



UNIVERSITAT DE
BARCELONA

Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

La fita de Hasse per a corbes el·líptiques

Autor: Eduardo Martirena Mateo

Director: Dr. Francesc Fité Naya

**Realitzat a: Departament
de Matemàtiques i Informàtica**

Barcelona, 10 de juny de 2026

Abstract

The main goal of this work is to give an introduction of the theory of elliptic curves and to prove Hasse's bound for the number of rational points on an elliptic curve defined over a finite field. To achieve these objectives we will introduce all the notions needed from algebraic curve theory and the concepts leading to the statement of the Riemann-Roch theorem. Lastly, we will define elliptic curves and isogenies. The study of their properties will lead us to the proof of Hasse's bound.

Resum

L'objectiu d'aquest treball és demostrar la fita de Hasse sobre el nombre de punts racionals en una corba el·líptica definida sobre un cos finit. La teoria que hem hagut de desenvolupar per a assolir aquesta demostració representa una bona introducció a la teoria de corbes el·líptiques. Es treballen conceptes bàsics de corbes algebraïques fins a l'enunciat del teorema de Riemann-Roch, aleshores es presenten i treballem les nocions bàsiques de corbes el·líptiques definides sobre cossos arbitraris. Finalment, es demostra la fita de Hasse a partir de resultats i conceptes demostrats en el desenvolupament de la teoria.

Agraïments

Primerament, m'agradaria agrair al meu tutor, Francesc Fité per la seva guia i confiança al llarg de la construcció d'aquest treball. Gràcies a les seves aportacions i ajut he pogut descobrir i entendre una branca de les matemàtiques que m'era pràcticament desconeguda i he tingut la sort de poder gaudir en aquest treball.

Vull agrair també a tots els companys de facultat amb qui hem compartit moments de tot tipus i sense els quals aquest viatge hagués estat molt menys enriquidor. Així vull mencionar especialment a l'Eudald Vilar, que ha estat un gran mentor més enllà de lo acadèmic i al Joan Blay, la meva inseparable mà esquerra.

Mereixen també un agraïment tots els professors que ensenyen matemàtiques amb la passió i solemnitat que aquesta disciplina mereix. Particularment, al Juan Carlos Rincón, qui em va obrir els ulls fa més de 5 anys ensenyant-me què eren les matemàtiques.

Finalment, gràcies totals a tota la meva família pels in comptables esforços que han portat a terme per tal que jo pugui gaudir plenament de la meva etapa educativa. En particular, als meus pares, Andrea i Marcelo per haver-me inculcat des de petit la importància de buscar el saber pel saber i a la meva germana Paula per haver estat una inesgotable font de llum tots aquests anys. A tots tres, per haver-me suportat més del que em mereixia i haver confiat en mi més del jo ho feia.

Índex

Introducció	1
1 Corbes algebraiques	3
1.1 Preliminars	3
1.2 Aplicacions entre corbes algebraiques	5
1.2.1 Ramificació	8
1.2.2 El morfisme de Frobenius	10
1.3 Diferencials	13
2 Divisors i Riemann-Roch	18
2.1 Divisors	18
2.1.1 Divisor d'una funció	19
2.1.2 Divisor d'una forma diferencial	22
2.2 Aproximació al teorema de Riemann-Roch	23
3 Corbes el·líptiques i isogènies	29
3.1 Definició de corba el·líptica	29
3.2 Estructura de grup	30
3.3 Isogènies	35
4 Fita de Hasse per a cossos finits	42
4.1 La diferencial invariant	42
4.2 Isogènia dual	45
4.3 Fita de Hasse	50
Conclusions	53
Bibliografia	54

Introducció

Avui en dia, la teoria de nombres té tres branques diferenciades. Es pot fer teoria de nombres a partir de l'anàlisi, i hom estarà fent teoria analítica de nombres; es pot atacar des de l'àlgebra, teoria de nombres algebraica i es pot a partir de la geometria en l'estudi de les corbes el·líptiques. En aquest treball ens introduïrem en aquesta última branca, l'estudi de les corbes el·líptiques.

Les corbes el·líptiques són un objecte d'estudi molt ample així que nosaltres ens enfocarem en corbes el·líptiques per a cossos arbitraris i seguirem el camí necessari per a arribar a demostrar l'anomenada fita de Hasse:

Teorema. *Sigui E una corba el·líptica definida sobre K el cos finit de q elements $(\mathbb{F}_q)$ i $E(K)$ els punts de E amb coordenades a K . Aleshores*

$$|\#E(K) - (q + 1)| \leq 2\sqrt{q}$$

Aquest resultat va ser conjeaturat inicialment per Emil Artin i demostrat per Helmut Hasse al 1933. Més enllà de l'interés intrínsec que té qualsevol resultat matemàtic, la fita de Hasse pot tenir aplicacions interessants en diverses matèries. Un exemple n'és la criptografia, amb tota una branca desenvolupada a partir de corbes el·líptiques.

En aquest context, i considerant nombres primers grans, la fita de Hasse ens permet aproximar $\#E(\mathbb{F}_q)$ amb un error de l'ordre de l'arrel quadrada de q . En altres paraules, essencialment q i $\#E(\mathbb{F}_q)$ tenen el mateix nombre de xifres i en comparteixen la primera meitat.

Com mostrarem, les corbes el·líptiques són corbes de gènere 1. L'any 1949 André Weil va generalitzar la fita de Hasse per a corbes de gènere qualsevol, resultat que es pot trobar anomenat com la fita de Hasse-Weil.

Teorema. *Sigui E una corba de gènere g definida sobre $K = \mathbb{F}_q$, aleshores:*

$$|\#E(K) - (q + 1)| \leq 2g\sqrt{q}$$

On veiem immediatament que si $g = 1$, recuperem la fita de Hasse. El següent pas natural d'aquest treball podria haver estat arribar a la demostració alternativa d'Enrico Bombieri de la fita de Hasse-Weil presentada 30 anys després.

El treball comença, a nivell conceptual, on acabaria una assignatura de corbes algebraiques i suposarem, durant tota la llargada del treball que el lector ha cursat assignatures com Equacions Algebraiques o Teoria de Galois i Àlgebra commutativa, així com mencionarem que pot arribar a ser d'especial interès per aquell qui hagi cursat Teoria de Nombres Algebraica.

Al primer capítol del treball introduïrem els conceptes bàsics referits a corbes algebraïques. Veurem la relació entre morfismes de corbes i els cossos de funcions respectius, donarem resultats sobre la separabilitat i la ramificació de morfismes de corbes. Acabarem el capítol estudiant l'espai de formes diferencials d'una corba projectiva llisa i la seva relació amb els conceptes definits.

Per a poder arribar a la fita de Hasse haurem d'introduir el concepte de gènere, a partir del teorema de Riemann-Roch que donarem al final del segon capítol on haurem treballat amb resultats sobre el grup de divisors d'una corba. En aquest segon capítol arribarem a demostrar el teorema de Riemann a partir del qual podrem definir el gènere d'una corba.

Al tercer capítol, amb el teorema de Riemann-Roch present i havent definit el gènere d'una corba, definirem corba el·líptica, veurem quina importància té el gènere i tractarem l'estructura de grup de les corbes el·líptiques i les isogènies, dotant-nos de tota la maquinària en corbes el·líptiques que necessitaríem al capítol final.

Finalment, al darrer capítol, obtindrem el primer resultat que ens aproximarà a la demostració de la fita de Hasse, la condició de separable de l'aplicació $1-\phi$ on ϕ és l'endomorfisme de Frobenius. Aquest fet, amb els resultats de isogènies duals ens permetran donar una demostració molt elegant del teorema central i final d'aquest treball.

Treballarem, normalment, sobre cossos arbitraris, no necessàriament algebraicament tancats ni de característica zero i buscarem la generalitat dels resultats sempre que sigui possible. Al llarg del treball anirem fent al·lusió a la teoria de nombres algebraica, a geometria algebraica més general i a temes d'àlgebra commutativa. Diversos resultats (principalment aquells que citarem directament de les referències) provenen d'aquests altres camps i permeten al lector veure l'estreta relació entre aquestes branques de les matemàtiques que per a l'autor ha estat una gran troballa en el camí per al desenvolupament de la teoria sobre corbes el·líptiques i l'enteniment i demostració de la fita de Hasse.

Capítol 1

Corbes algebraiques

En aquest capítol treballarem sobre les nocions bàsiques en la teoria de corbes algebraiques. Definirem els morfismes entre cobres algebraiques i estudiarem les seves propietats. Posteriorment, introduïrem l'espai vectorial de formes diferencials i veurem la relació que té aquesta construcció abstracta amb la teoria que haurem desenvolupat.

1.1 Preliminars

En aquesta secció donarem una sèrie de definicions i resultats que no demostrarem però necessitem com a base i per contextualitzar tot el material que desenvoluparem.

Definició 1.1.1 (Varietat afí). *Siguin K un cos perfecte i $I \subseteq K[x_1, \dots, x_n]$ un ideal. La varietat afí associada a I és el conjunt*

$$V(I) := \{p \in \mathbb{A}^n(\overline{K}) \mid f(p) = 0 \ \forall f \in I\}.$$

Una varietat afí és un conjunt $V(I)$ per a algun ideal I primer.

Definició 1.1.2 (Anell de coordenades). *D'una varietat afí V amb ideal I :*

$$K[V] = K[x_1, \dots, x_n]/I$$

Definició 1.1.3 (Cos de funcions). *D'una varietat V ,*

$$K(V) = \text{Frac}(K[V])$$

Definim també $\overline{K}[V]$ i $\overline{K}(V)$ reemplaçant K per $\overline{K}$ i la dimensió d'una varietat afí com el grau de transcendència de $\overline{K}(V)$ sobre $\overline{K}$.

Definició 1.1.4 (Regular). *El punt $p \in V$ si per a un conjunt de generadors de I $\{f_1, \dots, f_m\} \subset \overline{K}[V]$ la matriu $(\partial f_i / \partial x_j(p))_{i \in \{1, \dots, m\}, j \in \{1, \dots, n\}}$ té rang $n - \dim(V)$. Direm que una varietat V és regular (o no singular, o llisa) si ho és per a tot $p \in V$.*

Definició 1.1.5 (Anell local en p). *Sigui $M_p := \{f \in \overline{K}[V] \mid f(p) = 0\}$ (anell maximal), definim l'anell local de V en p com la localització de $\overline{K}[V]$ en M_p .*

$$\overline{K}[V]_p := \{f/g \in \overline{K}(V) \mid f, g \in \overline{K}[V], g(p) \neq 0\}$$

Un element de $\overline{K}[V]_p$ és una funció regular en p .

Definició 1.1.6 (Espai projectiu). Definim l'espai projectiu de dimensió n sobre $\overline{K}$ com

$$\mathbb{P}^n(\overline{K}) = (\overline{K}^{n+1} \setminus \{0\}) / \sim \quad \text{on} \quad (x_0, \dots, x_n) \sim (y_0, \dots, y_n)$$

si existeix $\lambda \in \overline{K}$ tal que $(x_0, \dots, x_n) = (\lambda y_0, \dots, \lambda y_n)$. Denotem la classe de $(x_0, \dots, x_n)$ per

$$[x_0 : \dots : x_n].$$

Definició 1.1.7 (Varietat projectiva). Sigui

$$I \subseteq \overline{K}[x_0, \dots, x_n]$$

un ideal homogeni.

Definim

$$V(I) = \{p \in \mathbb{P}^n(\overline{K}) \mid f(p) = 0 \ \forall f \in I\}.$$

Una varietat projectiva és un subconjunt de $\mathbb{P}^n(\overline{K})$ de la forma $V(I)$.

Definim per a una varietat projectiva V els conceptes de cos de funcions, anells locals, anell de coordenades a partir d'aquestes definicions per a la varietat afí $V \cap \mathbb{A}^n$.

Definició 1.1.8 (Aplicació racional). Sigui V_1, V_2 dues varietats projectives amb $V_2 \subset \mathbb{P}^n$ una aplicació racional és una aplicació

$$\begin{aligned} \phi : V_1 &\longrightarrow V_2 \\ \phi &= [f_0, \dots, f_n] \end{aligned}$$

on $f_0, \dots, f_n \in \overline{K}(V_1)$

Definició 1.1.9 (Regular). Una aplicació racional $\phi = [f_0, \dots, f_n] : V_1 \longrightarrow V_2$ és regular en p si existeix $g \in \overline{K}(V_1)$ tal que gf_i és regular en p per a tot i , per a algun i , $gf_i(p) \neq 0$. Una aplicació racional regular en tot punt és un morfisme.

Definició 1.1.10 (Corba algebraica). Definim corba algebraica com una varietat projectiva irreductible de dimensió 1

Proposició 1.1.11. Sigui E una corba (algebraica), aleshores per a tot $p \in E$, $\overline{K}[E]_p$ és un anell de valuació discreta.

Definició 1.1.12 (Ordre). Sigui E una corba i p un punt regular definim l'ordre d'una funció $f \in \overline{K}[E]_p$:

$$\text{ord}_p(f) = \max\{d \in \mathbb{Z} \mid f \in M_p^d\}$$

Considerant $\text{ord}_p(f/g) = \text{ord}_p(f) - \text{ord}_p(g)$ estenem la definició d'ordre a $\overline{K}(E)$.

Si $\text{ord}_p(f) > 0$, direm que f té un zero a p , si $\text{ord}_p(f) < 0$, direm que té un pol. Si

Definició 1.1.13 (Uniformitzant). L'element $\tau \in \overline{K}(E)$ és un uniformitzant si $\text{ord}_p(\tau) = 1$. Equivalentment, τ és un generador de M_p .

Proposició 1.1.14. Sigui E una corba llisa i $f \in \overline{K}(E)$. Aleshores f té un nombre finit de pols i zeros. A més, si f no presenta cap pol, $f \in \overline{K}$.

Donat que l'objecte central d'aquest treball són les corbes el·líptiques que com veurem són sempre llises treballarem generalment amb corbes llises. Tenint en compte tots els conceptes definits podem començar.

1.2 Aplicacions entre corbes algebraiques

En aquesta secció, treballarem sobre les aplicacions de corbes algebraiques.

Tot i que al nostre treball ens interessin principalment els resultats sobre isogènies (morfismes de corbes el·líptiques), aquestes són un cas particular d'aplicació de corbes algebraiques així que hem considerat interessant mantenir la generalitat i tractar els conceptes de separabilitat, regularitat a corbes algebraiques (projectives i irreductibles) qualssevol

Començarem veient que una aplicació racional està sempre ben definida per a tots els punts d'ambdues corbes.

Proposició 1.2.1. *sigui E una corba, $V \subset \mathbb{P}^N$ una varietat algebraica, $p \in E$ un punt regular i $\phi : E \rightarrow V$ una aplicació racional. Aleshores ϕ és regular a p . Si E és llisa, aleshores ϕ és un morfisme.*

Demostració. Un a aplicació racional es pot escriure sempre com

$$\phi = [f_0, \dots, f_N] \text{ amb } f_i \in \overline{K}(E)$$

Considerem $\tau \in \overline{K}(E)$ un uniformitzant a p i considerem $m = \min_{0 \leq i \leq N} \{\text{ord}_p(f_i)\}$

Aleshores

$$\text{ord}_p(\tau^{-n} f_i) \geq 0 \quad \forall i \quad \text{i} \quad \text{ord}_p(\tau^{-n} f_j) = 0 \text{ per a algun } j$$

D'aquesta manera cada $\tau^{-n} f_i$ és regular a p i $\tau^{-n} f_j(p) \neq 0$ i, per tant ϕ és regular en p .

□

Donem ara un resultat molt important, que ens permetrà en moltes ocasions simplificar enunciats i poder definir tant el *pullback* com al capítol 3 la isogènia dual:

Teorema 1.2.2. *sigui $\phi : E_1 \rightarrow E_2$ un morfisme de corbes algebraiques. Aleshores ϕ és constant o exhaustiva*

Demostració. Farem servir un argument topològic:

Com E_1 és corba projectiva llisa, un espai complet, $\phi(E_1)$ ha de ser un tancat de Zariski. Recordant, els oberts de Zariski de E_2 són $\{E_2, \emptyset, E_2 \setminus A\}$ on A és un conjunt format per un nombre finit de punts de E_2 . Com $\phi(E_1)$ ha de ser un tancat de Zariski, és a dir, el complementari d'un obert de Zariski tenim 3 possibilitats:

1. $\phi(E_1) = E_2^c = \emptyset$, impossible. Donat que ϕ és una aplicació, la imatge de E_1 no pot ser el conjunt buit.
2. $\phi(E_1) = (E_2 \setminus A)^c = A$. Aleshores $\phi(E_1)$ és un conjunt finit de punts de E_2 . Observem que, en aquest cas, com E_1 és projectiva i llisa, E_1 té una única component connexa, així, la seva imatge no poden ser múltiples punts de E_2 . Per tant, $\phi(E_1) = A = \{p\}$ i ϕ és constant.
3. $\phi(E_1) = \emptyset^c = E_2$.

Recuperant, tenim que, donades E_1, E_2 corbes llises i $\phi : E_1 \rightarrow E_2$ un morfisme,

$$\phi(E_1) = q \in E_2 \text{ (constant), o bé } \phi(E_1) = E_2 \text{ (exhaustiva).}$$

□

Ara, l'exhaustivitat dels morfismes no constants de corbes ens permetrà definir el *pullback*, que serà un objecte central a l'estudi de corbes algebraiques ja que ens permetrà relacionar cada morfisme de corbes amb una extensió algebraica de cossos.

Definició 1.2.3. *Siguin $E_1/K, E_2/K$ dues corbes i $\phi : E_1 \longrightarrow E_2$ aplicació no constant definida sobre K . Anomenarem pullback a la següent aplicació induïda per ϕ :*

$$\phi^* : K(E_2) \longrightarrow K(E_1)$$

$$\phi^*(f) \longmapsto f \circ \phi$$

Teorema 1.2.4. *Siguin E_1, E_2 corbes definides sobre un cos K .*

- i) Siguí $\phi : E_1 \longrightarrow E_2$ una aplicació no constant definida sobre K . Aleshores $K(E_1)$ és una extensió (algebraica) finita de $\phi^*(K(E_2))$.*
- ii) Siguí $\iota : K(E_2) \longrightarrow K(E_1)$ una injecció de cossos de funcions fixant K . Aleshores existeix una única aplicació no constant $\phi : E_1 \longrightarrow E_2$ (sobre K) tal que*

$$\phi^* = \iota$$

- iii) Siguí ara $F \subset K(E_1)$ subcos d'índex finit contenint K . Aleshores existeix una única corba projectiva E_2/K (tret de K -isomorfisme) i una aplicació no-constant $\phi : E_1 \longrightarrow E_2$ definida sobre K tal que*

$$\phi^*(K(E_2)) = F$$

Demostració. i) Com ϕ és exhaustiva, induïx una injecció $\phi^*(K(E_2)) \hookrightarrow K(E_1)$. Ara com els dos cossos son extensions finitament generades de K amb grau de transcendència 1, $K(E_1)$ ha de ser una extensió algebraica i finita de $\phi^*(K(E_2))$.

- ii) Siguí $E_2 \subset \mathbb{P}^N$ i, per a cada $i = 1, \dots, N$, considerem $g_i \in K(E_2)$ la funció corresponent a la X_i/X_0 -èssima coordenada. Aleshores

$$\phi : [1, \iota g_1, \dots, \iota g_N]$$

defineix una aplicació $\phi : E_1 \longrightarrow E_2$ tal que $\phi^* = \iota$. Ara ϕ és no constant ja que les g_i no ho son i ι és injectiva.

Suposem ara $\psi = [f_0, \dots, f_N]$ una altra aplicació tal que $\psi^* = \iota$. Repetint el procediment, per a cada i :

$$f_i/f_0 = \psi^*(g_i) = \iota(g_i) = \phi^*(g_i)$$

Amb el que $\phi = \psi$

- iii) Sense les eines necessàries, direm que hi ha una bijecció entre extensions finites de cossos de funcions i aplicacions de corbes algebraiques. Així es pot construir E_2/K com la corba tal que el seu cos de funcions satisfà $\phi^*(K(E_2)) = F$.

□

Hem vist, que donat un morfisme entre corbes algebraiques $\phi : E_1 \longrightarrow E_2$, el *pullback* dona una injecció $\phi^* : K(E_2) \hookrightarrow K(E_1)$ i que la relació entre aquests cossos és una extensió finita. Per altra banda, hem vist que per a cada parell de cossos de funcions i K -morfisme entre ells existeix una única aplicació de corbes associada. Així veiem que és raonable associar de manera directa un morfisme de corbes a l'extensió de cossos generada a partir del *pullback*. Nocions com la de separabilitat que treballarem i seran centrals en la teoria que desenvoluparem seran definides a partir del *pullback* i el seu efecte sobre els cossos de funcions de les corbes. Per molt que més endavant parlem només d'aplicacions entre corbes i treballem amb les propietats d'aquestes, cal que recordem que remeten a l'estructura subjacent del *pullback* i els cossos de funcions.

Passem a definir aquests conceptes:

Definició 1.2.5. *Sigui $\phi : E_1 \longrightarrow E_2$ una aplicació de corbes definida sobre K no constant. Direm que és finita i definirem el seu grau com*

$$\deg(\phi) = [K(E_1) : \phi^* K(E_2)]$$

Observem que el grau serà un nombre enter positiu (ja que com hem vist l'extensió serà finita). Si ϕ és constant direm que té grau 0.

Definició 1.2.6. *Direm que $\phi : E_1 \longrightarrow E_2$ és separable, no-separable, purament inseparable si l'extensió*

$$\begin{array}{c} K(E_1) \\ \downarrow \\ \phi^*(K(E_2)) \end{array}$$

és separable, no separable o purament inseparable.

Definirem també els graus separable ($\deg_s$) i inseparable ($\deg_i$) de ϕ com els graus separable i inseparable de l'extensió.

Donem primerament un exemple natural que serà molt útil per a propers resultats:

Exemple 1.2.7. Sigui E/K una corba projectiva llisa i $f \in K(E)$ una funció. Aleshores existeix una aplicació racional, induïda per f , que, abusant de notació, també anomenarem f :

$$\begin{aligned} f : E &\longrightarrow \mathbb{P}^1 \\ p &\longmapsto [f(p), 1] \end{aligned} \tag{1.2.1}$$

Aquesta aplicació és un morfisme de corbes. Es pot considerar també com

$$f(p) = \begin{cases} [f(p), 1] & \text{si } f \text{ és regular en } p \\ [1, 0] & \text{si } f \text{ té un pol en } p \end{cases}$$

Havent definit el *pullback* hem passat a treballar amb $K(E_2)$ com a cos principal, o de sortida. Ens serà interessant una mena d'invers.

Definició 1.2.8. *Sigui $\phi : E_1 \longrightarrow E_2$ una aplicació no constant de corbes definida sobre K . Definim*

$$\begin{aligned} \phi_* : K(E_1) &\longrightarrow K(E_2) \\ \phi_* &= (\phi^*)^{-1} \circ N_{K(E_1)/\phi^* K(E_2)} \end{aligned}$$

Recordem la norma d'un element respecte d'una extensió de cossos:

Donat B un A -mòdul lliure finit, la norma d'un element $x \in B$ és el determinant de la matriu associada a l'aplicació multiplicació per x en alguna A -base de B .

Pel que acabem de demostrar, $K(E_1)$ serà sempre un $\phi^*K(E_2)$ -mòdul lliure i clarament finit. Observem un resultat que s'escapa pràcticament de les definicions donades:

Proposició 1.2.9. *Siguin E_1, E_2 corbes projectives i sigui $\phi : E_1 \rightarrow E_2$ aplicació de grau 1. Aleshores ϕ és un isomorfisme*

Demostració. Per la definició de grau, $\deg(\phi) = 1 \implies \phi^*K(E_2) = K(E_1)$ i, per tant ϕ^* és un isomorfisme. Considerem $(\phi^*)^{-1} : K(E_1) \rightarrow K(E_2)$ l'invers del *pullback* que és, particularment un K -morfisme de cossos.

Pel resultat que hem vist prèviament, sabem que existeix una única aplicació no constant $\psi : E_2 \rightarrow E_1$ tal que $\psi^* = (\phi^*)^{-1}$.

Aleshores:

$$\psi^* \circ \phi^* = (\phi \circ \psi)^* = \text{Id}_{K(E_2)} \quad , \quad \phi^* \circ \psi^* = (\psi \circ \phi)^* = \text{Id}_{K(E_1)}$$

Ara, per a cada identitat, podem considerar el fet que existeix una única aplicació $f_i : E_i \rightarrow E_i$ tal que $f_i^* = \text{Id}_{K(E_i)}$. S'observa immediatament que l'aplicació identitat satisfà la condició i, per tant:

$$\phi \circ \psi = \text{Id}_{E_2} \quad , \quad \psi \circ \phi = \text{Id}_{E_1}$$

Hem arribat doncs, a que ϕ (i ψ) és un isomorfisme. □

Observació 1.2.10. Sense aprofundir massa, mencionarem que la relació tan estreta entre les aplicacions entre corbes i els seus *pullbacks*, més enllà de per la manera en què les definim està justificada pel fet que existeix una equivalència de categories entre

$$\mathcal{C}_1 = \begin{cases} \text{Objectes: } \{E/K, \text{ corbes projectives sobre } K\} \\ \text{Morfismes: } \{\phi : E_1 \rightarrow E_2, \text{ aplicacions racionals no constants}\} \end{cases}$$

i

$$\mathcal{C}_2 = \begin{cases} \text{Objectes: } \{\text{Extensions } \mathcal{K}/K \text{ transcendents de grau 1 amb } \mathcal{K} \cap \overline{K} = K\} \\ \text{Morfismes: } \{\text{Morfismes de cossos fixant } K \text{ (} K\text{-morfismes)}\} \end{cases}$$

1.2.1 Ramificació

Hem observat propietats i caracteritzacions globals de les aplicacions entre corbes. Sabent que (gairebé) tota aplicació de corbes és exhaustiva, ens serà interessant estudiar com pot ser el comportament local d'una aplicació finita entre corbes algebraiques i com es pot relacionar aquest amb característiques globals de la corba.

Comencem definint el concepte de ramificació que com veurem, és anàlog al comportament dels primers i la seva descomposició en (extensions de) cossos de nombres.

Definició 1.2.11. Sigui $\phi : E_1 \longrightarrow E_2$ una aplicació finita entre corbes projectives, i sigui $p \in E_1$. Definim l'índex de ramificació de ϕ a p com:

$$e_\phi(p) = \text{ord}_p(\phi^* \tau_{\phi(p)})$$

on $\tau_{\phi(p)} \in \overline{K}(E_2)$ és un uniformitzant a $\phi(p)$.

Ràpidament s'observa, $e_\phi(p) \geq 1$. Aleshores direm que p és no-ramificat (o bé que ϕ no ramifica en p) si $e_\phi(p) = 1$.

Direm que ϕ és no ramificada si ho és a tot $p \in E_1$.

Vegem com es relaciona aquest concepte amb les qualitats que sabem definir d'un morfisme finit de corbes algebraiques:

Proposició 1.2.12. Sigui $\phi : E_1 \longrightarrow E_2$ una aplicació no constant de corbes projectives, aleshores:

i) Per a cada $q \in E_2$,

$$\sum_{p \in \phi^{-1}(q)} e_\phi(p) = \deg(\phi)$$

ii) Per a tot, tret d'un nombre finit, $q \in E_2$,

$$\#\phi^{-1}(q) = \deg_s(\phi)$$

iii) Sigui ara $\psi : E_2 \longrightarrow E_3$ una altra aplicació no constant, $\forall p \in E_1$,

$$e_{(\psi \circ \phi)}(p) = e_\phi(p) e_\psi(\phi(p))$$

Demostració. i) Es segueix del següent lema que podem trobar a [3]:

Lema 1.2.13. Sigui A un anell de Dedekind, K el seu cos de fraccions, L/K una extensió finita. Sigui B la clausura entera de A en L . Aleshores sigui $\mathfrak{p}$ un primer de A . Aleshores

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$$

on $\mathfrak{P}$ son els ideals primers en els quals descomposa $\mathfrak{p}B$, $e_{\mathfrak{P}}$ l'índex de ramificació de l'ideal $\mathfrak{P}$ (potència amb la que $\mathfrak{P}$ apareix a la descomposició de $\mathfrak{p}B$) i $f_{\mathfrak{P}}$ el grau de l'extensió de cossos residuals $B/\mathfrak{P}$ sobre $A/\mathfrak{p}$.

Veiem aquest lema demostra el que volíem.

Observem que volem que $K = \phi^*(K(E_2))$ i $L = K(E_1)$, l'extensió és encara finita. Ara sigui A l'anell $\phi^*(K[E_2])$ format per les imatges de les funcions regulars de $K(E_2)$ en E_2 . Observem que si considerem B l'anell de funcions regulars de E_1 tenim que B és enter sobre A ja que una aplicació finita es pot caracteritzar a partir de que $K[E_1]$ sigui enter sobre $\phi^*(K[E_2])$ [7]. Observem $\phi^*(K[E_2]), K[E_1]$ són anells de Dedekind.

Ara, podem identificar cada punt p de E_1 (i $q \in E_2$) amb l'ideal de funcions regulars en p ($\mathfrak{p}_p$), ideal clarament primer, denotem $\mathfrak{P}_p$. Observem que

$$\forall p \in \phi^{-1}(q), \phi^*(\mathfrak{P}_q) = \mathfrak{p}_p \subset \mathfrak{P}_p$$

i $\mathfrak{p}$ descomposa en primers $\mathfrak{P}_p$ que apareixen amb potència $e_\phi(p)$. Finalment, el cos residual de localitzar per $\mathfrak{p}$, $\mathfrak{P}$ és K tant per $K[E]$ com per a $\phi^*(K[E_2])$ i $f_{\mathfrak{P}_p} = 1$. Així, recordant que $\deg(\phi) = [K(E_1) : \phi^*(K(E_2))]$,

$$\deg(\phi) = \sum_{p \in \phi^{-1}(q)} e_\phi(p)$$

ii) Es pot deduir de la fórmula de Riemann-Hurwitz que no arribem a introduir en aquest treball.

iii) Siguin $\tau_{\phi(p)}, \tau_{\psi(\phi(p))}$ uniformitzants a $\phi(p)$ i $\psi(\phi(p))$ respectivament.

Ara $\tau_{\phi(p)}$ té ordre 1 a $\phi(p) \implies \tau_{\phi(p)}^{e_\psi(\phi(p))}$ té ordre $e_\psi(\phi(p))$ que és $\psi^* \tau_{\psi(\phi(p))}$. Obtenim

$$\text{ord}_{\phi(p)} \left(\tau_{\phi(p)}^{e_\psi(\phi(p))} \right) = \text{ord}_{\phi(p)} \left(\psi^* (\tau_{\psi(\phi(p))}) \right)$$

Aplicant ϕ^* a ambdós elements de $K(E_2)$, i prenent l'ordre a p obtenim:

$$\begin{aligned} e_\phi(p) e_\psi(\phi(p)) &= e_\psi(\phi(p)) \text{ord}_p(\phi^*(\tau_{\phi(p)})) \\ &= \text{ord}_p \left(\phi^* \left(\tau_{\phi(p)}^{e_\psi(\phi(p))} \right) \right) \\ &= \text{ord}_p \left((\psi \circ \phi)^* (\tau_{\psi(\phi(p))}) \right) \\ &= e_{(\psi \circ \phi)}(p). \end{aligned}$$

□

Corol·lari 1.2.14. Una aplicació $\phi : E_1 \longrightarrow E_2$ és no ramificada si i només si $\#\phi^{-1}(q) = \deg(\phi) \quad \forall q \in E_2$

Demostració. De i) tenim

$$\sum_{p \in \phi^{-1}(q)} e_\phi(p) = \deg(\phi) = \#\phi^{-1}(q)$$

és a dir, la suma dels índexos de ramificació de les antiimatges de q i la quantitat d'antiimatges son iguals. Com $e_\phi(p) \geq 1$ tenim que necessàriament $\forall q \in E_2, e_\phi(p) = 1 \quad \forall p \in \phi^{-1}(q)$ i ϕ és, per tant, no ramificada □

1.2.2 El morfisme de Frobenius

Sabem que per a una extensió de cossos no separable qualsevol K/F existeix un cos intermig L , $F \subset L \subset K$ tal que L/F és separable i K/L inseparable.

Els cossos de funcions, per ser cossos, també tenen aquesta propietat tot i que no tinguem a priori, informació sobre el cos intermig. El morfisme de Frobenius ens donarà aquesta estructura.

Sabem que en un cos de característica 0, tots els polinomis irreductibles son separables. Així si estem considerant corbes definides sobre K amb $\text{char}(K) = 0$, les extensions de $K(E)$ seran separables per a qualsevol corba E . Així per a aquesta secció considerem el cos base K de característica $p > 0$ i fixarem $q = p^r$.

Per començar, considerem per a qualsevol polinomi $f \in K[x]$, $f^{(q)}$ obtingut elevant els coeficients de f a q .

Ara donada una corba E/K qualsevol definim la corba $E^{(q)}/K$ prenent com a ideal homogeni de $E^{(q)}$ l'ideal generat per $\{f^{(q)} : f \in I(E)\}$ essent $I(E)$ l'ideal homogeni definint E .

Prenem ara un element qualsevol de $E, [x_0, \dots, x_n]$ i $f \in I(E)$ tal que $f(x_0, \dots, x_n) = 0$. Observem ara però que donat que treballem sobre un cos de característica $p \mid q$,

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

A partir d'aquest fet definim el (q -èssim) morfisme de Frobenius com

$$\begin{aligned} \phi : E &\longrightarrow E^{(q)} \\ [x_0, \dots, x_n] &\longmapsto [x_0^q, \dots, x_n^q] \end{aligned}$$

Proposició 1.2.15. *Si $K = \mathbb{F}_q$, el q -èssim morfisme de Frobenius és un endomorfisme.*

Demostració. Recordant que $\forall x \in \mathbb{F}_q, x^q = x$ tenim que donat un polinomi $f \in \mathbb{F}_q[x]$, $f^{(q)} = f$. Efectivament:

$$\text{si } f = \sum a_i x^i, f^{(q)} = \sum a_i^q x^i \text{ on } a_i^q = a_i \text{ i, per tant } f^{(q)} = \sum a_i x^i = f$$

amb el que les corbes $E, E^{(q)}$ comparteixen ideal homogeni i son, per tant, el mateix objecte $\square$

Proposició 1.2.16. *Sigui $\phi : E \longrightarrow E^{(q)}$ el q -èssim morfisme de Frobenius sobre un cos finit K de característica p . Sigui $q = p^r$.*

1. *El morfisme ϕ és purament inseparable*
2. *$\phi^*(K(E^{(q)})) = K(E)^q := \{f^q : f \in K(E)\}$*
3. *$\deg(\phi) = q$*

Demostració. Comencem veient com es comporta el cos de funcions de $E^{(q)}$ respecte el *pullback* induït pel morfisme de Frobenius: Treballant amb $E^{(q)}, E$ com a varietats projectives recordem que una definició pel cos de funcions és el cos format per quocients de polinomis homogenis del mateix grau.

Així, per la definició del 'pullback' (composar amb ϕ) observem que per a un element qualsevol $f/g \in K(E^{(q)})$,

$$\phi^*(f/g) = f(X_0^q, \dots, X_n^q)/g(X_0^q, \dots, X_n^q)$$

Per altra banda els elements de $K(E)^q$ son de la forma: $f(X_0, \dots, X_n)^q/g(X_0, \dots, X_n)^q$ on, com K és un cos finit, per a qualsevol polinomi f

$$f(X_0, \dots, X_n)^q = g(X_0^q, \dots, X_n^q)$$

amb el coeficients de g essent les potències q -èssimes dels coeficients de f . Així, els subcossos $\phi^*(K(E^{(q)}))$ i $K(E)^q$ tenen els mateixos elements i

$$\phi^* : K(E^{(q)}) \longrightarrow K(E)^q$$

la restricció, és una aplicació bijectiva de cossos. Hem vist *ii*), ara observem ràpidament que l'extensió

$$K(E)/\phi^*(K(E^{(q)})) = K(E)/K(E)^q$$

és purament inseparable amb el que ϕ és purament inseparable.

Vegem ara el grau de ϕ . Considerem un uniformitzant $\tau \in K(E)$ en algun punt regular $p \in E$. Sabem que $K(E)/K(\tau)$ és una extensió separable.

Tenim el següent diagrama:

$$\begin{array}{ccc} & K(E) & \\ & \downarrow & \\ & K(E)^q(\tau) & \\ & \swarrow \quad \searrow & \\ K(E)^q & & K(\tau) \end{array}$$

on

$$[K(E) : K(E)^q(\tau)] = 1$$

amb el que

$$\deg(\phi) = [K(E)^q(\tau) : K(E)^q]$$

Tenim que $\tau^q \in \overline{K}(E)^q$, aleshores el grau de l'extensió serà com a molt q (ja que τ és arrel de $X^q - \tau^q \in \overline{K}(E)^q[x]$) així és prou veure que cap potència de τ menor a τ^q és a $K(E)^q$.

Sigui τ^a amb $a = p^s$, $s < r$. Si $a \in K(E)^q$, $\exists f \in K(E)$ tal que $f^q = \tau^a$ i

$$p^s = a = \text{ord}_p(\tau^a) = \text{ord}_p(f^q) = q * \text{ord}_p(f) = p^r * \text{ord}_p(f)$$

que és una contradicció.

□

Corol·lari 1.2.17. *Qualsevol aplicació $\psi : E_1 \longrightarrow E_2$ entre corbes llises sobre un cos K de característica $p > 0$ factoritza pel $\deg(\psi)$ -èssim morfisme de Frobenius.*

$$E_1 \xrightarrow{\phi} E_1^{(q)} \xrightarrow{v} E_2$$

on $q = \deg_i(\psi)$ i ϕ denota el q -èssim morfisme de Frobenius i v és separable

Demostració. Considerem L la clausura separable de $\psi^*(E_2)$ a $K(E_1)$. Aleshores $K(E_1)/L$ és una extensió purament inseparable de grau q , amb el que $K(E_1)^q \subseteq L$, però pel que acabem de provar

$$K(E_1)^q = \phi^*(K(E_1^{(q)})) \text{ , i també } [K(E_1) : \phi^*(K(E_1^{(q)}))] = q$$

Així, $L = \phi^* \left(K(E_1^{(q)}) \right)$ (tret de K -isomorfisme), així, tenim una torre:

$$\begin{array}{c} K(E_1) \\ | \\ \phi^* \left(K(E_1^{(q)}) \right) \\ | \\ \phi^* \left(K(E_2) \right) \end{array}$$

I només cal aplicar el fet que donat un K -morfisme de cossos de funcions $\iota : K(E_2) \longrightarrow K(E_1^{(q)})$, es pot trobar una aplicació $v : E_1^{(q)} \longrightarrow E_2$ amb $v^* = \iota$. Obtenim, per tant:

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_1^{(q)} \\ & \searrow \psi & \downarrow v \\ & & E_2 \end{array}$$

On ϕ és com sabem, purament inseparable, i v per construcció, separable. $\square$

1.3 Diferencials

En aquesta secció introduïrem el concepte de forma diferencial sobre una corba i l'espai vectorial que formen. Inicialment veurem com fan la funció de linearització amb els morfismes de corbes de manera anàloga a com funcionen les diferencials treballant en un context més analític. Observarem que les diferencials ens donaran un criteri més accessible per a quan una aplicació és separable que farem servir de manera recurrent. Al capítol 2 tractarem la definició de divisor d'una diferencial i més endavant, al capítol 4 farem servir la diferencial invariant, una construcció per a corbes elíptiques que ens permetrà de manera molt elegant arribar a un resultat sobre la separabilitat d'una aplicació on apareix l'endomorfisme de Frobenius que serà clau per al resultat final d'aquest treball.

Així, concernint aquest treball, els diferencials no seran tant un objecte d'estudi si no més, com veurem, una eina que ens permetrà simplificar caracteritzacions i càlculs.

Definició 1.3.1. *Definirem l'espai de formes diferencials sobre una corba E , que notarem com Ω_E , l'espai vectorial sobre $\overline{K}(E)$ generat per "símbols dx per a $x \in \overline{K}(E)$ complint les propietats:*

- i) $d(x + y) = dx + dy \quad \forall x, y \in \overline{K}(E)$ (Condicció de linealitat)
- ii) $d(xy) = xdy + ydx \quad \forall x, y \in \overline{K}(E)$ (Regla de Leibniz)
- iii) $dx = 0 \quad \forall x \in \overline{K}$ (Anulació de constants)

Anomenarem als elements d'aquest espai, diferencials o formes diferencials

Ara, recordant el *pullback* induït per una aplicació entre corbes definirem un morfisme entre espais de formes diferencials induït de manera similar que ens permetrà, entre

d'altres, tenir un criteri per a determinar quan un morfisme de corbes és separable en qüestió del *pullback* en l'espai vectorial de formes diferencials, que és una estructura més amigable que la dels cossos de funcions.

Definició 1.3.2. *Sigui $\phi : E_1 \longrightarrow E_2$ aplicació no constant entre corbes, i el pullback $\phi^* : \overline{K}(E_2) \longrightarrow \overline{K}(E_1)$, definim l'aplicació induïda per a diferencials:*

$$\begin{aligned} \phi^\dagger : \Omega_{E_2} &\longrightarrow \Omega_{E_1} \\ \phi^\dagger \left(\sum f_i dx_i \right) &= \sum (\phi^*(f_i)) d(\phi^*(x_i)) \end{aligned}$$

Amb l'objectiu de demostrar el següent resultat:

Proposició. *Sigui $\phi : E_1 \longrightarrow E_2$ una aplicació no constant entre corbes, aleshores ϕ és separable si i només si l'aplicació:*

$$\phi^\dagger : \Omega_{E_2} \longrightarrow \Omega_{E_1}$$

és injectiva.

Necessitarem certs resultats sobre la dimensió de Ω_E com a $\overline{K}(E)$ i $\overline{K}(x)$ -espai vectorial per a $x \in \overline{K}(E)$. Les eines usades per a la demostració d'aquests resultats escapen al que podem incloure en aquest treball així que partirem com a lema d'una caracterització que trobem a [6] per a la relació entre $\dim_K(\Omega_{K/F})$ i $\dim_L(\Omega_{L/F})$ on $L = K(t)$ una extensió, clarament finita.

La demostració d'aquesta caracterització es dona a partir de propietats pròpies de Ω_E , extensions de cossos i del producte tensorial, objecte que no presentarem en aquest treball però que és suficient per a provar els punts que necessitem.

Canviant lleugerament la notació, al Matsumura trobem:

Lema 1.3.3. *Sigui F un cos i K/F una extensió. Denotarem per $r(K) = \dim_K(\Omega_{K/F})$ el rang (o bé dimensió) de Ω com a K -espai vectorial. Sigui $L = K(t)$. Tenim 4 possibilitats:*

1. *Si t és transcendent sobre K , aleshores $r(L) = r(K) + 1$*
2. *Si t és algebraic i separable sobre K , aleshores $r(L) = r(K)$*
3. *Si $\text{char}(F) = p$, $t^p = a \in K$ i $d(a) = 0$, aleshores $r(L) = r(K) + 1$*
4. *Si $\text{char}(F) = p$, $t^p = a \in K$ però $d(a) \neq 0$, aleshores $r(L) = r(K)$*

En els cassos 3 i 4, tenim que L/K és una extensió purament inseparable. La diferència és la qualitat de l'element a respecte de les diferencials. Podem prendre com a intuïció el fet que en el cas 3, a és una 'constant' i quan adjuntem t , estem dotant K d'un nou element amb una diferencial K -linealment independent als de Ω_K i així el rang augmenta. A l'últim cas però no es dona així a no és nul per a les diferencials aleshores on tindrem que $d(a) = xd(t)$ per a algun $x \in \Omega_K$.

Corol·lari 1.3.4. *Sigui F un cos, K una extensió de F i L una extensió finita de K . Aleshores*

$$\dim_L(\Omega_{L/F}) \geq \dim_K(\Omega_{K/F}) + \deg(L/K)_{tr}$$

Demostració. Tota extensió finita de K es pot obtenir repetint extensions dels 4 tipus mencionats abans. Observant que com la dimensió en cap cas baixa, clarament $\dim_L(\Omega_{L/F}) \geq \dim_K(\Omega_{K/F})$. A més, pel cas 1 observem que per cada element transcendent que afegim, la dimensió de l'espai de formes diferencials augmenta. Obtenim per tant el resultat. $\square$

Teorema 1.3.5. *Sigui L una extensió finita de F . Aleshores*

$$\dim_L(\Omega_{L/F}) \geq \deg_{tr}(L/F)$$

I és una igualtat si i només si L és una extensió separablement generada sobre F .

El concepte de *Separablement generada* és, en el cas d'extensions transcendents, una extensió K/F on existeixen elements $x_1, \dots, x_n$ tal que $K/F(x_1, \dots, x_n)$ és una extensió separable i algebraica.

Observem que si l'extensió K/F és algebraica, separablement generada i separable son equivalents, que és la situació que ens serà més important.

Demostració. L'enunciat del teorema és un cas particular de la desigualtat previa.

Suposem que $\dim_L(\Omega_{L/F}) = 0$, per a qualsevol K cos intermig $F \subseteq K \subseteq L$ l'extensió L/K no correspon als cassos 1 i 3 del lema. Tampoc és possible el cas 4 ja que $\dim_L(\Omega_{L/F}) = 0 \implies \dim_K(\Omega_{K/F}) = 0$ aleshores no es pot trobar a $a \in K$ tal que $d(a) \neq 0$ (ja que l'existència d'aquest $a \implies \dim_K(\Omega_{K/F}) \geq 1$). Així, ens trobem en cas 2 i L és una extensió algebraica i separable de F ja que K/L és algebraica i separable per a qualsevol cos intermig.

Suposem ara que $\dim_L(\Omega_{L/F}) = r = \deg_{tr}(L/F)$. Aleshores prenem $x_1, \dots, x_r \in L$ tals que $\{d(x_1), \dots, d(x_r)\}$ sigui una L -base de $\Omega_{L/F}$. Considerem ara el fet que $\Omega_{L/F(x_1, \dots, x_r)} = 0$ i, pel que acabem de veure $L/F(x_1, \dots, x_r)$ és una extensió algebraica i finita i, per tant, L/F és extensió separablement generada. $\square$

Observació 1.3.6. Donada una extensió de cossos finita L/K , $\dim_L(\Omega_{L/K}) = 0$ si i només si L/K és una extensió algebraica separable.

Aquests resultats son suficients per a, recuperant el llenguatge, poder demostrar:

Proposició 1.3.7. *Sigui E una corba, aleshores:*

- i) Ω_E és $\overline{K}(E)$ -espai vectorial de dimensió 1.
- ii) *Sigui $x \in \overline{K}(E)$, aleshores $d(x)$ és base de Ω_E si i només si $\overline{K}(E)/\overline{K}(x)$ és una extensió finita i separable.*
- iii) *Sigui $\phi : E_1 \longrightarrow E_2$ una aplicació no constant entre corbes, aleshores ϕ és separable si i només si l'aplicació:*

$$\phi^\dagger : \Omega_{E_2} \longrightarrow \Omega_{E_1}$$

és injectiva.

Demostració. i) Directament del teorema anterior. Considerant $L = \overline{K}(E)$, $F = \overline{K}$, i recordant que el cos de funcions d'una corba és una extensió de $\deg_{tr} = 1$ i clarament separablement generada sobre $\overline{K}$, el cos base, tenim:

$$\dim_{\overline{K}(E)}(\Omega_{E/\overline{K}}) = \deg_{tr}(\overline{K}(E)/\overline{K}) = 1$$

on notem $\Omega_{E/\overline{K}}$ per a especificar a $\overline{K}$ com a cos base.

ii) Tenim que si $\overline{K}(E)/\overline{K}(x)$ és una extensió finita i separable

$$\dim_{\overline{K}(x)}\Omega = \dim_{\overline{K}(E)}\Omega = 1$$

Aleshores com $d(x)$ clarament és base per a Ω_E com a $\overline{K}(x)$ -espai vectorial, també ho serà sobre $\overline{K}(E)$.

iii) Fent servir els dos punts previs escollim $y \in \overline{K}(E_2)$ de manera que $d(y)$ sigui $\overline{K}(E_2)$ -base de Ω_{E_2} . Ara $\phi^*(\overline{K}(E_2))$ és separable sobre $\overline{K}(\phi^*(y))$. Aleshores:

$\phi^\dagger$ és injectiva $\iff d(\phi^*(y)) \neq 0$. Donat que $\dim_{\overline{K}(E_1)}(\Omega_{E_1}) = 1$ tenim que $d(\phi^*(y))$ és una base de Ω_{E_1} alhora això és $\iff \overline{K}(E_1)/\overline{K}(\phi^*(y))$ és separable i, com hem vist que $\phi^*(\overline{K}(E_2))/\phi^*(y)$ és separable: $\overline{K}(E_1)/\overline{K}(\phi^*(y))$ és separable $\iff \overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ és separable.

□

La següent proposició donarà lloc a poder formular una bona definició de l'ordre d'un diferencial:

Proposició 1.3.8. *Sigui $p \in E$ i sigui $\tau \in \overline{K}(E)$ un uniformitzant a p .*

- i) *Per a cada $\omega \in \Omega_E$ existeix una única funció $f \in \overline{K}(E)$ (fixats ω, τ) tal que $\omega = fd(\tau)$. Denotarem f com $\omega/d\tau$.*
- ii) *Sigui $f \in \overline{K}(E)$ una funció regular a p . Aleshores $d(f)/d\tau$ és també regular a p .*
- iii) *Sigui $\omega \in \Omega_E$, la quantitat*

$$\text{ord}_p(\omega/d\tau)$$

és independent de l'uniformitzant τ . Anomenarem a aquesta quantitat $\text{ord}_p(\omega)$ l'ordre de ω a p

Demostració. i) Recordant que, si $\tau \in \overline{K}(E)$ és un uniformitzant aleshores $\overline{K}(E)/\overline{K}(\tau)$ és una extensió separable (algebraica) i recordant la definició de base d'un espai vectorial obtenim el resultat.

- ii) Recordant els conceptes d'anell local a p , i que un uniformitzant és un generador de l'ideal maximal ($M_p \subset \overline{K}[E]_p$), donat que f és regular, podem escriure $f = \sum a_i \tau^i$ amb $i \geq 0$. Podem considerar (de manera general, per a qualsevol funció si tenim en compte potències negatives de τ) la diferencial de f sobre $\overline{K}(\tau)$ considerant les diferencials terme a terme. Ara $d_{\overline{K}(\tau)}(f)$ no té cap potència negativa de τ . Alhora, sabem que $\overline{K}(E)/\overline{K}(\tau)$ és una extensió finita i separable, per tant $d(\tau)$ és una $\overline{K}(E)$ -base de Ω_E i

$$d_{\overline{K}(\tau)}(f) \equiv d(f)/d\tau \in \overline{K}(E)$$

per definició.

Clarament, $d(f)/d\tau \in \overline{K}[E]_p$ i obtenim el resultat.

iii) Sigui $t \in \overline{K}(E)$ un altre uniformitzant a p , per l'apartat anterior, tenim que tant $d(t)/d\tau$ com $d(\tau)/dt$ son regulars a p , i, per tant $\text{ord}_p(d(t)/d\tau) = 0$. Aleshores donat que

$$\omega = gd(t) = g(d(t)/d\tau)d(\tau)$$

obtenim el resultat

□

Veiem ara una propietat molt útil per al càlcul de l'ordre d'una diferencial així com una demostració on es veu clarament com es pot fer servir la maquinària definida per a facilitar el càlcul.

Proposició 1.3.9. *Siguin $f, g \in \overline{K}(E)$ amb $g(p) = 0$. Sigui ara $q = \text{char}(K)$. Aleshores:*

$$\begin{aligned} \text{ord}_p(fd(g)) &= \text{ord}_p(f) + \text{ord}_p(g) - 1 & \text{si } q = 0 \text{ o } q \nmid \text{ord}_p(g) \\ \text{ord}_p(fd(g)) &\geq \text{ord}_p(f) + \text{ord}_p(g) & \text{si } q > 0 \text{ o } q \mid \text{ord}_p(g) \end{aligned}$$

Demostració. Donat τ un uniformitzant a p , considerem $g = u\tau^n$ amb $n = \text{ord}_p(g) \geq 1$ per definició. Aleshores $\text{ord}_p(u) = 0$. Calculem,

$$d(g) = (nu\tau^{n-1} + (d(u)/d\tau)\tau^n) d(\tau).$$

Ara $d(u)d\tau$ és regular a p pel resultat que acabem de veure. Així donat $n \neq 0$ l'ordre vindrà donat pel primer terme de la suma i obtenim la igualtat:

$$\text{ord}_p(fd(g)) = \text{ord}_p(fun\tau^{n-1}d(\tau)) = \text{ord}_p(f) + (n - 1)$$

Finalment, si $q > 0$ i $q \mid n$ el primer terme de la suma és idènticament zero i, per tant

$$\text{ord}_p(fd(g)) = \text{ord}_p(f(d(u)/d\tau)\tau^n d(\tau)) \geq \text{ord}_p(f) + n.$$

□

Capítol 2

Divisors i Riemann-Roch

En aquest capítol introduïrem el concepte de divisor d'una corba. Els divisors (de manera més general) es poden entendre com una generalització de la factorització de primers en un context de teoria de nombres algebraica i esdevenen una eina important en teoria d'esquemes, on es diferencien divisors de Weil i de Cartier. Tot i que hi ha molta teoria rere els divisors, nosaltres els definirem com un objecte purament abstracte i veurem, amb la relació entre divisors, funcions i diferencials la intuïció que pot haver-hi sota la definició formal del grup de divisors d'una corba. Els grups de divisors ens permetran establir una interessant relació entre corbes algebraiques i cossos de nombres i finalment, podrem arribar al teorema de Riemann-Roch d'on obtindrem la definició de gènere d'una corba i que serà d'extrema importància per a la teoria que desenvoluparem més endavant.

2.1 Divisors

Definició 2.1.1. *Definim el grup de divisors d'una corba E : $\text{Div}(E)$ com el grup abelià lliure generat pels punts de E . Així, un divisor $D \in \text{Div}(E)$ es una suma formal de punts de E . Podem escriure un divisor D com:*

$$D = \sum_{p \in E} a_p(p)$$

amb $a_p \in \mathbb{Z}$, $a_p = 0$ per a tot p tret d'un nombre finit.

Definim també l'ordre d'un divisor $D \in \text{Div}(E)$ com la suma dels coeficients:

$$\deg(D) = \sum_{p \in E} a_p$$

Observem ràpidament que la suma de dos divisors de grau 0 ha de ser un divisor de grau zero.

Definició 2.1.2. *Definim el subgrup:*

$$\text{Div}^0(E) := \{D \in \text{Div}(E) \mid \deg(D) = 0\}$$

Format per tots els divisors de grau 0.

2.1.1 Divisor d'una funció

Definició 2.1.3. *Si E corba llisa sobre K i $f \in \overline{K}(E)^*$ definim el divisor de f com*

$$\operatorname{div}(f) = \sum_{p \in E} \operatorname{ord}_p(f)(p)$$

A més, anomenem principal a tot divisor D tal que $D = \operatorname{div}(f)$ per a alguna $f \in \overline{K}(E)$

Donem ara un exemple del divisor associat a una funció sobre una corba

Exemple 2.1.4. Considerem la corba E definida sobre $\mathbb{F}_3$ d'equació:

$$E : y^2 = x^3 + x + 1$$

i la funció

$$f(x, y) = x + y + 2 \in \overline{\mathbb{F}_3}(E)^*$$

Calculem el divisor de f :

$$\operatorname{Div}(f) = \sum_{p \in E} \operatorname{ord}_p(f)(p)$$

Observem primer que f té zeros als punts $(1, 0), (0, 1)$ de la corba. Podem entendre $f(x, y) = x + y + 2$ com una recta al pla afí i sabem, pel teorema de Bézout (3.2.1) que E i f s'han de tallar en 3 punts comptats amb multiplicitat.

Calculant, f i E tenen multiplicitat d'intersecció 1 a $(1, 0)$ i 2 a $(0, 1)$, per tant,

$$\operatorname{ord}_{(0,1)}(f) = 2, \quad \operatorname{ord}_{(1,0)}(f) = 1.$$

i com no tenim més interseccions, cap altre punt $q \in E$ satisfà $\operatorname{ord}_q(f) > 0$.

Ara com clarament no tenim cap pol a les coordenades afins de E , podem, homogeneitzant i recuperant l'estructura projectiva, observar $\operatorname{ord}_{\mathcal{O}}(f) = -3$. Amb tot:

$$\operatorname{div}(f) = (1, 0) \oplus 2(0, 1) \oplus 3\mathcal{O}$$

Observem també $\deg(\operatorname{div}(f)) = 0$.

Trobem que l'estructura d'un divisor és una suma de punts amb coeficients a $\mathbb{Z}$. Al lector que hagi treballat amb corbes algebraiques, pot recordar-li a l'estructura de grup de les cúbiques, al següent capítol veurem la relació d'aquestes construccions.

Proposició 2.1.5. *Si E una corba suau i $f \in K(E)^*$ aleshores*

$$i) \operatorname{div}(f) \equiv 0 \iff f \in K^*$$

$$ii) \deg(\operatorname{div}(f)) = 0.$$

Demostració. i) Si $\operatorname{div}(f) = 0$ aleshores f no té pols, considerem l'aplicació $f : E \rightarrow \mathbb{P}^1$ definida a (1.2.1), que és morfisme de corbes. Com tot morfisme de corbes és exhaustiu o constant i $f^{-1}(\infty) = \{p \in E \mid f \text{ té un pol a } p\}$.

ii) La demostració d'aquest resultat, si bé és pot donar per altres mitjans, preferirem donar-la arrel d'un resultat posterior, sobre la relació entre morfismes de corbes i divisors.

□

Definició 2.1.6. Definim el grup de Picard $\text{Pic}(E)$ d'una corba E com el quocient del grup de divisors pel subgrup de divisors principals.

Anàlogament i havent vist que tot divisor principal té grau zero definim $\text{Pic}^0(E)$ el quocient del subgrup $\text{Div}^0(E)$ pel subgrup de divisors principals.

Proposició 2.1.7. Existeix una seqüència exacta:

$$1 \longrightarrow \overline{K}^* \longrightarrow \overline{K}(E)^* \longrightarrow \text{Div}^0(E) \longrightarrow \text{Pic}^0(E) \longrightarrow 0 \quad (2.1.1)$$

Demostració. Efectivament, definint les dues primeres aplicacions com la inclusió, de nucli trivial, l'exactitud és clara.

Continuant, si prenem divisors al cos de funcions de E , acabem de demostrar que les funcions constants són les úniques que tenen divisor equivalentment 0 i pertanyen al nucli.

Dins $\text{Div}^0(E)$ al fer el pas al quocient, cauran al nucli tots els divisors principals, és a dir, tots els divisors de la forma $\text{div}(f)$, $f \in \overline{K}(E)$.

Finalment una aplicació de pas al quocient és sempre exhaustiva i la seqüència és efectivament exacta. $\square$

Observació 2.1.8. Sigui K un cos de nombres, aquesta seqüència exacta que acabem de definir és anàloga a:

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^* \longrightarrow I_K \longrightarrow \mathcal{C}\ell_K \longrightarrow 1$$

on $\mathcal{O}_K^\times$ és el grup d'unitats de l'anell d'enters de K , I_K el conjunt d'ideals fraccionaris de K i $\mathcal{C}\ell_K$ el grup de classes. Vegem la semblança d'aquestes seqüències:

Les dues primeres aplicacions són inclusions, com a (2.1.1). Aleshores considerarem de K^* a I_K , l'aplicació que associa cada element $a \in K^*$ a l'ideal principal $(a) \subset I_K$ comunment anomenada *div*. Al nucli de *div* hi seran els elements de K^* que donin lloc a $\mathcal{O}_K$ (neutre per a I_K), és a dir, els elements invertibles de $\mathcal{O}_K$, $\mathcal{O}_K^\times$.

El grup de classes $\mathcal{C}\ell_K$, està definit com I_K/P_K on P_K és el grup d'ideals fraccionaris principals així com $\text{Pic}^0(E)$ és el quocient de $\text{Div}^0(E)$ per divisors principals.

La semblança entre l'estudi de corbes algebraiques i la teoria bàsica de nombres algebraica no es limita només als divisors. El resultat previ (1.2.13) sobre ramificació és clau per a l'estudi de les ramificacions dels ideals primers en cossos de nombres. Aquestes relacions, no només ens serveixen per a poder estudiar propietats compartides o treballar recolzant-nos en altres branques si no que també ens permeten veure que l'estudi de corbes té una important component d'àlgebra més abstracta que pot quedar amagada a primera vista.

Hem definit divisors en una corba, el següent pas natural és definir les aplicacions entre grups de divisors de dues corbes. Ho farem a partir d'una aplicació entre les corbes.

Vam veure que existia una estructura subjacent als cossos de funcions donades dues corbes i un morfisme entre elles, per a divisors tenim:

Definició 2.1.9. Donada $\phi : E_1 \longrightarrow E_2$ una aplicació no constant, definim ϕ^*, ϕ_* induïdes per ϕ :

$$\begin{aligned} \phi^* : \text{Div}(E_2) &\longrightarrow \text{Div}(E_1) & \phi_* : \text{Div}(E_1) &\longrightarrow \text{Div}(E_2) \\ (q) &\longmapsto \sum_{p \in \phi^{-1}(q)} e_\phi(p)(p) & (p) &\longmapsto (\phi(p)) \end{aligned}$$

On les imatges dels punts defineixen les imatges de tot el grup de divisors per ésser generadors.

Vegem com es relacionen amb els conceptes de grau i elements del cos de funcions

Proposició 2.1.10. *Sigui $\phi : E_1 \longrightarrow E_2$ una aplicació suau no constant entre corbes aleshores:*

- i) $\deg(\phi^*(D)) = (\deg(\phi))(\deg(D)) \quad \forall D \in \text{Div}(E_2)$
- ii) $\phi^*(\text{div}(f)) = \text{div}(\phi^*(f)) \quad \forall f \in \overline{K}(E_2)^*$
- iii) $\deg(\phi_*D) = \deg(D) \quad \forall D \in \text{Div}(E_1)$
- iv) $\phi_*(\text{div}(f)) = \text{div}(\phi_*(f)) \quad \forall f \in \overline{K}(E_1)^*$
- v) *L'endomorfisme $\phi_* \circ \phi^*$ actua com multiplicació per $\deg(\phi)$ en $\text{Div}(E_2)$*
- vi) *Sigui ara $\psi : E_2 \longrightarrow E_3$ aplicació suau entre corbes, aleshores*

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \text{ i } (\psi \circ \phi)_* = \psi_* \circ \phi_*$$

Demostració. i) Sigui $D = \sum_{p_i \in E_2} a_i(p_i)$, aleshores

$$\phi^*(D) = \sum_{p_i \in E_2} a_i \sum_{q \in \phi^{-1}(p_i)} e_\phi(q)(q)$$

Ara, prenem graus i, recordant que per a cada $p \in E_2$ la suma dels índexs de ramificació dels $q \in \phi^{-1}(p)$ és el grau de ϕ obtenim:

$$\deg(\phi^*(D)) = \sum_{p_i \in E_2} a_i \sum_{q \in \phi^{-1}(p_i)} e_\phi(q) = \sum_{p_i \in E_2} a_i (\deg(\phi)) = \deg(D) \deg(\phi)$$

- ii) Cal que recordem $\text{ord}_p(\psi^*(f)) = e_\psi(p) \text{ord}_{\psi(p)}(f) \quad \forall f \in \overline{K}(E_2), \forall \psi : E_1 \longrightarrow E_2$. Aleshores, recordant la definició del divisor d'una funció com la suma d'ordres a cada punt:

$$\phi^*(\text{div}(f)) = \phi^* \left(\sum_{p_i \in E_2} \text{ord}_{p_i}(f)(p_i) \right) = \sum_{p_i \in E_2} \text{ord}_{p_i}(f) \left(\sum_{q \in \phi^{-1}(p_i)} e_\phi(q)(q) \right)$$

Ordenant els termes i veient que $\text{ord}_{\phi(q)}(f) = 0$ si $q \notin \phi^{-1}(p_i)$ per a algun i

$$\phi^*(\text{div}(f)) = \sum_{q \in E_1} \text{ord}_{\phi(q)}(f) e_\phi(q)(q) = \sum_{q \in E_1} \text{ord}_q(\phi^*(f))(q) = \text{div}(\phi^*(f))$$

- iii) Només cal observar que el grau d'un divisor depèn únicament dels coeficients, els quals no canvien sota l'acció de ϕ_* .

iv) **Recuperar referències**

v) Sigui $D \in \text{Div}(E_2)$, $D = \sum_p a_p(p)$. Amb el que hem vist:

$$\phi_* \circ \phi^*(D) = \phi_* \left(\sum_{p \in E_2} a_p \sum_{q \in \phi^{-1}(p)} e_\phi(q)(q) \right) = \sum_{p \in E_2} a_p \sum_{q \in \phi^{-1}(p)} e_\phi(q)(p)$$

Si reordenem, trobem que cada p , està multiplicat per l'índex de ramificació de tots els punts a la seva antiimatge. Altre cop, aquesta suma és igual al grau de l'aplicació i s'obté:

$$\phi_* \circ \phi^*(D) = \sum_{p \in E_2} a_p [\deg(\phi)](p) = [\deg(\phi)] \sum_{p \in E_2} a_p(p) = [\deg(\phi)] (D)$$

vi) Per a la primera igualtat només cal recordar que donada una composició de morfismes de corbes no constants, l'índex de ramificació de la composició és la multiplicació d'índexos i el resultat és directe. La segona igualtat és trivial. □

Demostrem un resultat que ens ha quedat pendent:

Demostració de la proposició (2.1.5) ii). Donada $f \in \overline{K}(E)$, recordem el morfisme de corbes induït $f : E \rightarrow \mathbb{P}^1$ (1.2.1), observant que els únics punts amb ordre no nul tenen com a imatge 0 o $\infty \in \mathbb{P}^1$:

$$\deg(\text{div}(f)) = \deg(f^*((0) - (\infty))) = \deg(f) - \deg(f) = 0$$

□

2.1.2 Divisor d'una forma diferencial

El següent pas serà definir el divisor d'una diferencial. Més endavant, quan parlem de l'invariant diferencial veurem com molts resultats es deriven de poder considerar el divisor d'una diferencial i una funció.

Proposició 2.1.11. *Per a tot, tret d'un nombre finit, $p \in E$:*

$$\text{ord}_p(\omega) = 0$$

per a tot $\omega \in \Omega$.

Demostració. Sigui $x \in \overline{K}(E)$ tal que $d(x)$ genera Ω_E . Aleshores $\omega = fd(x)$ per a alguna $f \in \overline{K}(E)$ No ho entenc, preguntar. □

Definició 2.1.12. *Sigui $\omega \in \Omega_E$. Definim el divisor associat a ω com:*

$$\text{div}(\omega) = \sum_{p \in E} \text{ord}_p(\omega)(p) \in \text{Div}(E)$$

La següent definició ens permetrà donar un millor context a les diferencials com a paral·lelisme de les diferencials al càlcul:

Definició 2.1.13. Direm que una diferencial $\omega \in \Omega$ és regular (o bé holomorfa) si

$$\text{ord}_p(\omega) \geq 0 \quad \forall p \in E$$

i que és sense zeros (*non-vanishing*) si

$$\text{ord}_p(\omega) \leq 0 \quad \forall p \in E$$

Observació 2.1.14. Si $\omega_1, \omega_2 \in \Omega_E$ son dues diferencials no nul·les, aleshores, del fet que Ω_E és un $\overline{K}(E)$ -espai vectorial de dimensió 1 sabem que ha d'existir $f \in \overline{K}(E)^*$ tal que $\omega_1 = f\omega_2$ i:

$$\text{div}(\omega_1) = \text{div}(f) + \text{div}(\omega_2)$$

justificant la següent definició

Definició 2.1.15. Definirem la classe de divisors canònics de E com la imatge a $\text{Pic}(E)$ de $\text{div}(\omega)$ per a qualsevol diferencial no nul·la $\omega \in \Omega_E$. Qualsevol divisor en aquesta classe és un divisor canònic.

En aquest treball ens quedarem a les portes de demostrar el teorema de Riemann-Roch, on els (o la classe de) divisors canònics juguen un paper important, donem la definició per tal que s'entengui l'enunciat del teorema de Riemann-Roch.

2.2 Aproximació al teorema de Riemann-Roch

Al llarg d'aquesta secció, K serà un cos algebraicament tancat ja que així es troba definit normalment a la literatura. Quan, més endavant, treballem amb cossos arbitraris només ens caldrà considerar que tots els resultats d'aquesta secció son idèntics per a la clausura algebraica del cos base.

Recuperem el llenguatge de divisors, d'ara en endavant $D = \sum a_p(p)$, $a_p \in \mathbb{Z}$, $p \in E$ serà un divisor a E/K . Donarem un ordre parcial sobre els divisors:

Definició 2.2.1. Direm que un divisor D és positiu (o efectiu), i denotarem $D \geq 0$, si $a_p \geq 0 \quad \forall p \in E$.

Donats dos divisors D_1, D_2 , escriurem $D_1 \geq D_2$ si $D_1 - D_2$ és positiu.

Un raonament comú a la geometria és, arrel d'un conjunt finit de punts, veure quins objectes interactuen amb aquests punts d'una manera específica. Per exemple, a l'estudi de corbes algebraiques és una qüestió interessant definir una corba a partir d'un conjunt de punts i multiplicitats. L'estudi de quantes corbes de cert grau existeixen que passin per uns punts determinats amb certa multiplicitat és tan útil com interessant i dona lloc a veure les corbes des d'un altre punt de vista: Passem de considerar els punts com a un element, o un afegit a una corba definida per un ideal a considerar les corbes definides com els punts que hi pertanyen.

De manera similar, donat un divisor $D = \sum a_p(p)$, voldrem determinar sota quines circumstàncies existeix una funció racional amb pols a p d'ordre no major a a_p .

Definició 2.2.2. Sigui $D = \sum a_p(p)$, definirem $\mathcal{L}(D)$ l'espai de funcions:

$$\mathcal{L}(D) = \{f \in K(E) \mid \text{ord}_p \geq -a_p, \quad \forall p \in E\}$$

Observem que $f \in \mathcal{L}(D) \iff \text{div}(f) + D > 0$ o bé $f = [0]$.
És fàcil veure que per a cada D , $\mathcal{L}(D)$ és un K espai vectorial ja que multiplicar una funció per una constant no canvia els zeros ni l'ordre en cap punt i tenim, per a cada p , donades $f, g \in K(E)^*$

$$\text{ord}_p(af + bg) \geq \min \{ \text{ord}_p(f), \text{ord}_p(g) \}$$

Ens serà interessant la dimensió d'aquest espai vectorial. Serà la mesura de 'quantes' funcions tenen a cada p ordre major a $-a_p$.

Proposició 2.2.3. *Siguin $D_1, D_2 \in \text{Div}(E)$ i sigui $\ell(D) = \dim_K(\mathcal{L}(D))$.*

- i) *Si $D_1 < D_2$, aleshores $\mathcal{L}(D_1) \subset \mathcal{L}(D_2)$ i $\dim_K(\mathcal{L}(D_2)/\mathcal{L}(D_1)) \leq \deg(D_2 - D_1)$.*
- ii) *$\mathcal{L}(0) = K$, A més $\mathcal{L}(D) = 0$ només si $\deg(D) < 0$.*
- iii) *Per a qualsevol $D \in \text{Div}(E)$, $\mathcal{L}(D)$ és un espai vectorial de dimensió finita. De fet, si $\deg(D) \geq 0$, aleshores*

$$\ell(D) = \deg(D) + 1$$

- iv) *Si $D_1 \equiv D_2$, aleshores $\ell(D_1) = \ell(D_2)$.*

Demostració. Mantenint la notació:

- i) Si $D_1 < D_2$, aleshores $D_2 = D_1 + (p_r) + \dots + (p_s)$ (amb p_i no necessàriament diferent de p_j per a $i, j \in \{s, s+1, \dots, r\}$) i clarament

$$\mathcal{L}(D_1) \subset \mathcal{L}(D_1 + (p_r)) \subset \dots \subset \mathcal{L}(D_1 + (p_r) + \dots + (p_s)) = \mathcal{L}(D_2).$$

Aleshores, només ens cal demostrar $\dim_K(\mathcal{L}(D + (p))/\mathcal{L}(D)) \leq 1$.

Sigui $a_p \in \mathbb{Z}$ el coeficient de p en D . Fent servir l'estructura d'espai vectorial, considerem, essent $\tau \in K(E)$ un uniformitzant a p l'aplicació lineal:

$$\varphi : \mathcal{L}(D + (p)) \longrightarrow K$$

$$f \longmapsto (\tau^{a_p+1}(f))(p)$$

Observem que si $f \in \mathcal{L}(D)$, $\text{ord}_p(f) \geq -a_p$ i, per tant $\text{ord}_p(\tau^{a_p+1}f) > 0$. Així $\text{Ker} \varphi = \mathcal{L}(D)$ i pel primer teorema d'isomorfia tenim el resultat.

- ii) $\mathcal{L}(0) = K$ és trivial. Qualsevol funció no constant té algun pol i, per tant, ordre estrictament negatiu en algun punt de la corba.
Ara, suposem $D = D_+ - a_1(p_1) - \dots - a_r(p_r)$ on $a_i \in \mathbb{Z}_{>0}$ i amb D_+ denotem els punts amb coeficients positius de D (la part positiva, si escau). Suposem $\exists f \in \mathcal{L}(D)$. Aleshores $\text{ord}_{p_i}(f) \geq a_i$, com una funció racional té tants zeros com pols tenim que f ha de tenir pols amb multiplicitats sumant $\sum_{i=1, \dots, r} a_i$. En el millor dels cassos, f presenta pols on D un punt amb coeficient positiu. Tenim però que $\deg(D) < 0$ i, per tant, la suma de les multiplicitats dels pols de f serà major a $\deg(D_+)$. Així, existeix algun $p \in E$ tal que $\text{ord}_p(f) < a_p$ si a_p és el coeficient de p a D_+ i hem arribat a una contradicció.

- iii) Si $\deg(D) = n \geq 0$, triem $p \in E$ i definim $D^* = D - (n+1)(p)$. Aleshores $\mathcal{L}(D^*) = 0$ ja que $\deg(D^*) < 0$ i, pel que hem demostrar a i),

$$\dim_K(\mathcal{L}(D)/\mathcal{L}(D^*)) \leq n+1 \xRightarrow[\mathcal{L}(D^*)=0]{} \ell(D) \leq n+1$$

- iv) Siguin D_1, D_2 dos divisors amb la mateixa classe a $\text{Div}^0(E)$. Aleshores $D_1 = D_2 + \text{div}(f)$ per a alguna $f \in K(E)$ i podem definir l'aplicació

$$\varphi : \mathcal{L}(D_1) \longrightarrow \mathcal{L}(D_2)$$

$$g \longmapsto gf$$

Ara φ és un isomorfisme d'espais vectorials i $\ell(D_1) = \ell(D_2)$

□

Podem definir per a cada divisor, el seu grau sobre un subconjunt de E . Aquesta construcció ens serà interessant de cara a demostrar futurs resultats.

Definició 2.2.4. *Sigui $S \subset E$ un subconjunt, i sigui $D = \sum a_p(p)$ a E aleshores definim:*

$$\deg^S(D) = \sum_{p \in S} a_p \quad \text{i} \quad \mathcal{L}^S(D) = \{f \in K(E) \mid \text{ord}_p(f) \geq -a_p \ \forall p \in S\}$$

Lema 2.2.5. *Sigui $D_1 < D_2$, aleshores $\mathcal{L}^S(D_1) \subset \mathcal{L}^S(D_2)$.*

Si S és un conjunt finit, $\dim_K(\mathcal{L}^S(D_2)/\mathcal{L}^S(D_1)) = \deg^S(D_2 - D_1)$

Demostració. La demostració és pràcticament igual que a la donada per la última proposició. □

La següent proposició ens permetrà aproximar-nos al càlcul de dimensions $\ell(D)$ per a un tipus de divisor en particular.

Definició 2.2.6. *Sigui $f \in K(E)$ definim el seu divisor de zeros com:*

$$(f)_0 = \sum_{\text{ord}_p(f) > 0} \text{ord}_p(f)(p).$$

Clarament, $(f)_0$ és un divisor positiu per a cada f , té sentit considerar $\mathcal{L}((f)_0)$.

Proposició 2.2.7. *Sigui $f \in K(E)$ no constant, sigui $(f)_0 = \sum a_p(p)$ el divisor de zeros de f i $n = [K(E) : K(f)]$. Aleshores*

$$i) \deg((f)_0) = n$$

ii) $\forall r \in \mathbb{Z}$ existeix una constant d tal que:

$$\ell(r(f)_0) \geq rn - d$$

Demostració. Sigui $m = \deg((f)_0)$, veurem primer que $m \leq n$, provarem ii) i a partir d'aquest fet trobarem que $m \geq n$ i hauréu demostrat la proposició.

Sigui $S = \{p \in E \mid a_p \geq 0\}$ Escollim $f_1, \dots, f_m \in \mathcal{L}(0)$ tals que les imatges $\overline{f_1}, \dots, \overline{f_m} \in \mathcal{L}^S(0)/\mathcal{L}^S(-(f)_0)$ siguin base (Pel lema anterior la dimensió de l'espai vectorial $\mathcal{L}^S(0)/\mathcal{L}^S(-(f)_0)$ és m). Veurem que $f_1, \dots, f_n$ son $K(f)$ -linealment independents:

Suposem que no, aleshores podem trobar $w_i = b_i + fh_i \in K[f]$ (sempre podem aconseguir

aquesta expressió, desfont denominadors i multiplicant per alguna potència de f) tals que

$$\sum_{i=1}^m w_i f_i = 0$$

Amb no tots els b_i nuls. Tenim però:

$$\sum_{i=1}^m b_i f_i = -f \sum_{i=1}^m h_i g_i$$

Ara, el terme de la dreta de la igualtat és de $\mathcal{L}^S(-(f)_0)$ amb el que $\sum w_i f_i \xrightarrow{\mathcal{L}^S(-(f)_0)} 0$, que és una contradicció.

Per tant, $f_1, \dots, f_m$ son $K(f)$ -linealment independents $\implies m \leq n$.

Vegem ii):

Sigui ara $\{g_1, \dots, g_n\}$ una $K(f)$ -base de $K(E)$. Podem considerar, que cada g_i satisfà una equació

$$g_i^{m_i} + c_{i1}g_i^{m_i-1} + \dots = 0, \quad a_{ij} \in K[1/f]$$

Aleshores per a $p \notin S$ es té $\text{ord}_p(c_{ij}) \geq 0$. Així si $\text{ord}_p(g_i) < 0$ i $p \notin S$

$$\text{ord}_p(g_i^{m_i}) < \text{ord}_p(c_{ij}g_i^{m_i-j})$$

que no pot ser. Per tant $\text{ord}_p(g_i) \geq 0 \quad \forall p \notin S$. És a dir, per a algun t

$$\text{div}(g_i) + t(f)_0 > 0$$

per a tot $i = 1, \dots, n$. Aleshores $g_i f^{-j} \in \mathcal{L}((r+t)(f)_0)$ per a $i = 1, \dots, n, j = 0, 1, \dots, r$.

Ara tenim que cada les g_i son independents sobre $K(f)$ mentre que $x^{-1}, \dots, x^{-r}$ son clarament independents sobre K . Aleshores

$$\{g_i f^{-j} \mid i = 1, \dots, n; j = 0, \dots, r\}$$

son independents sobre K . Així $\ell((r+t)(f)_0) \geq n(r+1)$. Per altra banda però

$$\ell((r+t)(f)_0) = \ell(r(f)_0) + \dim_K(\mathcal{L}((r+t)(f)_0)/\mathcal{L}(r(f)_0)) \leq \ell(r(f)_0) + tm$$

Aleshores,

$$\ell(r(f)_0) \geq n(r+1) - tm = rn - \tau$$

Finalment, tenint en compte que per a un divisor positiu D , $\ell(D) \leq \deg(D) - 1$,

$$rn - \tau \leq \ell(r(f)_0) \leq rm + 1$$

si prenem r tant gran com volguem veiem que $n \leq m$ i hem acabat. $\square$

Arribem al teorema que defineix el gènere d'una corba:

Teorema 2.2.8 (de Riemann). *Existeix una constant $g \in \mathbb{Z}_{\geq 0}$ tal que, per a qualsevol divisor $D \in E$:*

$$\ell(D) \geq \deg(D) + 1 - g$$

El menor dels g per als quals es dona la desigualtat serà el gènere de E .

Demostració. Per a cada D considerem $S(D) = \deg(D) + 1 - \ell(D)$. Veurem que per a qualsevol D , $S(D) \leq g$. Primerament cal que tinguem en compte les següents consideracions:

1. $S(0) = 0$, per tant si g existeix ha de ser major o igual a zero.
2. Si $D \equiv D^*$ aleshores $S(D) = S(D^*)$.
3. Si $D < D^*$, aleshores $S(D) \leq S(D^*)$.

Sigui $f \in K(E)$ no constant i considerem $Z = (f)_0$. Triem τ la menor de les constants tal que $\forall r$, $\ell(rZ) \geq rn - \tau$ si $n = [K(E) : K(f)] = \deg(Z)$. Ara, com per a qualsevol r , $S(rZ) = rn + 1 - \ell(rZ) \leq \tau + 1$ i $rZ < (r+1)Z$, tenim per la consideració (3) que $S(rZ) = \tau + 1$ per a tota $r > 0$.

Sigui $g = \tau + 1$. Aleshores, per (2) i (3) és prou veure que per qualsevol divisor D existeix $D^* \equiv D$ i un enter $r \geq 0$ tal que $D^* < rZ$ per a algun $Z = (f)_0$.

Considerem $Z = \sum a_p(p)$ (tot recordant $a_p = \text{ord}_p(f) > 0$) i suposem $D = \sum \alpha_p(p)$. Voldrem $D^* = D - \text{div}(F)$ pel que necessitem $a_p - \text{ord}_p(F) \leq r\alpha_p$ per a tot p .

Sigui $T = \{p \in E \mid a_p > 0, \text{ord}_p(1/f) \geq 0\}$ definim

$$F = \prod_{p \in T} (1/f - 1/f(p))$$

Aleshores $a_p - \text{ord}_p(F) \leq 0$ on $\text{ord}_p(1/f) \geq 0$ i, si $\text{ord}_p(1/f) < 0$, $\alpha_p > 0$ i per a r prou gran $D^* < rZ$.

Ambo tot, hem trobat que per a qualsevol divisor D , existeix un divisor $D^* \equiv D$ tal que $S(D) = S(D^*) \leq S(rZ) = g$ i

$$\ell(D) \geq \deg(D) + 1 - g$$

□

Veiem algunes implicacions del teorema de Riemann.

Exemple 2.2.9. Sigui E una corba.

1. $g = 0 \iff E \cong \mathbb{P}^1$.
2. $g = 1 \iff E$ és biracionalment equivalent (els respectius cossos de funcions són isomorfs) a una cúbica no singular.
3. $g = 2 \implies E$ és una corba hiperel·líptica i existeix una aplicació de grau 2 de $E \longrightarrow \mathbb{P}^1$

La formulació de Riemann ens és prou per a definir el gènere i entendre les implicacions, tot i així, a l'hora de fer càlculs, o de trobar resultats més precisos ens serà útil la 'compleció' del teorema, donada per Roch, estudiant de Riemann, que no podrem demostrar però sí entendre el resultat.

Teorema 2.2.10 (de Riemann-Roch). *Sigui W un divisor canònic en E , aleshores per a qualsevol divisor D ,*

$$\ell(D) = \deg(D) + 1 - g + \ell(W - D) \quad (2.2.1)$$

El següent corol·lari serà important:

Corol·lari 2.2.11. *Sigui W un divisor canònic:*

i) $\ell(W) = g$

ii) $\deg(W) = 2g - 2$

iii) *Si, per a un divisor D , $\deg(D) > 2g - 2$, aleshores*

$$\ell(D) = \deg(D) - g + 1$$

Demostració. i) Només cal prendre $D = 0$ a (2.2.1) i, recordant que $\ell(0) = 1$ tenim
 $1 = 0 + 1 - g + \ell(W - 0) \implies \ell(W) = g$.

ii) Prenem ara $D = W$ i de (2.2.1) tenim

$$\ell(W) = \deg(W) + 1 - g + \ell(W - W)$$

$$\deg(W) = \ell(W) + g - 2$$

i, aplicant *i)* obtenim el resultat.

iii) Directament de (2.2.1)

$$\ell(D) = \deg(D) + 1 - g + \ell(W - D)$$

on si $\deg(D) > 2g - 2$, $W - D < 0$ i $\ell(W - D) = 0$.

□

Observació 2.2.12. Per a una corba de gènere $g = 1$ l'apartat *iii)* aplica per a qualsevol divisor positiu.

Capítol 3

Corbes el·líptiques i isogènies

Arribem a l'objecte d'estudi central d'aquest treball. En aquest capítol definirem corba el·líptica, veurem perquè representen un tipus de corba interessant i treballarem tant amb la seva estructura de grup com amb les isogènies, que seran els morfismes de corbes el·líptiques. Una particularitat de les corbes el·líptiques és l'isomorfisme entre l'estructura de grup de la corba i el subgrup de classes de divisors amb grau 0, $\text{Pic}^0(E)$.

3.1 Definició de corba el·líptica

Havent donat la definició de gènere d'una corba podem finalment, definir corba el·líptica.

Definició 3.1.1. *Una corba el·líptica és un parell $(E, \mathcal{O})$ on E és una corba de gènere 1 i $\mathcal{O} \in E$ un punt fixat que serà anomenat el punt de l'infinit.*

Aquesta definició purament abstracta no sembla massa il·luminadora a l'hora de caracteritzar les corbes el·líptiques. La següent proposició ens mostrarà com tota corba el·líptica es pot identificar amb una cúbica plana d'equació particular.

Proposició 3.1.2. *Si E és una corba el·líptica definida sobre K aleshores existeixen funcions $x, y \in K(E)$ tals que l'aplicació*

$$\phi : E \longrightarrow \mathbb{P}^2$$

$$\phi = [x : y : 1]$$

és un isomorfisme entre E i una corba d'equació:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad (3.1.1)$$

amb coeficients a K i tal que $\phi(\mathcal{O}) = [0 : 1 : 0]$

Demostració. Considerem $\mathcal{L}(\mathcal{O})$ l'espai vectorial definit a partir del divisor en E : $(\mathcal{O})$. Tenim que, per a cada $n \in \mathbb{Z}_{>0}$, $\deg(n(\mathcal{O})) = n > 0$. Així, per últim corol·lari del capítol anterior, tenim que $\ell(n(\mathcal{O})) = n$. Aleshores, tenim $\ell(2(\mathcal{O})) = 2$ i per tant, $\dim_K(\mathcal{L}(2(\mathcal{O}))) = 2$ per tant, existeix una funció $x \in K(E)$ tal que

$$\mathcal{L}(2(\mathcal{O})) = \langle 1, x \rangle$$

on x ha de tenir un pol d'ordre exactament 2 en $\mathcal{O}$. Repetim l'argument i triem $y \in K(E)$ amb un pol d'ordre exactament 3 en $\mathcal{O}$. Aleshores tenim:

$$\begin{aligned}\ell((\mathcal{O})) &= 1 \implies \mathcal{L}((\mathcal{O})) = \langle 1 \rangle_K \\ \ell(2(\mathcal{O})) &= 2 \implies \mathcal{L}(2(\mathcal{O})) = \langle 1, x \rangle \\ \ell(3(\mathcal{O})) &= 3 \implies \mathcal{L}(3(\mathcal{O})) = \langle 1, x, y \rangle \\ \ell(4(\mathcal{O})) &= 4 \implies \mathcal{L}(4(\mathcal{O})) = \langle 1, x, y, x^2 \rangle \\ \ell(5(\mathcal{O})) &= 4 \implies \mathcal{L}(5(\mathcal{O})) = \langle 1, x, y, x^2, xy \rangle \\ \ell(6(\mathcal{O})) &= 6 \implies \mathcal{L}(6(\mathcal{O})) = \langle 1, x, y, x^2, xy, x^3 \rangle\end{aligned}$$

On observem però que $y^2 \in \mathcal{L}(6(\mathcal{O}))$ aleshores y^2 és combinació K -lineal dels generadors de $\mathcal{L}(6(\mathcal{O}))$ i, ajustant termes i renombrent x, y per múltiples podem escriure la relació:

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

i obtenim (3.1.1). Tenim aleshores que

$$\phi : E \longrightarrow \mathbb{P}^2 \text{ on } \phi = [x : y : 1]$$

envia E als punts d'una corba C amb equació (3.1.1) on, clarament $\phi(\mathcal{O}) = [0 : 1 : 0]$. Ara, per la primera proposició del treball, ϕ és un morfisme de corbes i, per tant, exhaustiu (ja que no és constant). Així per veure que ϕ dona lloc a un isomorfisme, només ens cal veure que $\deg(\phi) = 1$. Si considerem l'aplicació $[x, 1] : E \longrightarrow \mathbb{P}^1$, com x té un pol d'ordre 2 a $\mathcal{O}$ i cap altre pol per (1.2.12), $\deg([x, 1]) = 2$, repetint el procés per a y tenim

$$[K(E) : K(x)] = 2, [K(E) : K(y)] = 3 \implies [K(E) : K(x, y)] \text{ divideix } 2 \text{ i } 3$$

aleshores, $[K(E) : K(x, y)] = 1$ i $\deg(\phi) = 1$ amb el que ϕ és un isomorfisme de corbes. $\square$

Una equació de amb la forma descrita s'anomena de Weierstrass. D'ara en endavant acostumarem a considerar sempre per a una corba el·líptica la seva equació de Weierstrass. Si bé una corba el·líptica no té associada una única equació de Weierstrass, dues equacions per a la mateixa corba es poden relacionar mitjançant un canvi de variables lineal, així la informació que podem extreure serà sempre la mateixa. Anomenarem a les funcions x, y funcions coordenades de E .

Observem la importància del teorema de Riemann-Roch. A partir únicament del fet que E fos de gènere 1 hem pogut veure que E es pot encabir en un pla projectiu definint una cúbica plana que podem caracteritzar a partir d'una equació amb una forma determinada. Així, hem pogut associar un objecte geomètrico-algebraic abstracte a una (classe d') equació en $\mathbb{P}^2$, molt més fàcilment estudiable.

3.2 Estructura de grup

El lector que hagi treballat amb corbes algebraiques estarà familiaritzat amb l'estructura de grup que presenten les cúbiques, corbes algebraiques definides a partir d'un polinomi (homogeni, si escau) de grau 3.

En aquest treball ens basarem en la definició que es dona a

The arithmetic of elliptic curves de Joseph H. Silverman on es treballa amb E una corba

amb equació de Weierstrass que ens permetrà facilitar alguns càlculs i no sortir del context de corbes el·líptiques.

En trobem la justificació arrel del teorema de Bezout:

Teorema 3.2.1. *Siguin M, N dues varietats algebraiques definides per polinomis $F, G \in \overline{K}[X, Y, Z]$ de graus n, m respectivament. Aleshores M, N es tallen en nm punts comptats amb multiplicitat.*

Corol·lari 3.2.2. *Una cúbica i una recta (en un mateix pla) es tallen en 3 punts (comptats amb multiplicitat).*

Ara, donats dos punts p, q diferents en un espai de dimensió arbitrària, existeix una única recta r (o bé, varietat algebraica definida per un polinomi de grau 1) tal que $p, q \in r$. Si aquests dos punts es troben sobre C una cúbica, aleshores pel resultat que acabem de veure, existeix un únic punt o tal que $o, p, q \in C \cap r$.

Aquesta propietat (que com veurem, no és tan simple ni es compleix per a tots els punts) serà la inspiració per a definir una estructura de grup sobre una cúbica.

A partir d'ara treballarem amb E donada per una equació de Weierstrass (3.1.1):

Podem entendre $E \subset \mathbb{P}^2$ conformada pels punts $p = (x, y)$ satisfent l'equació i el punt de l'infinit $\mathcal{O} = [0 : 1 : 0]$. Sigui ara $V \subset \mathbb{P}^2$ una recta, pel que acabem de veure V interseca E en exactament tres punts o, p, q que poden no ser tots tres diferents.

Definim aleshores el grup format per $p : p \in E$ amb suma $+$ definida:

Definició 3.2.3. *Siguin $p, q \in E$, V la recta connectant p i q (tangent a p si $p = q$) i r el tercer punt d'intersecció entre V i E . Sigui W la recta connectant r i $\mathcal{O}$. Aleshores definim $p + q$ com el punt tal que $W \cap E = \{r, \mathcal{O}, p + q\}$*

Veiem que efectivament, aquesta definició de suma de punts compleix les propietats necessàries per a definir l'aplicació d'un grup (abelià).

Proposició 3.2.4. *La suma que hem definit compleix les següents propietats:*

i) *Siguin $p, q, r \in E$ (no necessàriament diferents) sobre una recta, aleshores:*

$$(p + q) + r = \mathcal{O}$$

ii) $p + \mathcal{O} = p \quad \forall p \in E$.

iii) $p + q = q + p \quad \forall p, q \in E$.

iv) *Sigui $p \in E$. Aleshores existeix un altre punt en E (que denotarem com $-p$) tal que:*

$$p + (-p) = \mathcal{O}$$

v) *Siguin $p, q, r \in E$, aleshores:*

$$(p + q) + r = p + (q + r).$$

Demostració. Al llarg de la demostració, en moments determinats pot donar-se que trac-tem un mateix punt amb dos 'noms' diferents. Entendrem que si $p = q$, la recta $p \vee q$ és la recta tangent a E en p . De igual manera, si la recta $p \vee \mathcal{O}$ és tangent en p , i hem dit que r era el tercer punt d'intersecció amb la recta, haurem d'entendre que $r = p$.

- i) Directe de la definició, el punt $p + q$ és aquell tal que la recta $(p + q) \vee \mathcal{O}$ interseca E en $p + q, \mathcal{O}, r$ on r és el tercer punt d'intersecció de la recta $p \vee q$.
- ii) Considerem $p + \mathcal{O}$. Aleshores les rectes L_1 : recta que passa per $p, \mathcal{O}$ i talla E en algun punt r , i L_2 : recta que passa per r i $\mathcal{O}$, son les mateixes. Així, el tercer punt d'intersecció de $r \vee \mathcal{O}$ amb E és clarament p .
- iii) Clarament, les $p \vee q$ i $q \vee p$ defineixen la mateixa recta i, per tant, el tercer punt d'intersecció r és el mateix considerem $p + q$ o $q + p$. Així, si ambdues expressions defineixen un mateix r i $\mathcal{O}$ és sempre el mateix punt, $p + q = q + p$.
- iv) Sigui q tal que $p \vee \mathcal{O} \cap E = \{p, \mathcal{O}, q\}$, aleshores $p + q = (p + \mathcal{O}) + q = \mathcal{O}$, on fem servir els resultats previs.
- v) Es pot demostrar a partir de les fórmules per a la suma (3.2.6) que donarem més endavant (poc interessant) o, a partir de l'isomorfisme $\sigma : \text{Pic}^0 \longrightarrow E$.

□

Proposició 3.2.5. *Suposem que E està definida sobre K , aleshores*

$$E(K) := \{p = (x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

és un subgrup de E .

Demostració. Si p, q tenen coordenades a K , aleshores l'equació de $p \vee q$ té coeficients a K , si, adicionalment, E està definida sobre K , el tercer punt de la intersecció entre $p \vee q$ i E vindrà donat per la solució d'una equació formada per combinacions de coeficients de E i $p \vee q$ i, per tant, la solució d l'equació, per a cada coordenada es trobarà a K . Podrem veure aquest raonament de manera més clara a partir del pròxim lema. Essencialment, combinant punts amb coordenades a $K \times K$ no sortim de $K \times K$. □

El punts $p \in E(K)$ s'anomenen punts racionals. La fita de Hasse, objectiu final d'aquest treball busca aproximar la quantitat de punts en $E(K)$ és a dir $\#E(K)$ per a K un cos finit.

A continuació donarem un resultat per al càlcul de les coordenades de $p + q$, donades les de p, q i l'equació de Weierstrass de la corba.

Per motius d'espai i de interès teòric no donarem la demostració, el lector interessat trobarà que no hi ha cap complexitat en desenvolupar aquestes formules. Tot i així, l'existència d'aquestes ens serà molt útil per a certs arguments que farem servir més endavant i per a poder donatreballar amb els exemples. La construcció d'aquestes formes es pot trobar al Silverman, d'on extraurem:

Lema 3.2.6. *Sigui E una corba elíptica donada per una equació de Weierstrass :*

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

i) *Sigui $p_0 = (x_0, y_0) \in E$. Aleshores $(-p_0) = (x_0, -y_0 - a_1x_0 - a_3)$.*

D'ara en endavant siguin $p_1, p_2, p_3 \in E$ amb $p_i = (x_i, y_i)$ tals que $p_1 + p_2 = p_3$.

ii) *Si $x_1 = x_2$ i $y_1 + y_2 + a_1x_2 + a_3 = 0$, aleshores $p_1 + p_2 = \mathcal{O}$.*

Definim dues quantitats ζ, ξ tals que $y = \zeta x + \xi$ és equació de la recta $p_1 \vee p_2$ o, en cas que $p_1 = p_2$, la recta tangent a E en p_1

(a) Si $x_1 \neq x_2$

$$\zeta = \frac{y_2 - y_1}{x_2 - x_1}, \quad \xi = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

(b) Si $x_1 = x_2$

$$\zeta = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \xi = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

iii) $p_3 = p_1 + p_2$ ve donat per:

$$x_3 = \zeta^2 + a_1\zeta - a_2 - x_1 - x_2, \quad y_3 = -(\zeta + a_1)x_3 - \xi + a_3.$$

Un exemple de l'ús d'aquestes formes és el corol·lari:

Corol·lari 3.2.7. *Diem que una funció $f \in \overline{K}(E) = \overline{K}(x, y)$ és parella si $f(p) = f(-p) \quad \forall p \in E$. Aleshores f és parella $\iff f \in \overline{K}(x)$*

Un resultat important que ens portarà a poder definir la isogènia dual al capítol 4 és la relació entre l'estructura de grup d'una corba el·líptica i el seu grup de divisors, veurem en aquesta secció la importància del teorema de Riemann-Roch.

Lema 3.2.8. *Segui E una corba el·líptica i $p, q \in E$ aleshores*

$$(p) \sim (q) \iff p = q$$

Demostració. Suposem $(p) \sim (q)$, aleshores existeix $f \in K(E)$ tal que

$$\text{div}(f) = (p) - (q)$$

Aleshores $f \in \mathcal{L}((q))$ amb $\ell((q)) = 1$ i com $\overline{K} \subset \mathcal{L}((q))$, $\ell((q)) = 1 \implies \overline{K} = \mathcal{L}((q)) \implies f \in \overline{K} \implies p = q$ $\square$

Donem ara una successió de resultats que ens portaran a veure l'isomorfisme que busquem.

Proposició 3.2.9. *Segui $(E, \mathcal{O})$ corba el·líptica, aleshores per a cada divisor $D \in \text{Div}^0(E)$ existeix un únic punt $p \in E$ tal que*

$$D \sim (p) - (\mathcal{O})$$

Demostració. Com E és corba de gènere 1, tenim, per Riemann-Roch $\ell(D + \mathcal{O}) = 1$, ja que $\deg(D) = 0$. Sigui $f \in \mathcal{L}(D + (\mathcal{O}))$, aleshores $\text{div}(f) \geq -D - \mathcal{O}$ i, com $\deg(\text{div}(f)) = 0$

$$\text{div}(f) = -D - (\mathcal{O}) + (p)$$

per a algun $p \in E$ i, aleshores $D \sim (p) - (\mathcal{O})$. Ara suposem q amb la mateixa propietat, aleshores $(p) \sim D - (\mathcal{O}) \sim (q)$ i pel lema anterior $p = q$. $\square$

Proposició 3.2.10. *L'aplicació*

$$\sigma : \text{Div}^0(E) \longrightarrow E$$

donada per l'associació de la proposició anterior és una aplicació exhaustiva i l'aplicació que indueix sobre Pic^0

$$\sigma : \text{Pic}^0(E) \longrightarrow E$$

és una bijecció

Demostració. Per a cada p considerem el divisor $D = (p) - (\mathcal{O})$, clarament $\sigma(D) = p$ i σ és exhaustiva.

Considerem ara $D_1, D_2 \in \text{Div}^0(E)$ amb $p_i = \sigma(D_i)$. Aleshores

$$D_1 - D_2 \sim (p_1) - (\mathcal{O}) - ((p_2) - (\mathcal{O})) = (p_1) - (p_2)$$

Clarament $p_1 = p_2 \implies D_1 \sim D_2$ i $D_1 \sim D_2 \implies (p_1) \sim (p_2) \implies p_1 = p_2$.
Recapitulant, hem vist

$$\sigma(D_1) = \sigma(D_2) \iff D_1 \sim D_2$$

i, per tant l'aplicació σ definida sobre el grup de classes Pic^0 és injectiva. $\square$

Proposició 3.2.11. *L'aplicació*

$$\sigma : \text{Pic}^0(E) \longrightarrow E$$

és un isomorfisme de grups d'invers

$$\kappa : E \longrightarrow \text{Pic}^0(E)$$

$$p \longrightarrow \overline{(p) - (\mathcal{O})}$$

Demostració. És clar que κ és invers de σ , per a cada $p, \kappa(p)$ és un divisor a la classe de $(p) - (\mathcal{O})$, per tant $\sigma(\kappa(p)) = p$. Ara per a cada classe de divisors $\overline{D} \in \text{Pic}^0(E)$, $\sigma(\overline{D})$ és un punt tal que $(p) - (\mathcal{O}) \in \overline{D}$ i $\kappa(\sigma(\overline{D})) = \overline{D}$.

Així, si veiem que κ és morfisme de grups obtindrem el resultat.

Clarament $\kappa(\mathcal{O}) = 0_{\text{Pic}^0(E)}$. Cal veure $\forall p, q \in E$

$$\kappa(p + q) = \kappa(p) + \kappa(q)$$

Considerarem $f/Z, g/Z \in \overline{K}(E)$ tals que $f(X, Y, Z)$ defineix a $\mathbb{P}^2$ la recta que passa per p, q i un tercer punt que anomenem r i $g(X, Y, Z)$ defineix la recta que passa per r i $\mathcal{O}$ (i $(p + q)$). Ara, recordant que $Z = 0$ interseca E en $\mathcal{O}$ amb multiplicitat 3, podem calcular els divisors de f/Z i g/Z com a (2.1.4)

$$\text{div}(f/Z) = (p) + (q) + (r) - 3(\mathcal{O})$$

$$\text{div}(g/Z) = (r) + (p + q) - 2(\mathcal{O})$$

Aleshores

$$0 \sim \text{div}(g/f) = (p + q) - (p) - (q) + (\mathcal{O})$$

Aplicant κ tenim:

$$\kappa(p + q) - (\kappa(p) + \kappa(q)) = 0$$

$\square$

Tenim aleshores un isomorfisme entre el grup de classes de divisors de grau 0 i el grup definit sobre els punts de la corba. Aquesta relació serà clau per a poder definir la isogènia dual més endavant.

Observació 3.2.12. Per a qualsevol corba el·líptica E , tenim la seqüència exacta, herència de (2.1.1):

$$1 \longrightarrow \overline{K}^* \longrightarrow \overline{K}(E)^* \longrightarrow \text{Div}^0(E) \xrightarrow{\sigma} E \longrightarrow 0$$

3.3 Isogènies

Les isogènies seran les aplicacions entre corbes el·líptiques que tractarem al treball i l'estudi de les seves propietats ens portaran a poder extreure resultats d'una corba el·líptica arrel del comportament de les isogènies que es poden definir sobre aquesta.

Definició 3.3.1. *Siguin E_1 i E_2 dues corbes el·líptiques una isogènia de E_1 a E_2 és una aplicació*

$$\phi : E_1 \longrightarrow E_2$$

tal que $\phi(\mathcal{O}) = \mathcal{O}$, els punts de l'infinit de E_1, E_2 respectivament.

Observem que l'aplicació $\phi(p) = \mathcal{O} \quad \forall p \in E_1$ és una isogènia.

Proposició 3.3.2. *Sigui $\phi : E_1 \longrightarrow E_2$ una isogènia. Aleshores $\phi(E_1) = \mathcal{O}$ o bé $\phi(E_1) = E_2$*

Demostració. Les isogènies son morfismes de corbes. Un morfisme de corbes és exhaustiu o constant. Per a qualsevol $\phi : E_1 \longrightarrow E_2$, $\mathcal{O} \in \phi(E_1)$. □

Així, per a cada isogènia no constant (no zero) ϕ , l'aplicació

$$\phi^* : K(E_2) \longrightarrow K(E_1)$$

$$\phi^*(f) = f \circ \phi$$

és un morfisme de cossos, ja que al ésser ϕ exhaustiva, donades $f, g \in K(E_2)$, $\phi^*(f) = \phi^*(g) \implies f(q) = g(q) \quad \forall q \in \phi(E_1) = E_2$ i, per tant $f = g$.

De igual manera que per a aplicacions racionals enter corbes definirem els graus separable i inseparable $\deg_s(\phi), \deg_i(\phi)$ respectivament com els graus separable i inseparable de l'extensió $K(E_1)/\phi^*K(E_2)$ així com les condicions de separabilitat de ϕ seran les de $K(E_1)/\phi^*K(E_2)$ com a extensió de cossos.

Direm que $\deg([0]) = 0$.

Definició 3.3.3. *Considerem ara*

$$\text{Hom}(E_1, E_2) = \{ \phi : E_1 \longrightarrow E_2 \text{ tal que } \phi \text{ és isogènia} \}$$

i observem que podem definir una suma a $\text{Hom}(E_1, E_2)$:

Donades $\phi, \psi \in \text{Hom}(E_1, E_2)$, $(\phi + \psi)(p) = \phi(p) + \psi(p)$ i obtenim una isogènia $((\phi + \psi)(\mathcal{O}_{E_1}) = \phi(\mathcal{O}_{E_1}) + \psi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2} + \mathcal{O}_{E_2} = \mathcal{O}_{E_2})$

Observació 3.3.4. Trobem que podem definir per a cada $\phi \in \text{Hom}(E_1, E_2)$ una isogènia $-\phi$ tal que $-(\phi(p)) = -\phi(p) \quad \forall p \in E_1$ i $\text{Hom}(E_1, E_2)$ és un grup amb la suma que hem vist abans.

Un pas natural serà definir $\text{End}(E)$ format per isogènies $\phi : E \longrightarrow E$. Amb la mateixa suma que acabem de definir i la composició (clarament la composició de dues isogènies de E en E és una isogènia de E en E) $\text{End}(E)$ és un anell. L'anell d'endomorfismes (que no arribarem a estudiar en profunditat) és un invariant clau de E amb destacada importància quan E/K amb K un cos finit.

Exemple 3.3.5. Podem definir per a cada $m \in \mathbb{Z}$ la isogènia multiplicació per m

$$[m] : E \longrightarrow E$$

$$[m](p) = p + p + \dots + p \quad m$$

on si $m < 0$ prendrem $[m](p) = [-m](-p)$, és a dir, $(-p) + (-p) + \dots + (-p)$, $-m$ vegades.

Si $m = 0$, $[0](p) = \mathcal{O} \quad \forall p \in E$.

És clar veure que multiplicació per m és una isogènia:

$$\forall m \in \mathbb{Z}, \quad [m](\mathcal{O}) = \mathcal{O} + \dots + \mathcal{O} = \mathcal{O}$$

Serà un resultat interessant veure que $[m]$ és una isogènia no constant per a qualsevol corba E

Per tal de veure el comportament de $[m]$ observarem com actua sobre una corba E :

Sigui $E/\mathbb{F}_3$ la corba d'equació: $y^2 = x^3 + x + 1$ i considerarem la isogènia $[2] : E \longrightarrow E$

A (referenciem Silverman) trobem equacions per a poder expressar la suma de dos punts com una funció sobre les coordenades dels punts. Fent servir aquestes equacions i observant que $[2](p) = p + p$;

$$[2] : E \longrightarrow E$$

$$(x_0, y_0) \longmapsto \left(\left(\frac{2x_0 + 1}{2y_0} \right)^2 - 2x_0, -\frac{2x_0 - 1}{2y_0} \left(\left(\frac{2x_0 + 1}{2y_0} \right)^2 - 2x_0 \right) + \frac{x_0^3 - x_0 - 2}{2y_0} \right)$$

Calculant,

$$[2](x_0, y_0) = \left(\frac{x_0^2 + x_0 + 1}{y_0^2} - 2x_0, \frac{x_0^3 + x_0^2 + x_0 + 1}{2y_0} - \frac{2x_0^3 + 1}{y_0^3} \right)$$

Observem que els y_0 dividint a l'equació no representen un problema ja que donat $p = (x_0, y_0)$, $-p = (x_0, -y_0)$ així si $y_0 = 0$, $p = -p$ i p és un punt de 2-torsió, $[2](p) = \mathcal{O}$.

Proposició 3.3.6. Sigui E/K una corba el·líptica i sigui $m \in \mathbb{Z}_{\neq 0}$. Aleshores $[m]$ és una aplicació no constant.

Demostració. Es pot veure a partir de (3.2.6). □

Aquest resultat, que sembla útil únicament per a les isogènies d'aquest tipus, ens permet definir millor l'estructura del grup d'homomorfismes entre dues corbes el·líptiques i l'anell d'endomorfismes:

Proposició 3.3.7. *i) Siguin E_1, E_2 corbes el·líptiques. Aleshores el grup $\text{Hom}(E_1, E_2)$ és un $\mathbb{Z}$ -mòdul lliure de torsió, o bé, un grup abelià.*

ii) Sigui E una corba el·líptica, $\text{End}(E)$ és un anell (amb la suma i la composició) de característica zero. A més, és domini d'integritat

Demostració. i) Suposem $\phi \in \text{Hom}(E_1, E_2)$ i $m \in \mathbb{Z}$ tal que

$$[m] \circ \phi = [0]$$

Aleshores, si considerem els graus $\deg([m])\deg(\phi) = 0$. Per tant, o bé $m = 0$ o $\phi = [0]$ ja que si $m \neq 0$, $[m]$ és no constant.

ii) Acabem de provar que $\text{End}(E)$ té característica 0. Només cal aplicar l'apartat anterior al cas $E_1 = E_2$

Ara, la composició de dues isogènies és una isogènia de grau la multiplicació de graus. Així, donades $\phi, \psi \in \text{End}(E)$ tals que $\phi \circ \psi = [0]$, $\deg(\phi)\deg(\psi) = \deg(\phi \circ \psi) = 0$.

Per tant, o bé $\deg(\phi) = 0 \implies \phi = [0]$ o bé $\deg(\psi) = 0 \implies \psi = [0]$ i $\text{End}(E)$ és un domini d'integritat. □

Un exemple interessant d'una aplicació entre corbes el·líptiques és la translació per q .

Exemple 3.3.8. Sigui E/K una corba el·líptica i $q \in E$. Definim l'aplicació translació per q :

$$\begin{aligned}\tau_q : E &\longrightarrow E \\ p &\longmapsto p + q\end{aligned}$$

Observem que τ_q és un isomorfisme d'invers τ_{-q} però no és isogènia tret de $q = \mathcal{O}$.

Ara la translació per q per molt que no sigui una isogènia ens permetrà construir una isogènia a partir de qualsevol aplicació i arribar al següent resultat:

Proposició 3.3.9. *Qualsevol aplicació entre corbes el·líptiques és pot descomposar en una isogènia i una translació.*

Demostració. Sigui $F : E_1 \longrightarrow E_2$ observem que

$$\phi = \tau_{-F(\mathcal{O})} \circ F$$

és una isogènia, ja que $\phi(\mathcal{O}_{E_1}) = F(\mathcal{O}_{E_1}) + (-F(\mathcal{O}_{E_1})) = \mathcal{O}_{E_2}$.

Així, tot recordant que $\tau_q \circ \tau_{-q} = \text{Id}$, obtenim, per a F aplicació entre corbes el·líptiques qualsevol:

$$F = \tau_{F(\mathcal{O}_{E_1})} \circ \phi$$

□

Exemple 3.3.10. El morfisme de Frobenius,

$$\phi_q : E \longrightarrow E^{(q)}$$

és una isogenia si E és una corba e-líptica.

Hem definit una isogènia com una aplicació entre corbes el·líptiques que envia el punt de l'infinit de la corba de sortida al punt de l'infinit de la corba d'arribada. Així, una isogènia compleix la primera característica per a ser un morfisme de grups. Observarem que, efectivament, les isogènies son morfismes de grups:

Teorema 3.3.11. *Si $\phi : E_1 \longrightarrow E_2$ una isogènia. Aleshores:*

$$\phi(p + q) = \phi(p) + \phi(q) \quad \forall p, q \in E_1$$

Demostració. Si ϕ és constant, $\phi(p) = \mathcal{O} \quad \forall p \in E_1$ i el resultat és cert.

En cas contrari, ϕ és un morfisme finit i induïx un morfisme de grups (*pushforward*):

$$\phi_* : \text{Pic}^0(E_1) \longrightarrow \text{Pic}^0(E_2)$$

Recordem que està definit prenent classes sobre $\phi_* : \text{Div}(E_1) \longrightarrow \text{Div}(E_2)$ on per a un divisor qualsevol $D = \sum a_i(p_i)$, $\phi^*(D) = \sum a_i(\phi(p_i))$.

Tenint en compte els isomorfismes

$$\kappa_i : E_i \longrightarrow \text{Pic}^0(E_i)$$

$$p \longmapsto \text{classe de } (p) - (\mathcal{O})$$

obtindrem el resultat del següent lema:

Lema 3.3.12. *Si $\phi : E_1 \longrightarrow E_2$ una isogènia ($\neq [0]$), aleshores el següent diagrama commuta:*

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

Demostració. Si $p \in E_1$. $\kappa_1(p) = \overline{(p) - (O_{E_1})}$. Ara aplicant el *pushforward* :

$$\phi_*(\kappa_1(p)) = \overline{(\phi(p)) - (\phi(O_{E_1}))} = \overline{(\phi(p)) - (O_{E_2})}$$

Per altra banda, és fàcil veure

$$\kappa_2(\phi(p)) = \overline{(\phi(p)) - (O_{E_2})}$$

per a qualsevol $p \in E_1$. □

Ara, observem que tant κ_1 com κ_2 son isomorfismes i ϕ_* és morfisme de grups amb el que ϕ ha de ser també morfisme de grups. Per contrarrecíproc:

Suposem que ϕ no és morfisme de grups. Aleshores existeix un parell $p, q \in E_1$ tal que $\phi(p + q) \neq \phi(p) + \phi(q)$

Considerem $\kappa_2(\phi(p+q))$. Com κ_2 és un isomorfisme (o, en particular, una aplicació injectiva)

$$\phi(p+q) \neq \phi(p) + \phi(q) \implies \kappa_2(\phi(p+q)) \neq \kappa_2(\phi(p) + \phi(q))$$

Per altra banda, com el diagrama anterior commuta i tenint en compte que κ_i i ϕ_* son morfismes de grups:

$$\kappa_2(\phi(p+q)) = \phi_*(\kappa_1(p+q)) = \phi_*(\kappa_1(p)) + \phi_*(\kappa_1(q)) = \phi_*(\kappa_2(p)) + \phi_*(\kappa_2(q)) = \kappa_2(\phi(p) + \phi(q))$$

i hem arribat a una contradicció: Si el diagrama commuta, ϕ ha de ser morfisme de grups. $\square$

Corol·lari 3.3.13. *Si $\phi : E_1 \longrightarrow E_2$ una isogènia no constant. Aleshores*

$$\ker(\phi) = \phi^{-1}(O)$$

és un subgrup finit d'ordre com a molt $\deg(\phi)$.

Demostració. Per a una aplicació entre corbes no constant,

$$\sum_{p \in \phi^{-1}(O)} e_\phi(p) = \deg(\phi)$$

i per definició $e_\phi(p) \geq 1, \forall p \in E_1$. Recordant que el nucli d'un morfisme de grups és un subgrup obtenim el resultat. $\square$

Teorema 3.3.14. *Si $\phi : E_1 \longrightarrow E_2$ una isogènia no constant.*

i) *Per a tot $q \in E_2$*

$$\#\phi^{-1}(q) = \deg_s(\phi)$$

ii) *Per a tot $p \in E_1$*

$$e_\phi(p) = \deg_i(\phi)$$

Demostració. i) Sabem, per (1.2.12) que $\#\phi^{-1}(q) = \deg_s(\phi)$ per a quasi tot $q \in E_2$. Ara però siguin $q_1, q_2 \in E_2$. Considerem $r \in E$ tal que $\phi(r) = q_2 - q_1$ aleshores per a cada $p \in \phi^{-1}(q_1)$, $p + r \in \phi^{-1}(q_2)$:

$$\phi(p+r) = \phi(p) + \phi(r) = q_1 + (q_2 - q_1) = q_2$$

Així considerant l'aplicació $\tau_r : E_1 \longrightarrow E_1$ que com hem mencionat és un isomorfisme, obtenim el resultat.

($\#\phi^{-1}(q) = \deg_s(\phi)$ es compleix per a tot $q \in E_2$ tret d'un nombre finit, però s'observa de la demostració que ens hagués estat prou saber-ho per a un únic punt).

ii) Siguin ara $p_1, p_2 \in E_1$ tals que $\phi(p_1) = \phi(p_2) = q$ i sigui $r = p_1 - p_2$. Aleshores $\phi(r) = \mathcal{O}_{E_2}$ i $\phi \circ \tau_r = \phi$. Per a $p \in E_1$:

$$\phi \circ \tau_r(p) = \phi(p+r) = \phi(p) + \phi(r) = \phi(p)$$

Ara, τ_r és un isomorfisme i, per tant, $e_{\tau_r}(p) = 1 \quad \forall p \in E_1$ i varem veure prèviament que donades dues aplicacions, l'índex de ramificació de la composició és la multiplicació d'índexos:

$$e_\phi(p_1) = e_{\phi \circ \tau_r}(p_1) = e_\phi(p_1 + r) e_{\tau_r}(p_1) = e_\phi(p_2)$$

i tots els punts a l'antiimatge de q tenen el mateix índex de ramificació. Concloent:

$$(\deg_s(\phi))(\deg_i(\phi)) = \deg(\phi) = \sum_{p \in \phi^{-1}(q)} e_\phi(p)$$

Triant un p^* qualsevol d'entre l'antiimatge de q :

$$(\deg_s(\phi))(\deg_i(\phi)) = (\#\phi^{-1}(q))e_\phi(p^*) = (\deg_s(\phi))e_\phi(p^*)$$

□

Hem observat com la condició de morfisme de grups d'una isogènia ens ha permès obtenir una descripció més directa dels graus separable i inseparable de la isogènia i les extensions entre cossos de funcions que indueix. Vegem més resultats interessants:

Proposició 3.3.15. *Donada $\phi : E_1 \longrightarrow E_2$, el nucli de ϕ i el grup d'automorfismes de $\overline{K}(E_1)$ que fixen $\phi^*(\overline{K}(E_2))$ son isomorfs*

Demostració. Considerem l'aplicació

$$I : \ker(\phi) \longrightarrow \text{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))]$$

$$P \longmapsto \tau_p^*$$

essent τ_p^* el *pullback* de l'aplicació translació per p i veiem que és un isomorfisme:

Comencem observant que efectivament si $p \in \ker(\phi)$, $\tau_p^* \in \text{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))]$. Sigui $f \in \overline{K}(E_2)$ aleshores

$$\tau_p^*(\phi^*(f)) = (\phi \circ \tau_p)^*(f) = \phi^*(f)$$

ja que $\phi \circ \tau_p = \phi$.

Tenim que donats $p, q \in \ker(\phi)$ $I(p + q) = \tau_{p+q}^* = (\tau_p \circ \tau_q)^* = I(p) \circ I(q)$ i I és morfisme de grups.

Finalment, pel teorema anterior $\ker(\phi) = \#\phi^{-1}(\mathcal{O}) = \deg_s(\phi)$ i, recuperant un resultat de teoria de Galois

$$\text{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))] \leq \deg_s(\phi) = \#\ker(\phi)$$

Així per a veure que I és isomorfisme serà suficient veure'n la injectivitat:

Vegem $\ker(I)$:

$$p \in \ker(I) \iff \tau_p \equiv \text{Id}_{\text{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))]} \iff f(p) = f(\mathcal{O}) \quad \forall f \in \overline{K}(E_1) \implies p = \mathcal{O}$$

Amb tot, hem construït un isomorfisme de $\ker(\phi)$ a $\text{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))]$ □

Arribem així a un dels resultats que ens aproparan més a aproximar el còmput de $E(K)$:

Teorema 3.3.16. *Sigui $\phi : E_1 \longrightarrow E_2$ isogènia separable, aleshores és no-ramificada,*

$$\#\ker \phi = \deg(\phi)$$

i $\overline{K}(E_1)/\phi^(\overline{K}(E_2))$ és una extensió de Galois.*

Demostració. Si ϕ és separable, sabem, altre cop pel teorema anterior, $\#\phi^{-1}(q) = \deg_s(\phi) = \deg(\phi) \forall q \in E_2$. Ara, sigui $q = O$:

$$\#\ker(\phi) = \deg(\phi).$$

Finalment veiem que el grup de $\phi^*(\overline{K}(E_2))$ -automorfismes de l'extensió $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ té $\deg(\phi) = [\overline{K}(E_1) : \phi^*(\overline{K}(E_2))]$ elements condició per a ser extensió de Galois. $\square$

En aquest resultat trobem per primer cop una noció de contar punts. A partir d'ara, donada una isogènia separable, sabem exactament la quantitat de punts que té el seu nucli. A la demostració de la fita de Hasse, aquest fet serà clau.

Corol·lari 3.3.17. *Siguin*

$$\phi : E_1 \longrightarrow E_2 \quad i \quad \psi : E_1 \longrightarrow E_3$$

isogènies no constants amb ϕ separable. Si $\ker(\phi) \subset \ker(\psi)$ aleshores existeix una única isogènia

$$\theta : E_2 \longrightarrow E_3$$

tal que $\psi = \theta \circ \phi$

Demostració. Acabem de veure, com ϕ és separable aleshores $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ és una extensió de Galois. Ara com $\ker(\phi) \subset \ker(\psi)$ com a subgrups de E_1 , recordant (3.3.15) tenim que $\text{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))] \subset \text{Aut}[\overline{K}(E_1)/\psi^*(\overline{K}(E_3))]$ amb el que tenim inclusió de cossos:

$$\psi^*(\overline{K}(E_3)) \subset \phi^*(\overline{K}(E_2)) \subset \overline{K}(E_1)$$

Ara, recordem un resultat "Donada una injecció entre cossos de funcions $(\iota : K(E_2) \hookrightarrow K(E_1))$ existeix una única aplicació no constant $\phi : E_1 \longrightarrow E_2$ tal que el pullback $\phi^* = \iota$ ". Prenent com a cossos $\psi^*(\overline{K}(E_3)) \subset \phi^*(\overline{K}(E_2))$ i ι la inclusió tenim que existeix una única aplicació $\theta : E_2 \longrightarrow E_3$ amb

$$\phi^*(\theta^*(\overline{K}(E_3))) = \psi^*(\overline{K}(E_3))$$

que alhora, implica $\theta \circ \phi = \psi$. Ara θ és isogenia ja que

$$\theta(O_{E_2}) = \theta(\phi(O_{E_1})) = \psi(O_{E_1}) = O_{E_3}$$

$\square$

Capítol 4

Fita de Hasse per a cossos finits

En aquest capítol donarem els últims resultats necessaris per a la demostració de la fita de Hasse que, com veurem, serà pràcticament directa.

4.1 La diferencial invariant

Hem vist, al teorema 2.3.16, que per a una isogènia separable, el nucli té tants elements com el grau de la isogènia. Seguint per aquest camí, voldrem veure la separabilitat d'una isogènia en particular, per això però necessitarem de la diferencial invariant.

Hem vist que tota corba el·líptica es pot relacionar amb una equació de Weierstrass. Aleshores suposem E/K donada per

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

Definició 4.1.1. *Definim la diferencial invariant:*

$$\omega = \frac{d(x)}{2y + a_1x + a_3} = \frac{d(y)}{3x^2 + 2a_2x + a_4 - a_1y}$$

Tot i que normalment farem servir la primera fórmula.

El nom de diferencial invariant prové de la següent propietat:

Proposició 4.1.2. *Sigui $\omega \in \Omega_E$ la diferencial invariant, i sigui τ_q l'aplicació translació per q ($\tau_q(p) = p + q$). Aleshores*

$$\tau_q^*(\omega) = \omega$$

Demostració. Donat que Ω_E és un $\overline{K}(E)$ -espai vectorial de dimensió 1 (per un resultat que no recordem) existeix una funció $\alpha_q \in \overline{K}(E)^*$ tal que

$$\tau_q^*(\omega) = \alpha_q \omega$$

Observem que com τ_q és isomorfisme, la imatge de la diferencial invariant no pot ser nul·la i, per tant, $\alpha_q \neq 0$. Ara, prenent divisors i tenint en compte que l'ordre d'un producte és la suma d'ordres,

$$\operatorname{div}(\tau_q^*(\omega)) = \operatorname{div}(\alpha_q \omega) = \operatorname{div}(\alpha_q) + \operatorname{div}(\omega)$$

$$\operatorname{div}(\alpha_q) = \tau_q^*(\operatorname{div}(\omega)) - \operatorname{div}(\omega)$$

Ara com $\text{div}(\omega) = 0$, tenim que $\text{div}(\alpha_q)$ no té ni zeros ni pols, i per tant, $\alpha_q \in \overline{K}^*$. Fins ara, hem vist que $\tau_q^*(\omega)$ és, per a cada q un múltiple de ω . Vegem que per a tot q $\alpha_q = 1$:

Considerem l'aplicació:

$$\begin{aligned} f : E &\longrightarrow \mathbb{P}^1 \\ q &\longmapsto [\alpha_q, 1] \end{aligned}$$

És fàcil veure que es pot computar α_q com a una aplicació racional de les coordenades de q a partir de la fórmula per a la suma de dos punts que hem donat al capítol anterior. Aleshores f és una aplicació racional entre corbes algebraiques llises, i per (1.2.1) f és exhaustiva o constant.

Observem que $\nexists q \in E \mid \alpha_q = 0$ i per tant $[0, 1] \notin f(E)$, amb el que α_q és constant per a tot q .

Ara, $\alpha_O = 1$ ja que τ_q és la identitat en E i tenim que

$$\forall q \in E, \alpha_q = 0 \implies \forall q \in E, \tau_q^*(\omega) = \omega$$

□

La principal utilitat de la diferencial invariant és la linealitzar la suma d'isogènies. El següent resultat ens permetrà relacionar la suma d'isogènies (a partir de l'estructura de grups de les corbes el·líptiques) amb la suma a l'espai vectorial de formes diferencials.

Teorema 4.1.3. *Siguin E_1 i E_2 corbes el·líptiques i ω el diferencial invariant en E i dues isogènies $\phi, \psi : E_1 \longrightarrow E_2$. Aleshores*

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$$

Demostració. Observem que si $\phi = [0]$ o $\psi = [0]$ no hi ha res a demostrar.

Si $\phi + \psi = [0]$, aleshores $\psi = -\phi$, amb el que $\psi^* = \phi^* \circ [-1]^*$. Ara, recordem el primer apartat del lema (2.2.6). Sigui $(x, y) \in E_1$

$$[-1](x, y) = (x, -y - a_1x - a_3)$$

Aleshores,

$$\psi^*(\omega) = [-1]^* \left(\frac{d(x)}{2y + a_1x + a_3} \right) = \frac{d(x)}{2(-y - a_1x - a_3) + a_1 + a_3}$$

i,

$$\psi^*(\omega) = \frac{d(x)}{2(-y - a_1x - a_3) + a_1x + a_3} = \frac{d(x)}{(-1)(2y + a_1x + a_3)} = -\omega$$

I hem provat el resultat per a $\phi + \psi = 0$.

Suposem ara que $\phi, \psi, \phi + \psi \neq 0$. Considerem $p_1, p_2 \in E_2$ punts genèrics i $p_3 \in E_2$ i les seves funcions coordenades x_i, y_i de manera que

$$p_i = (x(p_i), y(p_i)) = (x_i, y_i) \quad \text{i,} \quad p_3 = p_1 + p_2$$

voldrem veure que aplicar la diferencial invariant manté la relació entre els punts.

Considerem per a cada (x_i, y_i) la diferencial:

$$\omega(x_i, y_i) = \frac{d(x_i)}{2y_i + a_1x_i + a_3} \in \Omega_{E_2}$$

Ara, recordant la fórmula per la suma i les propietats de les formes diferencials, podem escriure $\omega(x_3, y_3)$ en termes de $\omega(x_1, y_1)$ i $\omega(x_2, y_2)$:

$$\omega(x_3, y_3) = f(x_1, y_1, x_2, y_2)\omega(x_1, y_1) + g(x_1, y_1, x_2, y_2)\omega(x_2, y_2)$$

amb f, g funcions racionals en x_1, y_1, x_2, y_2 . Voldrem veure que aquestes funcions son idènticament 1. Es pot veure desenvolupant les fórmules i calculant, tot i que ens sembla més interessant fer servir les propietats de la diferencial invariant.

Si donem a x_2, y_2 valors d'un punt fix q tal que $x_2 = x(q)$ i $y_2 = y(q)$, aleshores la funció x_2 és constant i $\omega(x_2, y_2) = 0$ ($\Leftarrow d(x_2) = 0$). Ara, observem per coeficients

$$\omega(x_3, y_3) = \tau_q^*(\omega(x_1, y_1)) = \omega(x_1, y_1)$$

per la invariabilitat de la diferencial sota translacions. Si $\omega(x_2, y_2) = \omega(x(q), y(q)) = 0$ i $\omega(x_3, y_3) = \omega(x_1, y_1)$ tenim que necessàriament $f(x_1, y_1, x(q), y(q)) \equiv 1$ com a funció racional de x_1, y_1 . Com aquest raonament és vàlid per a $q \in E_2$ qualsevol, f ha de ser idènticament 1. Repetir aquest raonament per a x_2, y_2 ens dona com a resultat que g ha de ser, alhora, idènticament 1 i tenim:

$$\omega(x_3, y_3) = \omega(x_1, y_1) + \omega(x_2, y_2)$$

Siguin ara x, y funcions de coordenades en E_1 i interpretant x_i, y_i com

$$(x_1, y_1) = \phi(x, y), \quad (x_2, y_2) = \psi(x, y), \quad (x_3, y_3) = (\phi + \psi)(x, y)$$

On $x, y \in K(E_1)$. Substituint, obtenim

$$(\omega \circ (\phi + \psi))(x, y) = (\omega \circ \phi)(x, y) + (\omega \circ \psi)(x, y)$$

i, de la definició de pullback en diferencials a partir de pullback de les funcions tenim que l'expressió és equivalent a

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$$

□

Vegem dos resultats que justifiquen la importància de la diferencial invariant.

Corol·lari 4.1.4. *Sigui ω diferencial invariant en E/K i $m \in \mathbb{Z}$ un enter.*

$$i) [m]^*\omega = m\omega.$$

ii) *Si m no és divisor de zero en K ($m \neq 0$ i m i $\text{char}(K)$ coprimers), l'aplicació multiplicació per m és endomorfisme no constant i separable.*

Demostració. Provem primer $[m]^*\omega = m\omega$ per inducció. Per a $m = 0$ i $m = 1$ el resultat és immediat.

Ara, suposem cert per a m . Considerem $\phi = [m]$ i $\psi = [1]$ (al capítol anterior hem vist que $[m]$ és isogènia), pel teorema previ:

$$[m+1]^*\omega = [m]^*\omega + \omega = m\omega + \omega = (m+1)\omega$$

Per a $m < 0$ podem repetir l'argument amb $\psi = [-1]$ i estenem el resultat a tot $\mathbb{Z}$.

Observem ràpidament que si m és segons les condicions de ii),

$$[m]^*\omega = m\omega \neq 0$$

i, per (1.3.7) l'aplicació $[m]$ és separable.

□

Arribem així al resultat que serà ingredient clau per a la demostració de la fita de Hasse.

Proposició 4.1.5. *Sigui $\text{char}(K) = p > 0$ i sigui $E/\mathbb{F}_q$ ($q = p^r$). Sigui $\phi : E \rightarrow E$ el q -èssim endomorfisme de Frobenius. Siguin $n, m \in \mathbb{Z}$, aleshores l'aplicació*

$$m + n\phi : E \rightarrow E$$

és separable si i només si $p \nmid m$

Demostració. Sigui ω diferencial invariant en E , ara de (1.3.7) un morfisme de corbes és separable si i només si el pullback que indueix és no nul. Així, un morfisme ψ és no separable si i només si (en particular) $\psi^*\omega = 0$. Sigui $\psi = m + n\phi$, aplicant el corol·lari anterior:

$$(m + n\phi)^*\omega = m\omega + n\phi^*(\omega)$$

Ara $\phi^*(\omega) = 0$ ja que ϕ és inseparable o, alternativament, $\phi^*(d(x)) = d(x^q) = 0$. Aleshores

$$(m + n\phi)^*\omega = m\omega$$

que és zero si i només si $p|m$ □

Corol·lari 4.1.6. *Amb la mateixa notació,*

$$1 - \phi : E \rightarrow E$$

és separable

4.2 Isogènia dual

En aquesta secció introduïrem el concepte d'isogènia dual qua actuarà com una mena de invers per a una isogènia donada i donarà diversos resultats interessants.

Recordant la teoria de divisors, una isogènia no constant qualsevol ($\phi : E_1 \rightarrow E_2$) induïx una aplicació entre el grup de divisors de les corbes i, en particular sobre els grups de Picard.

$$\begin{aligned} \phi^* : \text{Div}(E_2) &\rightarrow \text{Div}(E_1), & \text{restringint: } \phi^* : \text{Pic}^0(E_2) &\rightarrow \text{Pic}^0(E_1) \\ (q) &\mapsto \sum_{p \in \phi^{-1}(q)} e_\phi(p)(p) & \text{on, } \deg(D) = 0 &\implies \deg(\phi^*(D)) = 0 \end{aligned}$$

Per altra banda tenim definit un isomorfisme natural de la corba al seu grup de Picard⁰ (3.2.11)

$$\begin{aligned} \kappa : E &\rightarrow \text{Pic}^0(E) \\ p &\mapsto \overline{(p) - (O)} \end{aligned}$$

Amb tot, podem construir un morfisme en direcció inversa a una isogènia donada:

$$\hat{\phi} : E_2 \xrightarrow{\kappa_2} \text{Pic}^0(E_2) \xrightarrow{\phi^*} \text{Pic}^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1 \quad (4.2.1)$$

Proposició 4.2.1. *Sigui $\phi : E_1 \longrightarrow E_2$ una isogènia no constant i $\hat{\phi}$ definida com abans. Aleshores:*

$$\hat{\phi} \circ \phi(p) = [\deg(\phi)]p$$

Demostració. Sigui $q \in E_2$. Considerem $\hat{\phi}(q)$:

$$\hat{\phi}(q) = \text{sum}\{\phi^*((q) - (\mathcal{O}))\}$$

Ara, aplicant ϕ^* i sum (que no és més que passar de la suma formal dels punts en divisors a la suma geomètrica en E) obtenim

$$\hat{\phi}(q) = \text{sum} \left(\sum_{p \in \phi^{-1}(q)} [e_\phi(p)](p) - \sum_{r \in \phi^{-1}(\mathcal{O})} [e_\phi(r)](r) \right)$$

Aleshores, recordant el teorema (3.3.14), l'índex de ramificació d'una isogènia no constant en qualsevol punt és el grau inseparable de la isogènia.

$$\phi(q) = [\deg_i(\phi)] \left(\sum_{p \in \hat{\phi}^{-1}(q)} p - \sum_{r \in \hat{\phi}^{-1}(\mathcal{O})} r \right)$$

Ara, si fixem $p_0 \in \phi^{-1}(q)$ trobem que podem pensar el conjunt d'antiimatges de q com

$$\phi^{-1}(q) = p_0 + \ker(\phi)$$

Així podem reescriure:

$$\hat{\phi}(q) = [\deg_i(\phi)] \left(\sum_{p \in \phi^{-1}(q)} p - \sum_{r \in \phi^{-1}(\mathcal{O})} r \right) = [\deg_i(\phi)] \left(\sum_{\mu \in \ker(\phi)} (p_0 + \mu) - \sum_{r \in \phi^{-1}(\mathcal{O})} r \right)$$

Observant que $\ker(\phi) = \phi^{-1}(\mathcal{O})$ i recordant també que la quantitat d'antiimatges d'un punt és igual al grau separable de la isogènia tenim

$$\hat{\phi}(q) = [\deg_i(\phi)] \left(\sum_{\mu \in \phi^{-1}(q)} p_0 \right) = [\deg_i(\phi)][\deg_s(\phi)]p_0 = [\deg(\phi)]p$$

com ho hem fet per a qualsevol $p \in \phi^{-1}(q)$ obtenim el resultat:

$$\hat{\phi}(q) = \hat{\phi} \circ \phi(p) = [\deg(\phi)]p$$

□

Hem vist que existeix, donada una isogènia ϕ , una aplicació $\hat{\phi}$ tal que $\hat{\phi} \circ \phi = [\deg(\phi)]$ que s'obté a partir del pullback i de les imatges dels punts en els grups de Picard però no sabem si aquesta aplicació és un morfisme de corbes, o si és ni tan sols una aplicació racional. El següent resultat ens confirma que l'aplicació $\hat{\phi}$ és una isogènia.

Teorema 4.2.2. *Sigui $\phi : E_1 \longrightarrow E_2$ una isogènia no constant de grau m existeix una única isogènia $\hat{\phi} : E_2 \longrightarrow E_1$ tal que $\hat{\phi} \circ \phi = [m]$ sobre E_1 .*

Anomenarem a $\hat{\phi}$ la isogènia dual de ϕ

Demostració. Provarem primer la unicitat:

Siguin $\hat{\phi}, \hat{\phi}'$ dues isogènies tals que amb compondre-les amb ϕ obtenim l'aplicació multiplicar per m . Aleshores, considerem la isogènia $\hat{\phi} - \hat{\phi}'$:

$$(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = [0]$$

Ara com hem suposat que ϕ no és constant, ho ha de ser $\hat{\phi} - \hat{\phi}' = [0]$ per a tot punt a la imatge de ϕ que, com no és constant, és tot E_2 .

De cara a provar l'existència, observarem primer que si suposem l'existència de $\hat{\phi}$ i $\hat{\psi}$ per a isogènies $\phi : E_1 \rightarrow E_2, \psi : E_2 \rightarrow E_1$ de graus m, n respectivament, observem que les isogènies duals han de commutar amb la composició:

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [nm]$$

I tenim que $(\hat{\phi} \circ \hat{\psi})$ compleix les propietats per a ser la isogènia dual de $\psi \circ \phi$. Així només ens cal demostrar l'existència de la isogènia dual per isogènies separables i morfismes de Frobenius, ja que qualsevol altra isogènia es podrà escriure com a composició de isogènies d'aquest tipus (1.2.17), i la dual serà, aleshores, la composició de les duals.

Veiem primer el cas en que ϕ és separable. Com ϕ és de grau m i separable

$$\#\ker(\phi) = m \implies \ker(\phi) \subset \ker([m])$$

ja que $\ker\phi$ és un subgrup de E d'ordre m ($\subset E[m]$) i sabem per (3.3.17) que aleshores $\exists! \hat{\phi} : E_2 \rightarrow E_1$ tal que

$$\hat{\phi} \circ \phi = [m]$$

Suposem ara que ϕ és el q -èssim morfisme de Frobenius on $q = p^e$, aleshores ϕ serà la composició del p -èssim morfisme de Frobenius amb si mateix e cops. Per tant, ens serà prou demostrar l'existència de la dual per al p -èssim morfisme de Frobenius éssent p primer.

Sigui aleshores ϕ el p -èssim morfisme de Frobenius, $\deg(\phi) = p$. Així, volem veure que existeix una isogènia $\hat{\phi}$ tal que

$$\hat{\phi} \circ \phi = [p]$$

Si estudiem la isogènia $[p]$, i treballant amb el fet que ens trobem en un cos K , $\text{char}(K) = p$ tenim que, per a una diferencial invariant ω ,

$$[p]^*\omega = p\omega = 0$$

i $[p]$ és una isogènia no separable i es pot expressar com

$$[p] = \psi \circ \phi^e$$

On ψ és separable i ϕ^e és algun morfisme de Frobenius. De la descomposició de $[p]$ podem extreure:

$$[p] = (\psi \circ \phi^{e-1}) \circ \phi$$

I obtenim:

$$\hat{\phi} = \psi \circ \phi^{e-1}$$

□

Amb tot, hem vist que existeix la isogènia dual per a isogènies separables i per a morfismes de Frobenius. Hem vist també que la composició de isogènies duals és la isogènia dual de la composició. Aquests resultats amb (1.2.17) ens asseguren que per a qualsevol isogènia no constant ϕ , existeix una única isogènia $\hat{\phi}$, definida com a (4.2.1) tal que $\hat{\phi} \circ \phi = [\deg(\phi)]$. Havent vist que existeix definim aleshores la isogènia dual per a qualsevol isogènia (si $\phi = [0]$, $\hat{\phi} = [0]$) com l'aplicació existència de la qual acabem de provar.

El següent teorema ens proporcionarà les propietats bàsiques de la isogènia dual.

Teorema 4.2.3. *Sigui $\phi : E_1 \longrightarrow E_2$ una isogènia de grau m i $\hat{\phi}$ la seva dual.*

i) *La composició de ϕ i $\hat{\phi}$ dona lloc a multiplicació per m en ambdues corbes:*

$$\hat{\phi} \circ \phi = [m] \quad \text{en } E_1,$$

$$\phi \circ \hat{\phi} = [m] \quad \text{en } E_2.$$

ii) *Sigui $\psi : E_2 \longrightarrow E_3$ una altra isogènia. Aleshores*

$$\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}.$$

iii) *Sigui $\psi : E_1 \longrightarrow E_2$ una altra isogènia. Aleshores*

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}.$$

iv) *Per a tot $n \in \mathbb{Z}$,*

$$\widehat{[n]} = [n] \quad \text{i} \quad \deg([n]) = n^2$$

v)

$$\deg(\hat{\phi}) = \deg(\phi).$$

vi)

$$\hat{\hat{\phi}} = \phi.$$

Demostració. Observem que el teorema és trivial o manca d'interés si ϕ o ψ són constants, així que per a tota la demostració suposarem que les isogènies són totes no constants.

i) La primera part és la definició de isogènia dual. Per a la segona, considerem

$$(\phi \circ \hat{\phi}) \circ \phi = \phi \circ [m] = [m] \circ \phi$$

amb el que $\phi \circ \hat{\phi} = [m]$.

ii) Sigui $n = \deg(\psi)$ tenim

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n \circ \phi] = [n] \circ \hat{\phi} \circ \phi = [nm]$$

i, com existeix una única isogènia amb aquesta propietat per a $\psi \circ \phi$ tenim

$$\hat{\phi} \circ \hat{\psi} = \widehat{\psi \circ \phi}$$

- iii) Siguin $x_1, y_2 \in K(E_1)$ i $x_2, y_2 \in K(E_2)$ les funcions coordenada per a cada corba. Podem considerar E_2 com una corba el·líptica definida sobre el cos $K(E_1) = K(x_1, y_1)$
- i. Com una isogènia queda determinanda per la imatge del punt genèric podem identificar cada isogènia amb un punt (racional) de la corba:

$$\phi(x_1, y_1) \in E_2(K(x_1, y_1))$$

Podem fer el mateix per a $(\phi + \psi)$ i ψ , aleshores, considerem el divisor:

$$D = ((\phi + \psi)(x_1, y_1)) - (\phi(x_1, y_1)) - (\psi(x_1, y_1)) + (\mathcal{O})$$

Per construcció, aquest divisor suma $\mathcal{O}$ i és per tant, linealment equivalent a 0, és a dir, existeix una funció $f \in K(x_1, y_1)(E_2) = K(x_1, y_1, x_2, y_2)$ que, considerada funció de x_2, y_2 té divisor D .

Ara canviem de perspectiva i considerem f com a funció de x_1, y_1 , és a dir un element del cos de funcions de $E_1/K(x_2, y_2)$. Sigui ara $p_1 \in E_1(\overline{K(x_2, y_2)})$ tal que $\phi(p_1) = (x_2, y_2)$ aleshores de D podem veure que f presenta un pol en p_1 (ja que el coeficient que acompanyaria a p_1 és negatiu). De igual manera, f té un pol e p_1 si $\psi(p_1) = (x_2, y_2)$ i un zero si $(\phi + \psi)(p_1) = (x_2, y_2)$. De fet

$$\text{ord}_{p_1}(f) = e_{\phi, \psi, (\phi + \psi)}(p_1)$$

Així l'ordre de f en els punts (x_2, y_2) queda determinat pels índexs de ramificació de les isogènies considerades. Per tant, com a funció de x_1, y_1 , f té divisor:

$$(\phi + \psi)^*((x_2, y_2)) - \phi^*((x_2, y_2)) - \psi^*((x_2, y_2)) + \sum a_i(p_i) \in \text{Div}_{\overline{K(x_2, y_2)}}(E_1)$$

on els $p_i \in E_1(\overline{K})$, és a dir, l'últim terme és un divisor de E_1/K .

Ara, com hem computat el divisor d'una funció, ha de sumar $\mathcal{O} \in E_1$, per tant, $(\phi + \psi)^*((x_2, y_2)) - \phi^*((x_2, y_2)) - \psi^*((x_2, y_2))$ ha de ser un divisor fix de E_1 i no depèn de x_2, y_2 . Finalment, recuperant (4.2.1), observem que el que acabem de demostrar és :

$$(\widehat{\phi + \psi})(x_2, y_2) - \hat{\phi}(x_2, y_2) - \hat{\psi}(x_2, y_2)$$

no depèn de x_2, y_2 . Així podem triar $(x_2, y_2) = \mathcal{O}$ i

$$(\widehat{\phi + \psi})(x_2, y_2) - \hat{\phi}(x_2, y_2) - \hat{\psi}(x_2, y_2) = 0$$

i obtenim

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}.$$

- iv) Clarament, el primer resultat és cert per a $n = 0, 1$ així, fent servir l'apartat anterior i suposant cert per a n

$$\widehat{[n + 1]} = \widehat{[n]} + \widehat{[1]}$$

i per inducció tenim el resultat per tot $n \in \mathbb{Z}$ (si escau, considerant $[-1]$ per a $n < 0$).

Sigui ara $d = \deg([n])$ i estudiem multiplicació per d . Per la definició d'isogènia dual, $[d] = \widehat{[n]} \circ [n] = [n^2]$ (ja que $\widehat{[n]} = [n]$). Com l'anell d'endomorfismes d'una corba el·líptica és un $\mathbb{Z}$ -mòdul lliure de torsió, $[d] = [n^2] \implies d = n^2$.

- v) Amb $m = \deg(\phi)$ aplicant els apartats anteriors:

$$m^2 = \deg([m]) = \deg(\phi \circ \hat{\phi}) = \deg(\phi) \deg(\hat{\phi}) = m \deg(\hat{\phi})$$

vi) Amb la mateixa notació:

$$\hat{\phi} \circ \phi = [m] = [\widehat{m}] = \widehat{\hat{\phi} \circ \phi} = \hat{\phi} \circ \hat{\phi}$$

obtenint $\phi = \hat{\hat{\phi}}$.

□

La definició de la isogènia dual ens permetrà demostrar resultats sobre el grau com a aplicació del grup d'homomorfismes entre dues corbes i $\mathbb{Z}$. El resultat més important serà poder considerar el grau com a una aplicació quadràtica.

Definició 4.2.4. *Definim l'aplicació grau de la manera més natural o intuïtiva:*

$$\deg : \text{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$$

$$\phi \longmapsto \deg(\phi)$$

Proposició 4.2.5. *L'aplicació grau és una forma quadràtica definida positiva*

Demostració. Que és definida positiva és obvi. Si $\phi \in \text{Hom}(E_1, E_2)$, aleshores $\deg(\phi) \geq 0$ i és zero si i només si ϕ és constant, és a dir $\phi = [0]$ (element neutre de $\text{Hom}(E_1, E_2)$).

Per a que sigu quadràtica cal que:

- i) $\forall \phi \in \text{Hom}(E_1, E_2), \deg(\phi) = \deg(-\phi)$. Ara però si considerem $-\phi = \phi \circ [-1]$ i tenint en compte que $\deg([-1]) = (-1)^2 = 1$ ho tenim.
- ii) El producte $\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ ha de ser bilineal. Considerem aleshores multiplicació pel grau:

$$[\langle \phi, \psi \rangle] = [\deg(\phi + \psi)] - [\deg(\phi)] - [\deg(\psi)]$$

i, de la definició d'isogènia dual i aplicant dual de la suma és suma de duals::

$$[\langle \phi, \psi \rangle] = \widehat{(\phi + \psi)} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi = \hat{\phi} \circ \psi + \hat{\psi} \circ \phi$$

I obtenim una expressió que és clarament lineal tant per ϕ com per a ψ (teorema anterior tercer apartat).

Ara com cada enter representa un únic endomorfisme, la bilinearitat de $[\langle \phi, \psi \rangle]$ es traspasa a la de $\langle \phi, \psi \rangle$

□

4.3 Fita de Hasse

Arribem finalment a poder demostrar la fita de Hasse. En aquesta secció, E serà una corba el·líptica definida sobre K el cos finit de q elements per a q alguna potència positiva d'un primer p . Volem estimar la quantitat d'elements de $E(K)$, el subgrup de E format

pels punts de E amb coordenades a $K \times K$ (o bé racionals).
 Sigui E amb equació de Weierstrass:

$$E : Y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Els punts de $E(K)$ es corresponen a solucions d'aquesta equació amb $(x, y) \in K^2$. A primera vista, podem considerar que, fixant $x \in K$ tenim, com a màxim, dos possibles valors de y que satisfan l'equació. Aleshores, com tenim q elements a K sabem que $\#E(K) \leq 2q + 1$. La fita de Hasse millora (per molt) aquesta cota. Per a la seva demostració però, necessitem del següent lema:

Lema 4.3.1. *Sigui A un grup commutatiu i*

$$d : A \longrightarrow \mathbb{Z}$$

una forma quadràtica definida positiva aleshores $\forall \phi, \psi \in A$,

$$|d(\phi - \psi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}.$$

Demostració. Per a $\phi, \psi \in A$ definim

$$L(\phi, \psi) = d(\phi - \psi) - d(\phi) - d(\psi)$$

Com d és forma quadràtica, L és bilineal. Com d és definida positiva, per a qualsevol $m, n \in \mathbb{Z}$,

$$0 \leq d(m\phi - n\psi) = m^2d(\phi) + mnL(\phi, \psi) + n^2d(\psi)$$

En particular, si prenem $m = -L(\phi, \psi)$ i $n = 2d(\phi)$ obtenim:

$$0 \leq d(\phi)[4d(\phi)d(\psi) - L(\phi, \psi)^2]$$

i, com $d(\phi) > 0$ (si $d(\phi) = 0$, $\phi = 0$ i el resultat és trivial) tenim que, necessàriament

$$4d(\phi)d(\psi) - L(\phi, \psi)^2 \geq 0$$

Recuperant la definició de $L(\phi, \psi)$:

$$|d(\phi - \psi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}.$$

□

Arrel d'aquest últim resultat podem donar i demostrar el teorema que ha motivat aquest treball.

Conjecturada per primer cop per Emil Artin en la seva tesi doctoral i demostrada per primer cop per Helmut Hasse l'any 1933:

Teorema 4.3.2 (Fita de Hasse). *Sigui E/K una corba el·líptica definida sobre K cos de q elements. Aleshores*

$$|\#E(K) - q - 1| \leq 2\sqrt{q}$$

Demostració. Recordant l'endomorfisme de Frobenius:

$$\phi : E \longrightarrow E$$

$$(x, y) \longmapsto (x^q, y^q)$$

Observem que els punts de $E(K)$ són exactament els punts fixos de ϕ .

$$p \in E(K) \iff \phi(p) = p$$

Aleshores

$$E(K) = \ker(1 - \phi)$$

Ara, per (4.1.6) l'aplicació $1 - \phi$ és separable, i, per (3.3.17) el cardinal del nucli és igual al grau de $1 - \phi$. Tenim:

$$\#E(K) = \deg(1 - \phi)$$

Finalment, per (4.2.5) el grau és una forma quadràtica definida positiva i podem aplicar el lema previ:

$$|\deg(1 - \phi) - \deg([1]) - \deg(\phi)| \leq 2\sqrt{\deg([1])\deg(\phi)}$$

Tenim (4.2.3) $\implies \deg([1]) = 1$ i per (1.2.16) $\deg(\phi) = q$. Podem concloure per tant,

$$|\#E(K) - 1 - q| \leq 2\sqrt{q}$$

□

Conclusions

L'objectiu d'aquest treball era demostrar la fita de Hasse per a corbes el·líptiques i aconseguir assolir uns coneixements bàsics sobre corbes algebraïques que ens permetessin arribar a poder enunciar i demostrar la fita de Hasse. El resultat ha estat satisfactori. Hem pogut definir i treballar amb conceptes claus de la teoria en corbes algebraïques com la ramificació dels morfismes entre corbes, la importància de la condició de separabilitat i l'espai de formes diferencials sobre una corba. Hem aconseguit fer una passa més enllà i hem definit i treballat amb el grup de divisors d'una corba que ens ha permès donar la definició del gènere a partir del teorema de Riemann. Tot i que ens hem quedat a les portes de poder demostrar el teorema de Riemann-Roch, hem desenvolupat prou teoria com per a conèixer tots els ingredients que hi apareixen i poder emportar-nos una intuïció del significat del resultat. Així, hem aconseguit una bona introducció a la teoria de corbes el·líptiques, on, gràcies a tot el material treballat sobre corbes algebraïques hem pogut veure la importància d'estar treballant amb corbes de gènere 1 i com ens permet concretar molts resultats. L'estudi de les isogènies, l'estructura de grup i la diferencial invariant ens han portat, en última instància, a demostrar la fita de Hasse.

És interessant haver vist la relació entre les corbes algebraïques i la teoria algebraica de nombres al llarg del treball, fet que ens ha permès recordar la proximitat a la teoria de nombres quan estàvem treballant conceptes púrament de geometria algebraica. De la mateixa manera, volem remarcar com la fita de Hasse s'ha pogut demostrar amb eïnes que apareixien de manera natural en la teoria, sense haver necessitat donar cap definició que no fos important per a la teoria general de corbes el·líptiques. Aquest fet ens ha empès a treballar molt sobre corbes algebraïques i el·líptiques de manera que el teorema central del treball pugui semblar pràcticament un corol·lari.

Podriem resumir les conclusions dient que considerem que aquest treball constitueix una bona introducció a la teoria de corbes el·líptiques que, culminant amb un teorema molt elegant, obre les portes a l'estudi de la teoria de nombres mitjançant la geometria algebraica.

Bibliografia

- [1] Silverman, J. H.: *The Arithmetic of Elliptic Curves*, Springer, Graduate Texts in Mathematics 106, 1986.
- [2] Fulton, W.: *Algebraic Curves: An Introduction to Algebraic Geometry*, Addison-Wesley Publishing Company, 1969.
- [3] Lang, S.: *Algebraic Number Theory*, Springer, Graduate Texts in Mathematics 110, 2nd edition, 1994.
- [4] Lang, S.: *Introduction to Algebraic and Abelian Functions*, Springer, Graduate Texts in Mathematics 89, 2nd edition, 1982.
- [5] Hartshorne, R.: *Algebraic Geometry*, Springer, Graduate Texts in Mathematics 52, 1977.
- [6] Matsumura, H.: *Commutative Algebra*, 2nd edition, Benjamin/Cummings Publishing Company, 1980.
- [7] Shafarevich, I. R.: *Basic Algebraic Geometry 1: Varieties in Projective Space*, 2nd edition, Springer, 1994.
- [8] Robert, A.: *Elliptic Curves*, Springer, Universitext, 2008.
- [9] Washington, L. C.: *Elliptic Curves: Number Theory and Cryptography*, 2nd edition, Chapman & Hall/CRC, 2008.
- [10] Vilageliu Giró, J.: *Toward logarithmic sheaves on singular varieties: marked points in line arrangements*, Treball Final de Màster, Universitat de Barcelona, 2025.
- [11] Roman, S.: *Field Theory*, Springer, Graduate Texts in Mathematics 158, 2nd edition, 2006.
- [12] Howie, J. M.: *Fields and Galois Theory*, 2nd printing, Springer Nature, London.