $x_0, z_0 \in \mathbb{Z}_p$, és $y_0 \in \mathbb{Z}_p^\times$. Ebből

következik, hogy a mostani jelöléseink mellett egy ilyen P pontra $x'(P) \in p^n\mathbb{Z}_p$ és $z'(P) \in p^{3n}\mathbb{Z}_p$ teljesülnek. Legyenek $x'_i = x'(P_i)$ és $z'_i = z'(P_i)$ $i = 1,2,3$-ra. Azt állítjuk, hogy ekkor az x'_1, x'_2 és x'_3 számok között van két különböző. Tegyük fel ugyanis, hogy $x'_1 = x'_2 = x'_3$. Ekkor a

$$Z - x_1'^3 - ax'_1Z^2 - bZ^3 = 0$$

egyenlet megoldásai Z-re éppen z'_1, z'_2 és z'_3. Ebből azonban

$$\frac{1}{b} = z'_1z'_2 + z'_2z'_3 + z'_3z'_1 \in p^{6n}\mathbb{Z}_p$$

következik, ami lehetetlen, hiszen $\mathrm{ord}_p \frac{1}{b} \leq 0$. Tehát az x'_1, x'_2, x'_3 számok között van két különböző, feltehető, hogy ezek x'_1 és x'_2. Ekkor a P_1 és P_2 pontokat összekötő egyenes $Z = \alpha X + \beta$ alakú, ahol $\alpha = \frac{z'_2 - z'_1}{x'_2 - x'_1}$, és $\beta = z'_1 - \alpha x'_1$. Az

$$x_1'^3 = z'_1 - ax'_1z_1'^2 - bz_1'^3 \text{ és } x_2'^3 = z'_2 - ax'_2z_2'^2 - bz_2'^3$$

összefüggésekből

$$\alpha = \frac{z'_2 - z'_1}{x'_2 - x'_1} = \frac{x_1'^2 + x'_1x'_2 + x_2'^2 + az_2'^2}{1 - ax'_1(z'_2 + z'_1) - b(z_1'^2 + x'_1z'_2 + z_2'^2)}$$

adódik. $x'_1, x'_2 \in p^n\mathbb{Z}_p$ és $z'_1, z'_2 \in p^{3n}\mathbb{Z}_p$ miatt az előbbi tört nevezője $\mathbb{Z}_p^\times$-ben van, a számlálója pedig osztható p^{2n}-nel, tehát $\alpha \in p^{2n}\mathbb{Z}_p$, és ekkor $\beta = z'_1 - \alpha x'_1 \in p^{3n}\mathbb{Z}_p$. Mint láttuk a $P_1 + P_2 + P_3 = O$ feltétel ekvivalens azzal, hogy a P_1, P_2, P_3 pontok egy egyenesen vannak, ezért az

$$\begin{aligned}&\alpha X + \beta = X^3 + aX(\alpha X + \beta)^2 + b(\alpha X + \beta)^3 \Leftrightarrow \\ &\Leftrightarrow (1 + a\alpha^2 + b\alpha^3)X^3 + (2a\alpha\beta + 3b\alpha^2\beta)X^2 + (a\beta^2 + 3b\alpha\beta^2 - \alpha)X + b\beta^3 - \beta = 0\end{aligned}$$

egyenlet megoldásai éppen x'_1, x'_2 és x'_3. Ebből

$$x'_1 + x'_2 + x'_3 = -\frac{2a\alpha\beta + 3b\alpha^2\beta}{1 + a\alpha^2 + b\alpha^3} \in p^{5n}\mathbb{Z}_p.$$

□

A tétel bizonyításának befejezése: Egy $P \in E^n(\mathbb{Q}_p)$ pontra legyen

$$\bar{x}(P) = x'(P) \mod p^{5n}.$$

Ekkor a lemma szerint tetszőleges $P_1, P_2 \in E^n(\mathbb{Q}_p)$ pontokra

$$\bar{x}(P_1) + \bar{x}(P_2) + \bar{x}(-P_1 - P_2) = 0 \text{ és } \bar{x}(P_1 + P_2) + \bar{x}(-P_1 - P_2) + \bar{x}(O) = 0$$

teljesülnek. Ebből következik, hogy $\bar{x}(P_1 + P_2) = \bar{x}(P_1) + \bar{x}(P_2)$, hiszen $x'(O) = = 0 \Rightarrow \bar{x}(O) = 0$. Ez éppen azt jelenti, hogy a

$$P \mapsto \bar{x}(P) : E^n(\mathbb{Q}_p) \to p^n\mathbb{Z}_p/p^{5n}\mathbb{Z}_p$$

leképezés egy homomorfizmus.

Legyen most $P \in E^1(\mathbb{Q}_p)$ egy tetszőleges pont, amire $P \neq O$. Ekkor a 4.2.3 tétel (d) része szerint $P \in E^n(\mathbb{Q}_p) \setminus E^{n+1}(\mathbb{Q}_p)$ valamilyen $n \geq 1$-re. Ekkor, mint láttuk

$$\mathrm{ord}_p(x'(P)) = n \Rightarrow \bar{x} \in p^n\mathbb{Z}_p \setminus p^{n+1}\mathbb{Z}_p \mod p^{5n},$$

amiből

$$\bar{x}(pP) \in p^{n+1}\mathbb{Z}_p \setminus p^{n+2}\mathbb{Z}_p \mod p^{5n}.$$

Tehát $\bar{x}(pP) \neq 0 \Rightarrow pP \neq O$, és ezt kellett bizonyítanunk. □

4.3.3. Megjegyzés. *Az előző bizonyításból valójában adódik az is, hogy*

$$E^1(\mathbb{Q}_p) \simeq \mathbb{Z}_p^+ \simeq \varprojlim Z_{p^i}.$$

Bizonyítás (vázlat). A 4.2.3 tételből következik, hogy $n \geq 2$ esetén $E^1(\mathbb{Q}_p)/E^n(\mathbb{Q}_p)$ p-csoport, és a rendje pontosan p^{n-1}. Az előző bizonyításból látható, hogy $P \in \in E^1(\mathbb{Q}_p) \setminus E^2(\mathbb{Q}_p)$ esetén $p^kP \in E^{k+1}(\mathbb{Q}_p) \setminus E^{k+2}(\mathbb{Q}_p)$ tetszőleges $k \geq 1$ egészre, speciálisan $p^{n-2}P \notin E^n(\mathbb{Q}_p)$. Ez azonban csak akkor lehetséges, ha

$$E^1(\mathbb{Q}_p)/E^n(\mathbb{Q}_p) \simeq Z_{p^{n-1}}.$$

Tekintsük most a természetes módon adódó

$$E^1(\mathbb{Q}_p) \to \varprojlim E^1(\mathbb{Q}_p)/E^{i+1}(\mathbb{Q}_p)$$

homomorfizmust. Azt állítjuk, hogy ez egy izomorfizmus. Az injektivitás következik a 4.2.3 tétel (d) pontjából, a szürjektivitás pedig a 4.2.5 következmény bizonyításában leírtakhoz hasonlóan meggondolható. Ekkor tehát

$$E^1(\mathbb{Q}_p) \simeq \varprojlim E^1(\mathbb{Q}_p)/E^{i+1}(\mathbb{Q}_p) \simeq \varprojlim Z_{p^i}.$$

□

4.3.4. Következmény. *Ha $P = (x : y : 1) \in E(\mathbb{Q}_p)_{\mathrm{tors}}$, akkor $x, y \in \mathbb{Z}_p$.*

Bizonyítás. Tegyük fel, hogy a $P = (x : y : 1)$ pont torziópontja $E(\mathbb{Q}_p)$-nek. Ekkor ha x és y nincsenek benne egyszerre $\mathbb{Z}_p$-ben, akkor a P pont valamelyik $(x' : y' : z')$ primitív koordinátázásában $z' \in p\mathbb{Z}_p$, tehát $\bar{z} = 0$. Ekkor azonban csak $\bar{P} = \bar{O}$

lehetséges, és így $P \in E^1(\mathbb{Q}_p)$, ami a 4.3.1 tétel szerint ellentmond annak, hogy P torziópont. □

4.3.5. Következmény. *Ha $P = (x : y : 1) \in E(\mathbb{Q})_{\text{tors}}$, akkor $x, y \in \mathbb{Z}$.*

Bizonyítás. Ez az állítás könnyen következik az előbbi következményből, hiszen $r \in \mathbb{Q} \setminus \mathbb{Z}$ esetén $\text{ord}_p(r) < 0$ valamilyen p prímre, és ekkor $r \notin \mathbb{Z}_p$. □

4.3.6. Következmény. *Ha az E görbének jó redukciója van modulo p, akkor a*

$$P \to \bar{P} : E(\mathbb{Q})_{\text{tors}} \to \bar{E}(\mathbb{F}_p)$$

redukciós leképezés injektív.

Bizonyítás. Mivel E-nek jó redukciója van p-ben, ezért $E^0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$, így az $E(\mathbb{Q})_{\text{tors}} \to \bar{E}(\mathbb{F}_p)$ redukciós leképezés magja része $E^1(\mathbb{Q}_p)$-nek, és a 4.3.1 tétel szerint $E^1(\mathbb{Q}_p) \cap E(\mathbb{Q})_{\text{tors}} = \{O\}$. □

4.3.7. Állítás. *Tegyük fel, hogy $P = (x_1 : y_1 : 1) \in E(\mathbb{Q})$, és $2P = (x_2 : y_2 : 1)$. Ekkor ha x_1, y_1, x_2, y_2 egészek, akkor $y_1 = 0$ vagy $y_1 | \Delta$ ($\Delta = 4a^3 + 27b^2 \neq 0$).*

Bizonyítás. Tegyük fel, hogy $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ és $y_1 \neq 0$. Ekkor a 4.2.2 állítás jelöléseit használva $E_2(\mathbb{Q})$-nek a P' pontban húzott érintőjének az egyenlete $Y = \alpha X + \beta$ alakú, ahol $\alpha = \frac{\partial f}{\partial X}(P) / \frac{\partial f}{\partial Y}(P) = \frac{3x_1^2 + a}{2y_1}$, ahol

$$f(X, Y) = Y^2 - X^3 - aX - b.$$

($y_1 \neq 0$ miatt $\frac{\partial f}{\partial Y}(P) = 2y_1 \neq 0$.) Mivel $P + P + (-2P) = O$, ezért a 4.2.2 állítás bizonyításában leírtakhoz hasonlóan meggondolható, hogy ekkor $2x_1 + x'(-2P) = \alpha^2$, de $x'(-2P) = x'(2P) = x_2$, tehát

$$\alpha^2 = 2x_1 + x_2 \in \mathbb{Z} \Rightarrow \alpha \in \mathbb{Z} \Rightarrow y_1 | 3x_1^2 + a.$$

Ebből

$$\begin{aligned} y_1 | &-27(x_1^3 + ax_1 - b)y_1^2 + (3x_1^2 + 4a)(3x_1^2 + a)^2 = \\ &= -27(x_1^3 + ax_1 - b)(x_1^3 + ax_1 + b) + (3x_1^2 + 4a)(3x_1^2 + a)^2 = 27b^2 + 4a^3 = \Delta \end{aligned}$$

következik, és ezt kellett bizonyítanunk. □

4.3.8. Tétel (Lutz–Nagell)**.** *Ha $P = (x : y : 1) \in E(\mathbb{Q})_{\text{tors}}$, akkor $x, y \in \mathbb{Z}$ és $y = 0$ vagy $y | \Delta$.*

Bizonyítás. Legyen $P = (x : y : 1) \in E(\mathbb{Q})$ egy tetszőleges torziópont, ekkor a $2P = (x_2 : y_2 : 1)$ pont is torziópont, így a 4.3.5 következmény szerint $x, y, x_2, y_2 \in \mathbb{Z}$, és ekkor a 4.3.7 állítás szerint $y = 0$ vagy $y | \Delta$. □

A 4.3.8 tétel felhasználásával adható egy algoritmus, amivel meghatározható egy $E(\mathbb{Q})$ görbe összes torziópontja. Tekintsük ugyanis az összes ilyen y egész számot, amire $y = 0$ vagy $y|\Delta$. Ekkor, ha $x \in \mathbb{Z}$ és $P = (x : y : 1) \in E(\mathbb{Q})$, akkor

$$x^3 + ax + b - y^2 = 0 \Rightarrow x|b - y^2.$$

Tekintsük tehát az összes olyan x egész számot, amelyre $x|b - y^2$. Az összes ilyen (x, y) párra a $P = (x : y : 1)$ pontot ellenőrizve megkapjuk $E(\mathbb{Q})$ összes torziópontját. Ha $p \nmid \Delta$, akkor a 4.3.6 következmény miatt $\bar{E}(\mathbb{F}_p)$ elemszámával felülről becsülhető $E(\mathbb{Q})_{\text{tors}}$ rendje (és így a torzióelemek rendje is). Ezt felhasználva egy $P \in E(\mathbb{Q})$ pontról tudjuk ellenőrizni, hogy torzió-pont-e. Valójában egy torzió-pont rendje mindig legfeljebb 12, ugyanis igaz a következő tétel.

4.3.9. Tétel (Mazur)**.** *Az eddigi jelölések mellett $E(\mathbb{Q})_{\text{tors}}$ izomorf az alábbi csoportok valamelyikével:*
Z_n, ahol $1 \leq n \leq 10$ vagy $n = 12$; $Z_2 \times Z_n$, ahol $1 \leq n \leq 4$,
továbbá ez a 15 csoport mind elő is áll, mint valamilyen $\mathbb{Q}$ feletti elliptikus görbe torziócsoportja.

Bizonyítás. [2], [3]. □

Hivatkozások

[1] W. Fulton, Algebraic curves. An introduction to algebraic geometry. W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[2] B. Mazur, Modular curves and the Eisenstein ideal. IHES Publ. Math., (47):33–186 (1978), 1977.

[3] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math., 44(2):129–162, 1978.

[4] J. S. Milne, Algebraic Number Theory, 2011. http://www.jmilne.org/math/CourseNotes/ANTe6.pdf

[5] J. S. Milne, Elliptic Curves. BookSurge Publishers, 2006.

[6] A. Néron, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, IHES Publ. Math. 21: 361-482, 1964.

[7] J.-P. Serre, A course in arithmetic. Graduate Texts in Mathematics, No. 7., Springer-Verlag, New York, 1973.

[8] J. H. Silverman, The arithmetic of elliptic curves. Graduate Texts in Mathematics, No. 106., Springer-Verlag, New York, 1986.