Kapitel 2

Endomorfier

Vi vil i dette kapitel etablere nogle vigtige resultater vedrørende endomorfier på elliptiske kurver, som vi bl.a. vil benytte i beviset for Hasses sætning.

2.1 Endomorfier på elliptiske kurver

Lad K være et legeme og $\overline{K}$ en tilhørende algebraisk aflukning. I det følgende vil vi med en elliptisk kurve E mene en kurve på formen $y^2 = x^3 + Ax + B$. Vi begynder da med følgende definition:

Definition 3 *En endomorfi på E er en homomorfi $\alpha : E(\overline{K}) \to E(\overline{K})$ givet ved rationale funktioner.*

Med en rational funktion forstår vi en kvotient af polynomier. Det vil altså sige, at en endomorfi α skal opfylde, at $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ og der skal findes rationale funktioner $R_1(x, y)$ og $R_2(x, y)$, begge med koefficienter i $\overline{K}$, så

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

for alle $(x, y) \in E(\overline{K})$. Da α er en homomorfi gælder der specialt at $\alpha(\infty) = \infty$. Den trivielle endomorfi angives med 0 og er den endomorfi, som sender ethvert punkt til ∞. Vi vil fremover antage, at α ikke er den trivielle endomorfi, hvilket betyder at der findes $(x, y) \in E(\overline{K})$ sådan at $\alpha(x, y) \neq \infty$.

Eksempel 1. Lad E være en elliptisk kurve og lad α være givet ved, at $\alpha(P) = 2P$. Da er α en homomorfi og $\alpha(x, y) = (R_1(x, y), R_2(x, y))$, hvor

$$\begin{aligned} R_1(x, y) &= \left(\frac{3x^2 + A}{2y}\right)^2 - 2x, \\ R_2(x, y) &= \left(\frac{3x^2 + A}{2y}\right)\left(x - \left(\left(\frac{3x^2 + A}{2y}\right)^2 - 2x\right)\right) - y \\ &= \left(\frac{3x^2 + A}{2y}\right)\left(3x - \left(\frac{3x^2 + A}{2y}\right)^2\right) - y. \end{aligned}$$

Da både R_1 og R_2 er rationale funktioner er α en endomorfi for E. □

Vi ønsker nu, at finde en standard repræsentation for de rationale funktioner, som en endomorfi er givet ved. Følgende sætning gør dette muligt for os:

Sætning 2 *Lad E være en elliptisk kurve over et legeme K. En endomorfi α kan da skrives som*

$$\alpha(x,y) = (r_1(x), r_2(x)y) = \left(\frac{p(x)}{q(x)}, \frac{s(x)}{t(x)}y\right),$$

hvor p, q henholdsvis s, t ikke har nogen fælles faktor.

Bevis. For et punkt $(x,y) \in E(\overline{K})$ gælder der, at $y^2 = x^3 + Ax + B$. Dette medfører, at

$$y^{2k} = (x^3 + Ax + B)^k \quad \text{og} \quad y^{2k+1} = y^{2k}y = (x^3 + Ax + B)^k y, \quad k \in \mathbb{N}.$$

Vi kan altså erstatte en lige potens af y med et polynomium der kun afhænger af x, og en ulige potens med y ganget med et polynomium der kun afhænger af x. For en rational funktion $R(x,y)$ kan vi da beskrive en anden rational funktion, som stemmer overens med denne på punkter fra $E(\overline{K})$. Vi kan altså antage, at

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}. \tag{2.1}$$

Vi kan endda gøre det endnu simplere ved at gange udtrykket i (2.1) med $p_3(x) - p_4(x)$, hvilket gør at vi i nævneren får

$$(p_3(x) - p_4(x)y)(p_3(x) + p_4(x)y) = p_3(x)^2 - p_4(x)^2y^2,$$

hvorefter vi kan erstatte y^2 med $x^3 + Ax + B$. Dette giver os altså, at

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{2.2}$$

Da α er en endomorfi er den givet ved

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)),$$

hvor R_1 og R_2 er rationale funktioner. Da α specielt er en homomorfi bevarer den strukturen for en elliptisk kurve så vi har, at

$$\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y).$$

Dette medfører, at

$$R_1(x,-y) = R_1(x,y) \quad \text{og} \quad R_2(x,-y) = -R_2(x,y).$$

Skriver vi R_1 på samme form som i (2.2) må $q_2(x) = 0$, og ligeledes må vi for R_2 have at $q_1(x) = 0$. Vi kan altså antage, at

$$\alpha(x, y) = (r_1(x), r_2(x)y),$$

hvor $r_1(x)$ og $r_2(x)$ er rationale funktioner. Skriv da

$$r_1(x) = \frac{p(x)}{q(x)} \quad \text{og} \quad r_2(x) = \frac{s(x)}{t(x)}y,$$

hvor p, q henholdsvis s, t ikke har nogen fælles faktorer. Hvis $q(x) = 0$ for et punkt (x, y) lader vi $\alpha(x, y) = \infty$. Hvis $q(x) \neq 0$ giver (ii) i lemma 1, at $r_2(x)$ da også vil være defineret og vi har det ønskede. □

Vi viser da lemmaet, som blev benyttet i beviset ovenfor. Bemærk, at hvis to polynomier har en fælles rod må de nødvendigvis have en fælles faktor.

Lemma 1 *Lad α være en endomorfi givet ved*

$$\alpha(x, y) = \left(\frac{p(x)}{q(x)}, \frac{s(x)}{t(x)}y\right),$$

for en elliptisk kurve E. Lad p, q henholdsvis s, t være sådan, at de ikke har nogen fælles rødder. Da har vi, at

(i) For et polynomium $u(x)$, som ikke har en fælles rod med $q(x)$ har vi, at

$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}.$$

(ii) $t(x_0) = 0$ hvis og kun hvis $q(x_0) = 0$.

Bevis. (i) For et punkt $(x, y) \in E(K)$ har vi også, at $\alpha(x, y) \in E(K)$, da α er en endomorfi. Derfor har vi, at

$$\begin{aligned}\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} &= \frac{y^2 s(x)^2}{t(x)^2} = \left(\frac{s(x)}{t(x)}y\right)^2 \\ &= \left(\frac{p(x)}{q(x)}\right)^3 + A\left(\frac{p(x)}{q(x)}\right) + B \\ &= \frac{p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3}{q(x)^3} = \frac{u(x)}{q(x)^3},\end{aligned}$$

hvor $u(x) = p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3$. Antag nu, at $q(x_0) = 0$. Hvis nu også $u(x_0) = 0$ følger det, at

$$u(x_0) = p(x_0)^3 + Ap(x_0)q(x_0)^2 + Bq(x_0)^3 = 0 \Rightarrow p(x_0)^3 = 0,$$

så $p(x_0) = 0$. Men p og q havde pr. antagelse ingen fælles rødder. Så hvis $q(x_0) = 0$ må $u(x_0) \neq 0$ og de har dermed ingen fælles rødder.

(ii) Vi ved fra (i), at

$$(x^3 + Ax + B)s(x)^2q(x)^3 = u(x)t(x)^2. \tag{2.3}$$

Hvis $q(x_0) = 0$ følger det direkte fra (2.3), at

$$u(x_0)t(x_0)^2 = 0.$$

Da q og u ikke har nogen fælles rødder følger det, at $t(x_0) = 0$. Antag nu, at $t(x_0) = 0$, da har vi fra (2.3), at

$$({x_0}^3 + Ax_0 + B)s(x_0)^2q(x_0)^3 = 0.$$

Da s og t pr. antagelse ikke har nogen fælles rødder giver det yderligere, at

$$({x_0}^3 + Ax_0 + B)q(x_0)^3 = 0.$$

Hvis ${x_0}^3 + Ax_0 + B \neq 0$ er $q(x_0)^3 = 0$ og dermed må $q(x_0) = 0$. Hvis vi derimod har, at ${x_0}^3 + Ax_0 + B = 0$ er det klart, at $(x - x_0)$ deler $(x^3 + Ax + B)$. Med andre ord findes et polynomium $Q(x)$ sådan, at

$$(x^3 + Ax + B) = (x - x_0)Q(x),$$

hvor $Q(x_0) \neq 0$, da $x^3 + Ax + B$ ikke har nogen dobbeltrødder. Da $t(x_0) = 0$ findes der også et polynomium $T(x)$ sådan, at

$$t(x) = (x - x_0)T(x).$$

Udtrykket fra (2.3) kan da skrives, som

$$(x - x_0)Q(x)s(x)^2q(x)^3 = u(x)((x - x_0)T(x))^2,$$

hvilket efter division med $(x - x_0)$ giver os, at

$$Q(x)s(x)^2q(x)^3 = u(x)(x - x_0)T(x)^2.$$

I tilfældet, hvor $x = x_0$ har vi så, at

$$Q(x_0)s(x_0)^2q(x_0)^3 = 0,$$

men da $Q(x_0) \neq 0$ og $s(x_0) \neq 0$ må $q(x_0)^3 = 0$, hvilket i sidste ende giver os, at $q(x_0) = 0$. □

Med den nu etablerede standard repræsentation for endomorfier, er vi i stand til at give en definition for graden af en endomorfi:

Definition 4 *Graden af en endomorfi α er givet ved*

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\},$$

når α ikke er den trivielle endomorfi, altså for $\alpha \neq 0$. For $\alpha = 0$ lader vi $\deg(\alpha) = 0$.

En endomorfi siges at være *separabel* hvis den afledede $r_1'(x) \neq 0$.

Den følgende proposition er essentiel idet, at det tilknytter graden af en endomorfi til antallet af elementer i kernen for selvsamme endomorfi. Dette faktum benyttes direkte i beviset for Hasses sætning.

Proposition 1 *Lad E være en elliptisk kurve. Lad $\alpha \neq 0$ være en separabel endomorfi for E. Da er*

$$\deg \alpha = \#\ker(\alpha),$$

hvor $\ker(\alpha)$ *angiver kernen for homomorfien $\alpha : E(\overline{K}) \to E(\overline{K})$. I tilfældet hvor $\alpha \neq 0$ ikke er separabel gælder der, at*

$$\deg \alpha > \#\ker(\alpha).$$

Bevis. Vi skriver α på standardformen, som vi introducerede tidligere, altså sættes

$$\alpha(x, y) = (r_1(x), r_2(x)y)),$$

hvor $r_1(x) = p(x)/q(x)$. Da α er antaget til at være separabel er $r_1' \neq 0$ og dermed er $p'q - pq'$ (tælleren af r_1') ikke nulpolynomiet. Lad nu

$$S = \{x \in \overline{K} \mid (p'q - pq')(x)q(x) = 0\}.$$

Lad da $(a, b) \in E(\overline{K})$ være valgt sådan, at følgende er opfyldt

1. $a \neq 0$, $b \neq 0$ og $(a, b) \neq \infty$,
2. $\deg(p(x) - aq(x)) = \max\{\deg p(x), \deg q(x)\} = \deg \alpha$,
3. $a \notin r_1(S)$,
4. $(a, b) \in \alpha(E(\overline{K}))$.

Vi skal da argumentere for, at sådan et punkt findes. Da $\overline{K}$ er algebraisk lukket er $E(\overline{K})$ en uendelig mængde og vi kan derfor undgå de punkter, hvor $a = 0, b = 0$ eller $(a, b) = \infty$. Lad

$$p(x) = cx^n + (\text{led af lavere orden}), \quad q(x) = dx^m + (\text{led af lavere orden}).$$

Hvis $\deg p > \deg q$ er $n > m$ og dermed er $\deg(p - aq) = n$ som påkrævet. På samme måde gælder det hvis $\deg q > \deg p$. Hvis $n = m$ er (ii) ikke opfyldt når $c - ad = 0$,

men i dette tilfælde kan vi gange a med et heltal større end 1 og finde et punkt hvor (ii) er opfyldt. Da $p'q - pq'$ ikke er nulpolynomiet er S en endelig mængde, hvilket dermed også betyder, at $\alpha(S)$ er en endelig mængde. Funktionen $r_1(x)$ antager uendeligt mange forskellige værdier når x gennemløber $\overline{K}$, da en algebraisk aflukning indeholder uendeligt mange elementer. Da der for hvert x er et punkt $(x, y) \in E(\overline{K})$ følger det, at $\alpha(E(\overline{K}))$ er en uendelig mængde. Det er altså muligt, at vælge et punkt $(a, b) \in E(\overline{K})$ med egenskaberne ovenfor.

Vi vil vise, at der findes netop $\deg \alpha$ punkter $(x_1, y_1) \in E(\overline{K})$ sådan at

$$\alpha(x_1, y_1) = (a, b).$$

Det er velkendt fra gruppeteorien, at $\alpha^{-1}(\alpha(x_1, y_1)) = (x_1, y_1) \ker \alpha$, så dette vil medføre at $\ker \alpha$ har $\deg \alpha$ elementer. For et sådan punkt gælder der, at

$$\frac{p(x_1)}{q(x_1)} = a, \quad r_2(x_1)y_1 = b.$$

Da $(a, b) \neq \infty$ er $q(x_1) \neq 0$. Da $b \neq 0$ har vi også, at $y_1 = b/r_2(x_1)$. Dette betyder, at y_1 er bestemt ved x_1, så vi behøver kun at tælle værdier for x_1. Fra antagelse (2) har vi, at $p(x) - aq(x) = 0$ har $\deg \alpha$ rødder talt med multiplicitet. Vi skal altså vise, at $p - aq$ ikke har nogen multiple rødder. Antag for modstrid, at x_0 er en multipel rod. Da har vi, at

$$p(x_0) - aq(x_0) = 0 \quad \text{og} \quad p'(x_0) - aq'(x_0) = 0,$$

da hvis x_0 er en multipel rod er den også rod i den afledte. Dette kan omskrives til ligningerne $p(x_0) = aq(x_0)$ og $aq'(x_0) = p'(x_0)$, som vi ganger med hinanden og får, at

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Da $a \neq 0$ pr. (1) giver det os, at x_0 er en rod i $p'q - pq'$ så $x_0 \in S$. Altså er $a = r_1(x_0) \in r_1(S)$, hvilket er i modstrid med (3). Dermed har $p - aq$ netop $\deg \alpha$ forskellige rødder. Da der er præcist $\deg \alpha$ punkter (x_1, y_1) så $\alpha(x_1, y_1) = (a, b)$ har kernen for α netop $\deg \alpha$ elementer.

Hvis α ikke er separabel kan det samme bevis anvendes, hvor $p' - aq'$ dog altid er nulpolynomiet så $p - aq(x) = 0$ har altid multiple rødder, så den har færre end $\deg \alpha$ løsninger. □

Sætning 3 *Lad E være en elliptisk kurve over et legeme K. Lad $\alpha \neq 0$ være en endomorfi for E. Da er $\alpha : E(\overline{K}) \to E(\overline{K})$ surjektiv.*

Bevis. Lad $(a, b) \in E(\overline{K})$. Vi vil vise, at der findes et punkt $(x, y) \in E(\overline{K})$ sådan, at $\alpha(x, y) = (a, b)$. Da $\alpha(\infty) = \infty$ kan vi antage, at $(a, b) \neq \infty$. Lad $r_1(x) = p(x)/q(x)$. Vi skal betragte to tilfælde:

Hvis $p(x) - aq(x)$ ikke er et konstant polynomium har det en rod x_0. Hvis vi nu har, at $q(x_0) = 0$ må $p(x_0) = 0$, hvilket er i modstrid med at p og q ikke har nogen fælles rødder. Derfor har vi $q(x_0) \neq 0$ og det følger, at

$$p(x_0) - aq(x_0) = 0 \Rightarrow a = \frac{p(x_0)}{q(x_0)}.$$

Vælg nu $y_0 \in E(\overline{K})$ som en af kvadratrødderne af $x_0^3 + Ax_0 + B$. Da er $\alpha(x_0, y_0)$ defineret og $\alpha(x_0, y_0) = (a, b')$ for et b'. Da

$$(b')^2 = a^3 + Aa + B = b^2,$$

er $b = \pm b'$. Hvis $b' = b$ er vi færdige. Hvis $b' = -b$ har vi, at

$$\alpha(x_0, -y_0) = (a, -b') = (a, b).$$

Vi mangler nu, at betragte tilfældet hvor $p(x) - aq(x)$ er konstant. Da $E(\overline{K})$ er uendelig og $\ker \alpha$ er endelig afbilledes kun endeligt mange punkter fra $E(\overline{K})$ til en given x-koordinat. Derfor må enten $p(x)$ eller $q(x)$ være ikke-konstant, da hvis de begge var konstante ville der være uendeligt mange punter fra $E(\overline{K})$ der afbilledes til en x-koordinat. Hvis p og q er to ikke-konstante polynomier er der højest én konstant a sådan at $p - aq$ er konstant, da vi ellers for en anden sådan konstant a' har, at

$$(a' - a)q = (p - aq) - (p - a'q), \quad (a' - a)p = a'(p - aq) - a(p - a'q),$$

hvor begge ligninger er konstante, som medfører at p og q er konstante. Så der er højest to punkter (a, b) og $(a, -b)$ som ikke er i billedet af α. Lad (a_1, b_1) være et andet punkt end disse. Da er $\alpha(P_1) = (a_1, b_1)$ for et punkt P_1. Vi kan vælge (a_1, b_1) sådan, at $(a_1, b_1) + (a, b) \neq (a, \pm b)$, så der findes et punkt P_2 sådan, at $\alpha(P_2) = (a_1, b_1) + (a, b)$. Dermed har vi, at

$$\alpha(P_2 - P_1) = (a, b) \quad \text{og} \quad \alpha(P_1 - P_2) = (a, -b).$$

Vi har da ramt alle punkter, så α er surjektiv. □

Dette bevis konkluderer vores undersøgelse af endomorfier på generelle legemer K. Vi vil i kapitel 4 fortsat behandle endomorfier, men der vil det være for endelige legemer.