UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Corbes el·líptiques: Teorema de Mordell i Conjectura de Birch i Swinnerton-Dyer

Autor: Rubén García Pons

Director: Dr. Xavier Guitart Morales
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 20 de juny de 2021

Abstract

Elliptic curves play a very notable role in many number theory problems. In this work we study the structure of the group of rational points of elliptic curves defined over the rationals. More specifically, we give a proof of Mordell's Theorem and include some results to be able to present the Birch and Swinnerton-Dyer Conjecture.

Resum

Les corbes el·líptiques juguen un paper molt destacat en molts problemes en teoria de nombres. En aquest treball estudiem l'estructura del grup de punts racionals de corbes el·líptiques definides sobre els racionals. Més concretament, donem una demostració del Teorema de Mordell i incloem un conjunt de resultats per poder presentar la Conjectura de Birch i Swinnerton-Dyer.

Resumen

Las curvas elípticas juegan un papel muy importante en muchos problemas en teoría de números. En este trabajo estudiamos la estructura del grupo de puntos racionales de curvas elípticas definidas sobre los racionales. Más concretamente, damos una demostración del Teorema de Mordell e incluimos una serie de resultados para poder presentar la Conjetura de Birch y Swinnerton-Dyer.

2020 Mathematics Subject Classification. 14H52, 11G40, 11R34, 11R04, 11R29.

Agraïments

Vull donar les gràcies al Dr. Xevi Guitart per la proposta d'aquest tema i pel seguiment, les indicacions i les correccions durant tot el desenvolupament del treball. He après molt.

Quiero dar las gracias también a mis amigos y amigas, por haber hecho de estos cuatro años una etapa increíble.

Finalmente, a mis padres y a mi hermano, gracias, aunque creáis que todo el mérito es mío.

Índex

Introducció

L'estudi de les corbes el·líptiques ha sigut transcendental en molts problemes en teoria de nombres. El cas més destacat de la importància d'aquests objectes el podem trobar en la demostració de l'Últim Teorema de Fermat, on a cada presumpta solució (x, y, z), amb $xyz \neq 0$, de l'equació de Fermat, se li assigna una corba el·líptica amb unes certes propietats coneguda com a corba de Frey. Andrew Wiles va provar el 1995 que aquest tipus de corbes no existeixen, demostrant així l'Últim Teorema de Fermat.

Una corba el·líptica és una cúbica projectiva juntament amb un punt projectiu que satisfà una certa condició de regularitat. En aquest treball estudiarem principalment corbes el·líptiques definides sobre els racionals. Més concretament, ens centrarem en estudiar l'estructura del conjunt de punts racionals de corbes el·líptiques definides sobre $\mathbb{Q}$, és a dir, l'estructura del conjunt de punts amb coordenades racionals que satisfan l'equació que defineix la corba.

Les corbes el·líptiques tenen una riquesa algebraica i geomètrica molt destacada. Aquesta riquesa recau en el fet que podem definir geomètricament una llei d'addició sobre el conjunt de punts racionals d'una corba el·líptica que dota aquest conjunt d'estructura de grup abelià. Es coneixen resultats molt importants que ens permeten apropar-nos molt acuradament a l'estudi dels punts racionals d'una corba el·líptica definida sobre $\mathbb{Q}$. Un dels més rellevants és el Teorema de Mordell, demostrat el 1922 per Louis Mordell, que ens diu que el conjunt de punts racionals d'una corba el·líptica definida sobre $\mathbb{Q}$ és un grup abelià finitament generat, és a dir, donada una corba el·líptica amb coeficients racionals existeix un nombre finit de punts racionals de la corba a partir dels quals, utilitzant la llei d'addició mencionada anteriorment, podem trobar-ne tots els altres.

En l'estudi de l'estructura del grup de punts racionals d'una corba el·líptica trobem també una conjectura molt important: la Conjectura de Birch i Swinnerton-Dyer. Donada una corba el·líptica definida sobre $\mathbb{Q}$, la Conjectura de Birch i Swinnerton-Dyer ens relaciona el rang del grup de punts racionals de la corba amb un objecte analític associat a aquesta conegut com a funció L de la corba.

L'objectiu d'aquest treball és doble: d'una banda, donar la demostració del Teorema de Mordell; de l'altra, desenvolupar tota la teoria necessària per poder presentar en l'últim capítol de la memòria la Conjectura de Birch i Swinnerton-Dyer. Per fer-ho, necessitarem introduir alguns resultats previs. L'estructura de la memòria és la següent.

Al capítol 1 s'introdueixen definicions i resultats preliminars per poder definir el concepte de corba el·líptica al capítol 2.

Al capitol 2 es defineix què s'entén per corba el·líptica i s'introdueixen conceptes relacionats amb aquestes, com la llei de grup, els endomorfismes de corbes el·líptiques i l'invariant j. Es demostra que el conjunt de punts racionals d'una corba el·líptica amb la llei de grup mencionada abans té estructura de grup abelià i es presenta un endomorfisme de corbes el·líptiques que serà molt utilitzat durant tot el treball: l'endomorfisme $[n]$. Tot i que, majoritàriament, en tot el treball només considerem corbes el·líptiques definides sobre els racionals, en aquest capítol parlem breument de corbes el·líptiques definides sobre un cos finit. L'objectiu d'això és presentar el Teorema de Hasse, que serà utilizat en l'últim capítol del treball.

Al capítol 3 comencem a estudiar l'estructura del conjunt de punts racionals d'una corba el·líptica estudiant els seus punts de torsió. El resultat més important que demostrem en

aquest capítol és el Teorema de Lutz-Nagell, que ens diu com obtenir tots els punts de torsió d'una corba el·líptica definida sobre $\mathbb{Q}$. Com a conseqüència directa del Teorema de Lutz-Nagell, provem que el subgrup de torsió d'una corba el·líptica definida sobre $\mathbb{Q}$ és finit.

Al capítol 4 demostrem el Teorema de Mordell. La demostració d'aquest la dividim en tres parts: a la primera demostrem un teorema conegut com a Teorema de descens; a la segona desenvolupem la teoria d'altures; finalment, a la tercera part demostrem el Teorema feble de Mordell-Weil. D'aquest darrer donem dues demostracions diferents: d'una banda el demostrem utilitzant eines de teoria algebraica de nombres; de l'altra, donem una demostració basada en cohomologia de Galois.

Finalment, al capítol 5, presentem la funció L d'una corba el·líptica definida sobre $\mathbb{Q}$ i demostrem que aquesta funció convergeix en un semiplà concret del pla complex. Desenvolupada tota aquesta teoria, acabem el capítol enunciant la Conjectura de Birch i Swinnerton-Dyer.

1 Preliminars

En aquesta secció es definiran conceptes i es tractaran resultats que ens permetran més endavant definir què és una corba el·líptica i estudiar-ne algunes de les seves propietats.

Definició 1.1. *Siguin K un cos, $f \in K[x,y]$ un polinomi de grau n i $\mathbb{A}^2_K$ el pla afí. El conjunt*

$$C := \{(a,b) \in \mathbb{A}^2_K : f(a,b) = 0\}$$

s'anomena corba plana. Es diu que C és una recta si $gr(f) = 1$, que C és una cònica si $gr(f) = 2$ i que C és una cúbica si $gr(f) = 3$.

Escriurem

$$C : f(x,y) = 0$$

per denotar la corba plana C que ve donada pel polinomi f.

Exemple 1.2. Sigui $K = \mathbb{Q}$.

(a) $C : y - x = 0$ és una recta sobre $\mathbb{Q}$.

(b) $C : y - x^2 = 0$ és una cònica sobre $\mathbb{Q}$.

(c) $C : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Q}$, és una cúbica sobre $\mathbb{Q}$.

(d) Sigui $n \in \mathbb{N}$. La corba

$$C_n : x^n + y^n = 1$$

és una corba plana sobre $\mathbb{Q}$.

Recordem a continuació la definició d'espai projectiu sobre un cos K.

Definició 1.3. *Sigui $n \in \mathbb{N}$ $(n \geq 1)$. Es defineix l'espai projectiu de dimensió n sobre K com*

$$\mathbb{P}^n_K = \frac{K^{n+1} \setminus \{0\}}{\sim},$$

on $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ si i només si existeix $\lambda \in K^\times$ tal que $(x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)$.

Es denota la classe d'equivalència de $(x_0, \ldots, x_n)$ per $[x_0 : \ldots : x_n]$.

Particularment, ens interessarem pel pla projectiu $\mathbb{P}^2_K$. Dins de $\mathbb{P}^2_K$ distingim dos tipus de punts:

- Punts finits: són els punts $[x : y : z] \in \mathbb{P}^2_K$ amb $z \neq 0$. En aquest cas es té que $[x : y : z] = [\frac{x}{z} : \frac{y}{z} : 1]$.
- Punts de l'infinit: són els punts de $\mathbb{P}^2_K$ de la forma $[x : y : 0]$.

Recordem que es té una inclusió del pla afí $\mathbb{A}^2_K$ en $\mathbb{P}^2_K$ donada per:

$$i : \mathbb{A}^2_K \hookrightarrow \mathbb{P}^2_K$$

$$(x,y) \longmapsto [x : y : 1],$$

és a dir, podem identificar $\mathbb{A}^2_K$ amb els punts finits de $\mathbb{P}^2_K$.

Un problema que se'ns presenta a l'hora de treballar amb polinomis a $\mathbb{P}^2_K$ és que el conjunt de zeros d'un polinomi qualsevol no està ben definit. Per exemple, sigui $F = X^3 - YZ \in K[X,Y,Z]$ i sigui $[1:1:1] = [2:2:2] \in \mathbb{P}^2_K$. Es té que $F(1,1,1) = 0$, mentre que $F(2,2,2) = 4 \neq 0$. És a dir, no es pot dir si F s'anul·la o no al punt $[1:1:1]$. Introduïm a continuació el concepte de polinomi homogeni per solucionar aquest problema.

Definició 1.4. *Sigui K un cos. Sigui $F(X,Y,Z) \in K[X,Y,Z]$ un polinomi de grau n. Es diu que F és homogeni si tots els seus monomis tenen grau n, és a dir, si F és de la forma*

$$F(X,Y,Z) = \sum_{\substack{0 \leq i,j,k \leq n \\ i+j+k=n}} a_{ijk} X^i Y^j Z^k.$$

Treballar amb polinomis homogenis a $\mathbb{P}^2_K$ fa que el conjunt de zeros d'un polinomi homogeni F estigui ben definit. En efecte: si $F(X,Y,Z) \in K[X,Y,Z]$ és un polinomi homogeni de grau n, es té que $F(\lambda X, \lambda Y, \lambda Z) = \lambda^n F(X,Y,Z)$, per a tot $\lambda \in K^\times$. Per tant, si F és homogeni de grau n i $[x_1:y_1:z_1] = [x_2:y_2:z_2]$, se satisfà que $F(x_1,y_1,z_1) = 0$ si i només si $F(x_2,y_2,z_2) = 0$.

Donat $f \in K[x,y]$ un polinomi qualsevol podem transformar-lo en un polinomi homogeni (procés d'homogeneïtzació) de la manera següent:

Definició 1.5. *Sigui $f \in K[x,y]$ un polinomi de grau n. S'anomena homogeneïtzat de f al polinomi homogeni de grau n $F(X,Y,Z)$ donat per*

$$F(X,Y,Z) = Z^n f(\frac{X}{Z}, \frac{Y}{Z}).$$

Observem que podem recuperar f (procés de deshomogeneïtzació) fent $F(x,y,1) = f(x,y)$.

Per a poder definir el concepte de corba el·líptica en la secció següent necessitarem parlar de corbes projectives planes:

Definició 1.6. *Sigui K un cos. Sigui $F(X,Y,Z) \in K[X,Y,Z]$ un polinomi homogeni de grau n. S'anomena corba projectiva plana al conjunt*

$$\mathscr{C} := \{[a:b:c] \in \mathbb{P}^2_K : F(a,b,c) = 0\}.$$

Observació 1.7. El conjunt $\mathscr{C}$ de la Definició 1.6 està ben definit perquè el polinomi F és homogeni.

Escriurem

$$\mathscr{C} : F(X,Y,Z) = 0$$

per a denotar la corba projectiva plana $\mathscr{C}$ que ve donada pel polinomi homogeni F.

Definició 1.8. *Sigui K un cos. Sigui $C : f(x,y) = 0$ una corba plana sobre K. S'anomena completat projectiu de C (o homogeneïtzació de C) a la corba projectiva plana $\mathscr{C} : F(X,Y,Z) = 0$, on F és l'homogeneïtzat de f.*

Exemple 1.9. (a) El completat projectiu de la corba $C : y^2 = x^3 + Ax + B$ és

$$\mathscr{C} : Y^2Z = X^3 + AXZ^2 + BZ^3.$$

.

(b) El completat projectiu de la corba $C_n : x^n + y^n = 1$ és

$$\mathscr{C} : X^n + Y^n = Z^n.$$

.

Donada una corba $C : f(x, y) = 0$ sobre un cos K és molt natural voler estudiar el conjunt dels punts de C amb coordenades a un cos $L \supseteq K$, és a dir, el conjunt

$$C(L) := \{(x, y) \in L \times L : f(x, y) = 0\}.$$

Gran part d'aquest treball consistirà en estudiar el conjunt de punts amb coordenades racionals d'una corba el·líptica definida sobre $\mathbb{Q}$.

Veiem a continuació alguns exemples de com trobar punts racionals d'una corba plana C.

Exemple 1.10. (a) Sigui $C : x^2 + y^2 = 1$.

Observem primer que $(-1, 0) \in C(\mathbb{Q})$ i que si $P = (x, y) \in C(\mathbb{Q})$ amb $P \neq (-1, 0)$, aleshores el pendent que uneix $(-1, 0)$ i P és racional. Vegem ara el recíproc, és a dir, que si una recta que passa per $(-1, 0)$ té pendent racional, aleshores l'altre punt d'interesecció d'aquesta recta amb C té coordenades racionals, és a dir, pertany a $C(\mathbb{Q})$:

Considerem l'equació d'una recta que passi per $(-1, 0)$:

$$y = t(x + 1),$$

i busquem l'altre punt d'intersecció de la recta anterior amb C. Es té:

$$\left.\begin{array}{r} y = t(x+1) \\ y^2 + x^2 = 1 \end{array}\right\} \quad \Rightarrow \quad 1 - x^2 = t^2(x+1)^2.$$

Fixant t es té una equació quadràtica en x. Com que $x = -1$ és solució, s'obté que l'altra solució és

$$x = -\frac{t^2 - 1}{t^2 + 1} \quad \Rightarrow \quad y = \frac{2t}{1 + t^2} \quad \Rightarrow \quad P = \left(-\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{1 + t^2}\right).$$

Per tant, si $t \in \mathbb{Q}$, aleshores $P \in C(\mathbb{Q})$. Obtenim així una parametrització racional de la circumferència unitat, tal i com es veu a la Figura 1.

Observem que obtenim d'aquesta manera una bijecció entre $C(\mathbb{Q})$ i $\mathbb{Q} \cup \{\infty\}$, on ∞ és un punt tal que si $t = \infty$, aleshores $P = (-1, 0)$. Més concretament, observem que si t tendeix a ∞, es té $P = (-1, 0)$. Geomètricament parlant, si la recta que passa per $(-1, 0)$ és la recta vertical $x = -1$ (recta tangent a C per $(-1, 0)$), el segon punt d'intersecció entre la recta i C torna a ser $(-1, 0)$.

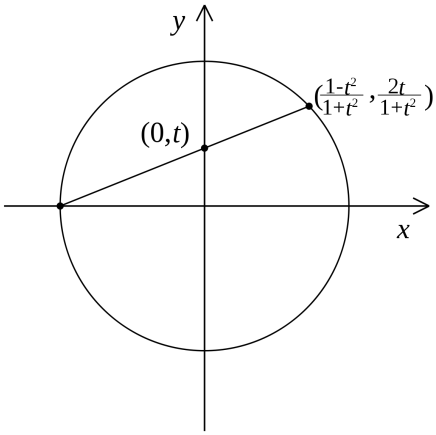

Figura 1: Parametrització racional de $C : x^2 + y^2 = 1$.

(b) Sigui $C : x^2 + y^2 = 3$. Vegem que $C(\mathbb{Q}) = \emptyset$:
Observem que és suficient veure que el completat projectiu de C

$$\mathscr{C} : X^2 + Y^2 = 3Z^2$$

tampoc té punts amb coordenades racionals.
Suposem que existeix $[a : b : c] \in \mathscr{C}(\mathbb{Q})$, és a dir, $a^2 + b^2 = 3c^2$, amb $a, b, c \in \mathbb{Q}$. Sense pèrdua de generalitat podem suposar que $a, b, c \in \mathbb{Z}$ i que són coprimers dos a dos. Reduïnt mòdul 4, tenim

$$a^2, b^2, c^2 \equiv 0, 1 \pmod 4 \quad \Rightarrow \quad a^2 + b^2 = 3c^2 \equiv 0, 3 \pmod 4.$$

Si $3c^2 \equiv 3 \pmod 4$, tindríem que $a^2 + b^2 \equiv 3 \pmod 4$, que no és possible. D'altra banda, si $3c^2 \equiv 0 \pmod 4$, aleshores $a^2 + b^2 \equiv 0 \pmod 4$, que implica que $a^2, b^2 \equiv 0 \pmod 4$. De $3c^2 \equiv 0 \pmod 4$ es dedueix també que $c^2 \equiv 0 \pmod 4$. Obtenim doncs que a^2, b^2, c^2 són nombres parells. Per tant, a, b, c també són nombres parells, que contradiu el fet que siguin coprimers dos a dos. Concloem així que $C(\mathbb{Q}) = \emptyset$.

Per finalitzar aquesta secció definim el concepte de corba projectiva plana regular.

Definició 1.11. *Sigui $\mathscr{C} : F(X, Y, Z) = 0$ una corba projectiva plana sobre un cos K. Sigui $P \in \mathscr{C}(\overline{K})$, on $\overline{K}$ denota la clausura algebraica del cos K. Es diu que P és singular si*

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Si alguna de les derivades anteriors no s'anul·la a P, es diu que el punt P és regular. Diem que $\mathscr{C}$ és una corba projectiva plana regular si tots els seus punts són regulars.

Observació 1.12. Anàlogament es defineix el concepte de corba plana regular per a una corba plana $C : f(x, y) = 0$ definida sobre un cos K. En aquest context, diem que $P \in C(\overline{K})$ és singular si

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

2 Corbes el·líptiques

En aquest capítol s'introdueix el concepte de corba el·líptica i es veu que es pot definir geomètricament una operació sobre el conjunt de punts d'una corba el·líptica que dota aquest conjunt de punts d'estructura de grup abelià. També s'estudien conceptes com l'invariant j i els endomorfismes d'una corba el·líptica.

2.1 Equació de Weierstrass

Comencem donant la definició de corba el·líptica.

Definició 2.1. *Sigui K un cos. Una corba el·líptica E definida sobre K és una corba projectiva plana cúbica regular de la forma*

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 = 0, \tag{2.1}$$

on $a_i \in K$, $1 \leq i \leq 6$.

Escriurem E/K per denotar una corba el·líptica definida sobre un cos K. L'equació (2.1) s'anomena *equació llarga de Weierstrass*. Fent $Z = 0$ a l'equació (2.1), s'obté que $X = 0$ i, per tant, l'únic punt de l'infinit de E és $\infty := [0 : 1 : 0]$.

Normalment treballarem amb coordenades no-homogènies (deshomogeneïtzem el polinomi $F(X, Y, Z)$ que defineix E) i estudiarem la corba afí

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2}$$

Es pot veure que si la característica del cos K és diferent de 2 i 3, l'equació (2.2) es pot transformar en

$$E : y^2 = x^3 + Ax + B, \tag{2.3}$$

amb $A, B \in K$. L'equació (2.3) s'anomena *equació de Weierstrass*.

A continuació presentarem un criteri de regularitat d'una equació de Weierstrass que ens caracteritzarà quan una equació d'aquest tipus defineix una corba el·líptica. Abans, però, recordem el concepte de discriminant d'un polinomi.

Definició 2.2. *Sigui K un cos. Sigui $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ un polinomi de grau n. Siguin $x_1, x_2, \ldots, x_n$ les arrels de $f(x)$ en $\overline{K}$. S'anomena discriminant de f a*

$$\Delta_f := a_n^{2n-2} \prod_{i<j} (x_i - x_j)^2.$$

Recordem també que si $f(x) = x^3 + ax^2 + bx + c \in K[x]$ és un polinomi cúbic, el discriminant de f ve donat per l'expressió

$$\Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

En particular, si considerem el polinomi $f(x) = x^3 + Ax + B \in K[x]$, es té que

$$\Delta_f = -4A^3 - 27B^2.$$

Definició 2.3. *Sigui $E : y^2 = f(x)$ una corba plana definida sobre un cos K, on $f(x) = x^3 + Ax + B$. S'anomena discriminant de E a*

$$\Delta_E := \Delta_f$$

Enunciem, finalment, el criteri de regularitat de què parlàvem.

Proposició 2.4. *Sigui K un cos amb $char(K) \neq 2$. Sigui $E : y^2 = f(x)$ una corba plana definida sobre K, on $f(x) = x^3 + Ax + B$. Aleshores E és una corba el·líptica si i només si $\Delta_E \neq 0$.*

Demostració. Sigui $F(x, y) = y^2 - f(x)$ i sigui $P = (x, y) \in E(\overline{K})$. P és un punt singular si i només si

$$\frac{\partial F}{\partial x} = -f'(x) = 0, \quad \frac{\partial F}{\partial y} = 2y = 0.$$

Com que $\text{char}(K) \neq 2$, de la segona igualtat tenim que $y = 0$. Afegint la condició que $P \in E(\overline{K})$, es té que P és singular si i només si $f(x) = f'(x) = 0$, és a dir, si i només si x és una arrel doble de f. De la definició de discriminant es dedueix, doncs, que P és singular si i només si $\Delta_E = 0$. □

D'ara en endavant, si no es diu el contrari, considerarem només corbes el·líptiques definides sobre $\mathbb{Q}$ de la forma

$$E : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q} \quad (\Delta_E \neq 0)$$

i ens centrarem principalment en estudiar el conjunt

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 + Ax + B\} \cup \{\infty\},$$

on $\infty = [0 : 1 : 0]$ és l'únic punt de l'infinit de E.

2.2 Llei de grup

Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre $\mathbb{Q}$. En aquest apartat definirem geomètricament una operació sobre $E(\mathbb{Q})$ que dotarà $E(\mathbb{Q})$ d'estructura de grup abelià. Veurem que el punt ∞ serà l'element neutre del grup. Denotarem aquesta operació per $+$. La definim a continuació.

Definició 2.5. *Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre $\mathbb{Q}$ i siguin $P_1, P_2 \in E(\mathbb{Q})$. Sigui r la recta que passa pels punts P_1 i P_2 (si $P_1 = P_2$, la recta r serà la recta tangent a E per P_1). La recta r interseca la corba en un tercer punt P_3'. Reflectint aquest punt respecte de l'eix x obtenim un altre punt P_3. Es defineix $P_1 + P_2$ com $P_1 + P_2 := P_3$ (veure Figura 2).*

Observació 2.6. De l'equació que defineix E es dedueix que si $P_3' = (x_3, y_3) \in E(\mathbb{Q})$, aleshores la reflexió de P_3' respecte de l'eix x, $P_3 = (x_3, -y_3)$, també pertany a $E(\mathbb{Q})$.

A l'hora d'estudiar l'estructura de $E(\mathbb{Q})$, tindríem un problema si, quan calculèssim la suma de punts de $E(\mathbb{Q})$ definida abans, obtinguèssim punts amb coordenades en alguna extensió de $\mathbb{Q}$. Veurem que això no succeeix, és a dir, que l'operació $+$ és tancada en $E(\mathbb{Q})$.

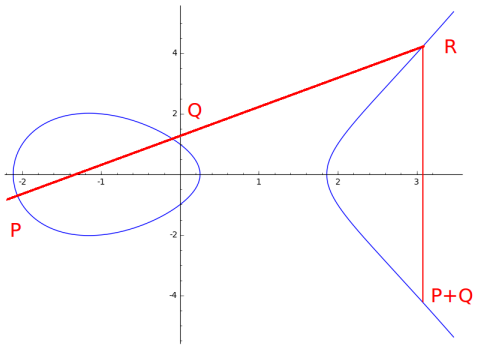

Figura 2: Suma de dos punts de la corba $E : y^2 = x^3 - 4x + 1$ sobre $\mathbb{R}$.

A continuació calcularem l'expressió en coordenades de $P_1 + P_2$ per a qualssevol dos punts P_1, P_2 de $E(\mathbb{Q})$. Abans, però, observem que el punt $\infty = [0 : 1 : 0] \in E(\mathbb{Q})$ pertany a qualsevol recta vertical. En efecte, si $r : x = t$ és una recta vertical, el completat projectiu de r ve donat per $X = tZ$. Clarament, el punt ∞ satisfà la darrera equació. Fem notar, doncs, que si per dos punts d'una corba el·líptica E passa una recta vertical, el tercer punt d'intersecció entre aquesta recta i E serà ∞.

Siguin $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{Q})$, on E ve donada per l'equació $y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Q}$. Procedim a calcular l'expressió de $P_1 + P_2$. Distingim casos:

1. $P_1 \neq P_2$ i $P_1, P_2 \neq \infty$. Distingim dos casos:

   (a) $x_1 \neq x_2$:
   El pendent de la recta r que passa per P_1 i P_2 és

   $$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

   L'equació de r és aleshores

   $$r : y = m(x - x_1) + y_1.$$

   Per trobar la intersecció de r amb E substituïm i obtenim

   $$(m(x - x_1) + y_1)^2 = x^3 + Ax + B.$$

   Desenvolupant el quadrat i agrupant termes s'obté l'equació

   $$0 = x^3 - m^2x^2 + \cdots .$$

   Com que x_1 i x_2 són solucions d'aquesta equació, la tercera arrel x_3 satisfá

   $$-(x_1 + x_2 + x_3) = -m^2. \tag{2.4}$$

   Aquest últim fet es dedueix de la teoria dels polinomis simètrics. Bàsicament, observem que si x_1, x_2, x_3 són les arrels del polinomi cúbic $x^3 + ax^2 + bx + c$, tenim les següents igualtats:

   $$\begin{aligned} x^3 + ax^2 + bx + c &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

De (2.4) s'obté

$$x_3 = m^2 - x_1 - x_2.$$

Per tant, el tercer punt d'intersecció de r i E és $P_3' = (x_3, m(x_3 - x_1) + y_1)$. Finalment, reflectint P_3' respecte l'eix x obtenim que $P_1 + P_2 = P_3 = (x_3, y_3)$, on

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1.$$

(b) $x_1 = x_2$:
La recta per P_1 i P_2 és vertical. Per tant, el tercer punt d'intersecció és ∞. Reflectint ∞ respecte l'eix d'abcisses obtenim ∞ un altre cop. (Això es pot deduir del fet que, quan reflectim el tercer punt d'intersecció respecte l'eix x, el que realment estem fent és unir aquest tercer punt d'intersecció amb el punt ∞ i veure on la recta vertical per aquests dos punts talla E. En el cas anterior, la recta que uneix ∞ i ∞ és la recta de l'infinit $Z = 0$. La recta de l'infinit talla $E : Y^2Z = X^3 + AXZ^2 + BZ^3$ amb multiplicitat 3 al punt ∞. Per tant, $P_1 + P_2 = \infty$.

2. $P_1 = P_2 = (x, y)$ i $P_1, P_2 \neq \infty$. Distingim dos casos:

a) $y \neq 0$:
La recta per P_1 i P_2 és la recta tangent a E per P_1 . Per trobar el pendent en aquest cas derivem implícitament i obtenim

$$2y\frac{dy}{dx} = 3x^2 + A \quad \Longrightarrow \quad m = \frac{dy}{dx} = \frac{3x^2 + A}{2y}.$$

Fent els mateixos càlculs que en el cas anterior, tenim que $P_1 + P_2 = P_3 = (x_3, y_3)$, on

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1.$$

b) $y = 0$:
En aquest cas la recta tangent és vertical i el tercer punt d'interesecció és ∞. Per tant, $P_1 + P_2 = \infty$.

3. Algun dels punts P_1, P_2 és ∞. Sense pèrdua de generalitat suposem que $P_2 = \infty$:
La recta per P_1 i ∞ és una recta vertical. El tercer punt d'intersecció en aquest cas és la reflexió respecte l'eix x de P_1. Per trobar $P_3 = P_1 + P_2$ reflectim respecte l'eix x aquest tercer punt d'intersecció. Observem que tornem a P_1. Per tant, $P_1 + \infty = P_1$.

Observació 2.7. Si $P_1, P_2 \in E(\mathbb{Q})$, en tots els casos es té que $P_1 + P_2 \in E(\mathbb{Q})$. Per tant, la operació $+$ és tancada en $E(\mathbb{Q})$.

Observació 2.8. Dels resultats anteriors es dedueix que l'operacio $+$ també es podria haver definit de la següent manera: si $P, Q, R \in E(\mathbb{Q})$, aleshores $P + Q + R = \infty$ si i només si P, Q, R estan sobre la mateixa recta.

El següent teorema ens diu que el conjunt $E(\mathbb{Q})$ amb aquesta operació de suma de punts és un grup abelià amb element neutre ∞.

Teorema 2.9. *Sigui $E/\mathbb{Q}$ una corba el·líptica. L'operació $+$ definida sobre $E(\mathbb{Q})$ compleix les següents propietats:*

1. $P_1 + P_2 = P_2 + P_1$ per a tot $P_1, P_2 \in E(\mathbb{Q})$ (commutativa).

2. *Existeix un punt $\infty \in E(\mathbb{Q})$ tal que $P + \infty = P$ per a tot $P \in E(\mathbb{Q})$ (element neutre).*

3. *Per a tot $P \in E(\mathbb{Q})$ existeix $P' \in E(\mathbb{Q})$ tal que $P + P' = \infty$. Denotem el punt P' per $-P$ (existència d'invers).*

4. *$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ per a tot $P_1, P_2, P_3 \in E(\mathbb{Q})$ (associativa).*

Demostració.

1. Es dedueix per construcció, ja que la recta que passa per P_1 i P_2 és la mateixa que la recta que passa per P_2 i P_1.

2. Es dedueix del cas 3 de la discussió anterior.

3. Donat $P = (x, y) \in E(\mathbb{Q})$, per la discussió anterior es té que $P' = -P = (x, -y) \in E(\mathbb{Q})$ satisfá $P + P' = \infty$.

4. No donarem la demostració de l'associativitat, ja que és bastant llarga i no té gaire pes en la continuació del treball. Es pot trobar a [2], pp 20-32.

□

2.3 Endomorfismes d'una corba el·líptica

Estudiarem a continuació els morfismes entre corbes el·líptiques. Fem notar que tota la teoria estudiada en aquesta secció serà desenvolupada sobre un cos K qualsevol.

Definició 2.10. *Sigui E/K una corba el·líptica. Un endomorfisme de E és un morfisme de grups $\alpha : E(\overline{K}) \to E(\overline{K})$ que ve donat per funcions racionals, és a dir, α és un morfisme de grups i existeixen funcions racionals $R_1(x, y), R_2(x, y) \in \overline{K}[x, y]$ tals que*

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

per a tot $(x, y) \in E(\overline{K})$.

Presentem a continuació un endomorfisme d'una corba elíptica que utilitzarem més d'un cop durant el treball: l'endomorfisme de duplicació. El denotarem per [2].

Exemple 2.11. Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre K. Definim per a tot $P = (x, y) \in E(\overline{K})$ $[2](P) := 2P$. Es té que [2] és un morfisme de grups i que

$$[2](x, y) = (R_1(x, y), R_2(x, y)),$$

on, per les expressions de la suma de punts de E,

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

Per tant, com que [2] és un morfisme de grups que ve donat per funcions racionals, es té que [2] és un endomorfisme de E.

El següent objectiu és definir els conceptes de grau i separabilitat d'un endomorfisme α d'una corba el·líptica E. Per fer-ho, necessitem caracteritzar les funcions racionals $R_1(x,y)$ i $R_2(x,y)$: observem que com que E ve definida per $y^2 = x^3 + Ax + B$, donada una funció racional qualsevol $R(x,y)$ es té que per a tot $P = (x,y) \in E(\overline{K})$ podem substituir les potències parelles de y per la potència corresponent de $x^3 + Ax + B$ i les potències senars de y per un polinomi en x multiplicat per y. Per tant, podem suposar que

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

Multiplicant numerador i denominador per $p_3(x) - p_4(x)y$ i tornant a substituir y^2 per $x^3 + Ax + B$ obtenim

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{2.5}$$

Com que α és morfisme de grups, se satisfà que $\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y)$ per a tot $P = (x,y) \in E(\overline{K})$. Per tant, si $\alpha(x,y) = (R_1(x,y), R_2(x,y))$, tenim que

$$R_1(x,-y) = R_1(x,y), \quad R_2(x,-y) = -R_2(x,y).$$

Aleshores, si R_1 ve donat per una expressió com (2.5), s'obté $q_2(x) = 0$, i si R_2 ve donat per una expressió com (2.5), s'obté $q_1(x) = 0$. Per tant, podem expressar α com

$$\alpha(x,y) = (\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}), \tag{2.6}$$

on $p(x)$ és coprimer amb $q(x)$ i $s(x)$ és coprimer amb $t(x)$.

Les funcions racionals anteriors estan ben definides. En efecte, si $q(x_0) = 0$ per a algun punt $P = (x_0, y_0) \in E(\overline{K})$, assumim que $\alpha(P) = \infty$. Si $q(x_0) \neq 0$, mostrem a continuació que aleshores es té $t(x_0) \neq 0$ i, per tant, $s(x)/t(x)$ está ben definit: per l'equació de E tenim que

$$y^2\frac{s(x)^2}{t(x)^2} = \frac{p(x)^3}{q(x)^3} + A\frac{p(x)}{q(x)} + B.$$

Per tant,

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

Com que $p(x)$ i $q(x)$ no tenen cap factor en comú, es té que els polinomis $u(x) := p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3$ i $q(x)$ tampoc en tenen cap. Escrivim $(x^3 + Ax + B)s(x)^2q(x)^3 = u(x)t(x)^2$ i supossem que $t(x_0) = 0$. Com que $t(x)$ i $s(x)$ són coprimers, tenim que $s(x_0) \neq 0$. Del fet que x_0 és una arrel doble de $t(x)^2$ i que $x^3 + Ax + B$ no té arrels dobles es dedueix que $q(x_0) = 0$, com volíem veure.

Definició 2.12. *Sigui α un endomorfisme de la forma (2.6) d'una corba el·líptica E/K. S'anomena grau de α a*

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

Si $\alpha = 0$, definim $\deg(\alpha) := 0$.

Definició 2.13. *Sigui $\alpha \neq 0$ un endomorfisme de la forma (2.6) d'una corba el·líptica E/K. Es diu que α és un endomorfisme separable si $(p(x)/q(x))' \neq 0$.*

Tot seguit presentem un parell de resultats sobre endomorfismes d'una corba el·líptica E/K. El primer ens relaciona l'ordre del nucli d'un endomorfisme amb el seu grau, mentre que el segon ens diu que tot endomorfisme no trivial de E és exhaustiu.

Proposició 2.14. *Sigui $\alpha : E(\overline{K}) \to E(\overline{K})$ un endomorfisme no trivial d'una corba el·líptica E/K. Aleshores:*

(a) si α és separable, llavors $\deg(\alpha) = \#\ker(\alpha)$.

(b) si α no és separable, llavors $\deg(\alpha) > \#\ker(\alpha)$.

Demostració. [2], Proposició 2.21. □

Proposició 2.15. *Siguin E/K una corba el·líptica i $\alpha \neq 0$ un endomorfisme de E. Aleshores, $\alpha : E(\overline{K}) \to E(\overline{K})$ és exhaustiu.*

Demostració. [2], Teorema 2.22. □

Presentem a continuació dos endomorfismes de corbes el·líptiques destacats: l'endomorfisme $[n]$ i l'endomorfisme de Frobenius. El primer serà molt important per al proper capítol del treball, on estudiarem els punts de torsió d'una corba el·líptica. El segon és un endomorfisme fonamental per a l'estudi de les corbes el·líptiques definides sobre cossos finits. Tot i que en aquest treball estem principalment interessats en l'estudi de les corbes el·líptiques definides sobre $\mathbb{Q}$, necessitem presentar l'endomorfisme de Frobenius per la seva importància en la demostració del teorema de Hasse. El teorema de Hasse ens dóna una fita del nombre de punts d'una corba el·líptica definida sobre un cos finit. Aquesta fita l'utilitzarem per a demostrar que la funció L associada a una corba el·líptica convergeix en un semiplà concret del pla complex. Per a no allunyar-nos de l'objectiu d'estudi d'aquest treball, no aprofundirem en la demostració del teorema de Hasse. No obstant, es donaran referències on poder trobar-la.

Definició 2.16. *Sigui $E/\mathbb{Q}$ una corba el·líptica i sigui $n \geq 1$ un nombre enter. S'anomena endomorfisme $[n]$ a l'aplicació*

$$\begin{aligned}[n]\colon E(\overline{\mathbb{Q}}) &\to E(\overline{\mathbb{Q}}) \\ P &\mapsto nP.\end{aligned}$$

Proposició 2.17. *Sigui $E/\mathbb{Q}$ una corba el·líptica i sigui $n \geq 1$ un nombre enter. L'endomorfisme $[n]$ és un endomorfisme de corbes el·líptiques separable de grau n^2.*

Demostració. Per demostrar aquest resultat s'han de fer servir els polinomis de n-divisió, que són uns polinomis associats a E definits recursivament. La prova es pot trobar a [2], pp 80-85. □

Corol·lari 2.18. $\#Ker([n]) = n^2$.

Demostració. Es dedueix de les proposicions 2.14 i 2.17. □

Definició 2.19. *Sigui $\mathbb{F}_q$ un cos finit i sigui $E/\mathbb{F}_q$ una corba el·líptica. S'anomena endomorfisme de Frobenius a l'aplicació*

$$\begin{aligned}\phi_q\colon E(\overline{\mathbb{F}}_q) &\to E(\overline{\mathbb{F}}_q) \\ (x, y) &\mapsto (x^q, y^q) \\ \infty &\mapsto \infty.\end{aligned}$$

Proposició 2.20. *Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre $\mathbb{F}_q$. Aleshores,*

1. *$\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$ per a tot $(x, y) \in E(\overline{\mathbb{F}}_q)$.*

2. *ϕ_q és un endomorfisme no separable de E de grau q.*

Demostració. Sigui $(x, y) \in E(\overline{\mathbb{F}}_q)$. Per a provar (1) recordem que per a tot $a, b \in \mathbb{F}_q$ se satisfà $(a + b)^q = a^q + b^q$ i $a^q = a$. Elevant a q l'equació que defineix E i utilitzant les igualtats anteriors tenim que

$$(y^q)^2 = (x^q)^3 + A^q x^q + B^q = (x^q)^3 + Ax^q + B.$$

Per tant, $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$. Es demostra així (1).
Com que $\phi_q(x, y) = (x^q, y^q)$, l'aplicació ϕ_q ve donada per funcions racionals (polinomis). Clarament, $\deg(\phi_q) = q$. Per veure que ϕ_q és un endomorfisme de E falta comprovar que $\phi_q(x_1, y_1) + \phi_q(x_2, y_2) = \phi_q((x_1, y_1) + (x_2, y_2))$ per a tot $(x_1, y_1), (x_2, y_2) \in E(\overline{\mathbb{F}}_q)$. Sigui $(x_3, y_3) := (x_1, y_1) + (x_2, y_2)$. Suposem que $x_1 \neq x_2$. Per les fórmules de la suma de punts es té

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{on } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Elevant totes les igualtats anteriors a q obtenim

$$x_3^q = (m')^2 - x_1^q - x_2^q, \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \quad \text{on } m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}.$$

Per tant,

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

Els altres casos es fan de manera anàloga utilitzant també les dues igualtats esmentades a l'inici de la demostració. Finalment, com que $q = 0$ a $\mathbb{F}_q$, la derivada de x^q és 0. Per tant, ϕ_q no és separable. □

Finalitzem aquesta secció enunciant el Teorema de Hasse.

Teorema 2.21. *(Hasse)*
Sigui $E/\mathbb{F}_q$ una corba el·líptica. Aleshores, l'ordre de $E(\mathbb{F}_q)$ satisfà

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Demostració. Veure [2], Teorema 4.2 o [3], Capítol 5, Teorema 1.1. □

2.4 L'invariant j

Sempre que s'estudia un objecte nou en matemàtiques és molt natural preguntar-se si, quan es consideren dos o més d'aquests objectes, és possible relacionar-los d'alguna manera, en el sentit que estudiant només un d'ells podem entendre l'estructura i les propietats de tots els altres relacionats amb aquest. Els invariants ens ajuden en tot això. En aquesta secció, on continuarem treballant sobre un cos K qualsevol, presentem l'invariant j d'una corba el·líptica E/K i veurem que dues corbes el·líptiques són isomorfes si i només si tenen el mateix invariant j.

Sigui K un cos i sigui $\mu \in \overline{K}^\times$. Considerem les dues corbes el·líptiques següents definides sobre K

$$E : y^2 = x^3 + Ax + B, \quad E' : y^2 = x^3 + A'x + B', \quad \text{on } A' = \mu^4 A, B' = \mu^6 B. \tag{2.7}$$

Observem que

$$\Delta_{E'} = -4A'^3 - 27B'^2 = -4\mu^{12}A^3 - 27\mu^{12}B^2 = \mu^{12}(-4A^3 - 27B^2) = \mu^{12}\Delta_E.$$

Per tant, E és una corba el·líptica si i només si E' és una corba el·líptica. El següent resultat motivarà la definició de corbes el·líptiques isomorfes.

Teorema 2.22. *Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre K. Sigui $\mu \in \overline{K}^\times$ i sigui E' la corba el·líptica definida a (2.7). Aleshores, l'aplicació*

$$\begin{aligned} \psi \colon E(\overline{K}) &\to E'(\overline{K}) \\ (x, y) &\mapsto (\mu^2 x, \mu^3 y) \end{aligned}$$

és un isomorfisme de grups.

Demostració. Observem primer que $(x, y) \in E(\overline{K}) \Leftrightarrow (\mu^2 x, \mu^3 y) \in E'(\overline{K})$ i que ψ té inversa $\psi^{-1} : E'(\overline{K}) \Rightarrow E(\overline{K}), (x, y) \mapsto (\mu^{-2}x, \mu^{-3}y)$. Observem també que per a tot $P = (x, y) \in E(\overline{K})$, $\psi(-P) = -\psi(P)$. Només ens falta veure que ψ és un morfisme de grups. Per veure això, és suficient comprovar que per a tot $P, Q, R \in E(\overline{K})$ se satisfà $P + Q + R = \infty \Rightarrow \psi(P) + \psi(Q) + \psi(R) = \infty$. En efecte, si posem $R := P + Q$, aleshores $P + Q - R = \infty$.
Per tant $\psi(P) + \psi(Q) + \psi(-R) = \psi(P) + \psi(Q) - \psi(R) = \infty \Rightarrow \psi(P) + \psi(Q) = \psi(R) = \psi(P + Q)$.
L'aplicació ψ en coordenades projectives (homogeneïtzem) ve donada per

$$\begin{aligned} \psi \colon E(\overline{K}) &\to E'(\overline{K}) \\ [X : Y : Z] &\mapsto [\mu^2 X : \mu^3 Y : Z]. \end{aligned}$$

Observem que $\psi(\infty) = \psi([0 : 1 : 0]) = [0 : \mu^3 : 0] = [0 : 1 : 0] = \infty$. Com que $P+Q+R = \infty$, P, Q i R estan sobre una mateixa recta. Sigui $L : aX+bY+cZ = 0$ la recta que talla E en els punts P, Q i R. Els punts de L són de la forma $[cX : bY : -aX - bY]$. La imatge per ψ d'aquests punts és $[c\mu^2 X : c\mu^3 Y : -aX - bY]$. Com que

$$\begin{aligned} &\{[c\mu^2 X : c\mu^3 Y : -aX - bY] \in \mathbb{P}^2_K : [X : Y] \in \mathbb{P}^1_K,\ a, b, c \in K\} \\ &= \{[X : Y : Z] \in \mathbb{P}^2_K : a/\mu^2 X + b/\mu^3 Y + cZ = 0,\ a, b, c \in K\}, \end{aligned}$$

tenim que la imatge de la recta L per ψ és la recta $L' : a'X + b'Y + c'Z$, on $a' = a/\mu^2, b' = b/\mu^3$ i $c' = c$. L' interseca E en tres punts (comptats amb multiplicitat). Aquests tres punts han de ser necessàriament $\psi(P), \psi(Q)$ i $\psi(R)$. Com que els tres punts anteriors estan sobre la mateixa recta, obtenim $\psi(P) + \psi(Q) + \psi(R) = \infty$, com volíem veure. □

Definició 2.23. *Siguin $E : y^2 = x^3 + Ax + B$, $E' : y^2 = x^3 + A'x + B'$ dues corbes el·líptiques definides sobre K. Es diu que E i E' són isomorfes si existeix $\mu \in \overline{K}^\times$ tal que $A' = \mu^4 A$, $B' = \mu^6 B$. Si $\mu \in K^\times$, diem que E i E' són isomorfes sobre K.*

Exemple 2.24.

(a) Les corbes el·líptiques

$$E_1 : y^2 = x^3 + x + 1, \quad E_2 : y^2 = x^3 + 16x + 64$$

són isomorfes sobre $\mathbb{Q}$ ($\mu = 2$).

(b) Les corbes el·líptiques

$$E_3 : y^2 = x^3 - 25x, \quad E_4 : y^2 = x^3 - 4x$$

no són isomorfes sobre $\mathbb{Q}$, però són isomorfes sobre $\mathbb{Q}(\sqrt{10})$ ($\mu = \sqrt{10}/2$).

Definim finalment l'invariant j d'una corba el·líptica i veiem que dues corbes el·líptiques són isomorfes si i només si els seus invariants j són iguals.

Definició 2.25. *Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre K. Es defineix l'invariant j de E com*

$$j(E) := -1728\frac{4A^3}{\Delta_E}.$$

Teorema 2.26. *Siguin $E : y^2 = x^3 + Ax + B$, $E' : y^2 = x^3 + A'x + B'$ dues corbes el·líptiques definides sobre K. Aleshores, E és isomorfa a E' si i només si $j(E) = j(E')$.*

Demostració. Suposem primer que E i E' són isomorfes. Per tant, existeix $\mu \in \overline{K}^\times$ tal que $A' = \mu^4 A, B' = \mu^6 B$. Hem vist a l'inici d'aquesta secció que, en aquest cas, $\Delta_{E'} = \mu^{12}\Delta_E$. Per tant,

$$j(E') = -1728\frac{4A'^3}{\Delta_{E'}} = -1728\frac{4(\mu^4 A)^3}{\mu^{12}\Delta_E} = -1728\frac{4A^3}{\Delta_E} = j(E).$$

Recíprocament, suposem que $j(E) = j(E') := j$. Distingim casos:

1. $j \neq 0, 1728$.
   Tenim
   $$j - 1728 = -1728\frac{4A^3}{\Delta_E} - 1728 = -1728\frac{4A^3 + \Delta_E}{\Delta_E} = 1728\frac{27B^2}{\Delta_E}.$$
   Per tant,
   $$\frac{j}{j - 1728} = -\frac{4A^3}{27B^2}.$$
   Com que $j(E) = j(E') = j$, obtenim
   $$\frac{4A^3}{27B^2} = \frac{4A'^3}{27B'^2} \Leftrightarrow \left(\frac{A}{A'}\right)^3 = \left(\frac{B}{B'}\right)^2. \tag{2.8}$$
   Sigui $\mu \in \overline{K}^\times$ una solució de l'equació
   $$\mu^2 = \frac{A}{A'}\frac{B'}{B}.$$

De (2.8) obtenim

$$\mu^4 = \left(\frac{A}{A'}\right)^2 \left(\frac{B'}{B}\right)^2 = \left(\frac{A}{A'}\right)^2 \left(\frac{A'}{A}\right)^3 = \frac{A'}{A} \Rightarrow A' = \mu^4 A.$$

Anàlogament,

$$\mu^6 = \left(\frac{A}{A'}\right)^3 \left(\frac{B'}{B}\right)^3 = \left(\frac{B}{B'}\right)^2 \left(\frac{B'}{B}\right)^3 = \frac{B'}{B} \Rightarrow B' = \mu^6 B.$$

Per tant, E i E' són isomorfes.

2. $j = 0$.
Com que $j = 0$, tenim que $A = A' = 0$. Per tant, $B, B' \neq 0$. Escollim en aquest cas $\mu \in \overline{K}^\times$ tal que $\mu^6 B = B'$.

3. $j = 1728$.
Com que $j = 1728$, tenim que $B = B' = 0$. Per tant, $A, A' \neq 0$. Escollim en aquest cas $\mu \in \overline{K}^\times$ tal que $\mu^4 A = A'$

□

Exemple 2.27. Tornem a les corbes el·líptiques de l'exemple 2.24.

(a) $j(E_1) = j(E_2) = 6912/31$. Per tant, E_1 i E_2 són isomorfes.

(b) $j(E_3) = j(E_4) = 1728$. Per tant, E_3 i E_4 són isomorfes.

3 Punts de torsió

En aquest capítol estudiarem els punts de torsió d'una corba el·líptica $E/\mathbb{Q}$, és a dir, els punts de $E(\mathbb{Q})$ d'ordre finit. Veurem que es coneixen molts resultats sobre aquests punts. Un dels més importants és que el subgrup de torsió d'una corba el·líptica $E/\mathbb{Q}$, és a dir, el subgrup de $E(\mathbb{Q})$ format per tots els punts d'ordre finit, és finit. Aquest resultat l'obtindrem com a conseqüència directa del teorema de Lutz-Nagell.

3.1 Subgrup de n-torsió i subgrup de torsió

Definició 3.1. *Sigui $E/\mathbb{Q}$ una corba el·líptica i sigui $n \geq 1$ un nombre enter. Es defineix el subgrup de n-torsió com*

$$E[n] := Ker([n]) = \{P \in E(\overline{\mathbb{Q}}) : nP = \infty\}.$$

Pel corol·lari 2.18, tenim que $\#E[n] = n^2$..

Exemple 3.2. Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica. Calcularem a continuació el subgrup de 2-torsió $E[2]$.
Podem escriure l'equació que defineix E com

$$y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

amb $\alpha_1, \alpha_2, \alpha_3 \in \overline{\mathbb{Q}}$. Observem que un punt $P = (x, y) \in E(\overline{\mathbb{Q}})$ satisfà $2P = \infty$ si i només si $P = -P$. Això és equivalent a que $(x, y) = (x, -y)$. Obtenim, doncs, $y = 0$. Per tant,

$$E[2] = \{\infty, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\}.$$

Com que tots els punts de $E[2]$ tenen ordre 2, es té que $E[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Per a qualsevol extensió $\mathbb{Q} \subseteq K \subset \overline{\mathbb{Q}}$ escriurem $E(K)[n]$ per indicar els punts de $E[n]$ amb coordenades a K.

Exemple 3.3. Sigui $E : y^2 = x(x^2 + 1)$. Es té que

$$E(\mathbb{Q})[2] = \{\infty, (0, 0)\}, \quad E(\mathbb{Q}(i))[2] = \{\infty, (0, 0), (i, 0), (-i, 0)\}.$$

Observació 3.4. Si en comptes de permetre que $E[n]$ contingui punts de E amb coordenades a $\overline{\mathbb{Q}}$, permetéssim que només contingués punts amb coordenades a $\mathbb{R}$, obtindríem que, o bé $E[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, o bé $E[2] \cong \mathbb{Z}/2\mathbb{Z}$, depenent de si $f(x) := x^3 + Ax + B$ té tres o una arrel real respectivament (veure figura 3). Si, a més, només permetéssim punts amb coordenades a $\mathbb{Q}$, tindríem que, o bé $E[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, o bé $E[2] \cong \mathbb{Z}/2\mathbb{Z}$, o bé $E[2] = \{\infty\}$, depenent de si $f(x)$ té tres, una o cap arrel racional respectivament.

El següent teorema ens generalitza el resultat obtingut a l'exemple 3.2.

Teorema 3.5. *Sigui $E/\mathbb{Q}$ una corba el·líptica i sigui $n \geq 1$ un nombre enter. Aleshores*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

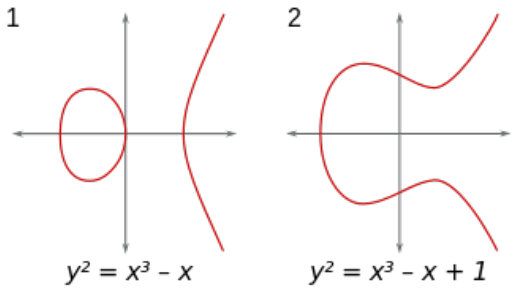

Figura 3: Dues corbes el·líptiques sobre $\mathbb{R}$. La primera té 3 punts de 2-torsió amb coordenades reals. La segona només en té un.

Demostració. Pel Teorema d'estructura dels grups abelians finitament generats,

$$E[n] \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z},$$

amb n_i enters positius i $n_i|n_{i+1}$ per a tot $1 \leq i \leq k$. Sigui p un primer que divideix n_1. Aleshores $p|n_i$ per a tot i. Per tant, $E[p] \subseteq E[n]$ té ordre p^k. Ara bé, com que $\#E[p] = p^2$, obtenim que $k = 2$. Com que l'endomorfisme $[n]$ anul·la $E[n] \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$, tenim que $n_2|n$. Finalment, com que $n^2 = \#E[n] = n_1n_2$, s'obté que $n_1 = n_2 = n$. □

Definició 3.6. *Sigui $E/\mathbb{Q}$ una corba el·lptíca. Es defineix el subgrup de torsió de E sobre $\overline{\mathbb{Q}}$ com*

$$E_{\text{tors}} := \bigcup_{n \geq 1} E[n].$$

E_{tors} és el subgrup de $E(\overline{\mathbb{Q}})$ que conté tots els punts d'ordre finit.

Definició 3.7. *Sigui $E/\mathbb{Q}$ una corba el·líptica. Es defineix el subgrup de torsió de E com*

$$E(\mathbb{Q})_{\text{tors}} := E(\mathbb{Q}) \cap E_{\text{tors}}.$$

En el que queda de capítol ens centrarem en estudiar $E(\mathbb{Q})_{\text{tors}}$, és a dir, els punts de $E(\mathbb{Q})$ d'ordre finit. Veurem que, com a conseqüència del Teorema de Lutz-Nagell, $E(\mathbb{Q})_{\text{tors}}$ és finit.

3.2 Teorema de Lutz-Nagell

En aquesta secció enunciarem i demostrarem el Teorema de Lutz-Nagell. Aquest teorema proporciona un mètode per calcular els punts de torsió d'una corba el·llíptica de manera fàcil.

Comencem observant que sempre que tenim una corba el·líptica E definida sobre $\mathbb{Q}$ podem trobar una altra corba el·líptica E' isomorfa a E, però definida sobre $\mathbb{Z}$. En efecte, si $E : y^2 = x^3 + Ax + B$, sigui D el màxim comú denominador de A i B. Aleshores, multipliquem l'equació de E per D^6 i apliquem el canvi de variable $(D^2x, D^3y) \mapsto (x, y)$. Posant $A' := AD^4$ i $B' := B^6B$, obtenim una corba $E' : y^2 = x^3 + A'x + B'$, amb $A', B' \in \mathbb{Z}$, isomorfa a E.

Per tant, sempre que tinguem una corba el·líptica $E/\mathbb{Q}$ la podrem considerar definida sobre $\mathbb{Z}$ en el sentit explicat abans. Enunciem a continuació el Teorema de Lutz-Nagell.

Teorema 3.8. *(Lutz-Nagell)*
Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica amb $A, B \in \mathbb{Z}$. Sigui $P = (x, y) \in E(\mathbb{Q})$ un punt d'ordre finit. Aleshores

1. $x, y \in \mathbb{Z}$.

2. *O bé* $y = 0$ *o bé* $y^2 | \Delta_E$.

Per demostrar aquest teorema necessitem una sèrie de resultats que presentarem a continuació. Suposarem sempre que tenim corbes el·líptiques $E : y^2 = x^3 + Ax + B$ amb $A, B \in \mathbb{Z}$.

Sigui p un nombre primer i sigui $x \in \mathbb{Q}^\times$. Podem escriure

$$x = p^r \frac{a}{b},$$

amb $a, b \in \mathbb{Z}$, $(a, b) = 1$ i $p \nmid ab$. Definim $v_p(x) := r$.

Definició 3.9. *Sigui p un nombre primer. L'aplicació*

$$\begin{aligned} v_p \colon \mathbb{Q} &\to \mathbb{Z} \cup \{\infty\} \\ x &\mapsto v_p(x) \\ 0 &\mapsto \infty \end{aligned}$$

s'anomena valoració p-àdica.

Lema 3.10. *Siguin $x, y \in \mathbb{Q}^\times$. Aleshores $v_p(xy) = v_p(x) + v_p(y)$.*

Demostració. Siguin

$$x = p^r \frac{a}{b}, \quad y = p^s \frac{c}{d},$$

amb $a, b, c, d \in \mathbb{Z}$, $p \nmid ab, p \nmid cd$. Aleshores,

$$xy = p^{r+s} \frac{ac}{bd},$$

amb $p \nmid abcd$. Per tant $v_p(xy) = r + s = v_p(x) + v_p(y)$. □

Definició 3.11. *Sigui p un nombre primer i sigui $x \in \mathbb{Q}$. S'anomena norma p-àdica (o valor absolut p-àdic) de x a*

$$\|x\|_p := p^{-v_p(x)}.$$

Si $x = 0$, posem $\|x\| = 0$.

Recordem que el cos dels nombres p-àdics $\mathbb{Q}_p$ és la compleció de $\mathbb{Q}$ respecte de la norma p-àdica $\| \cdot \|_p$.

Observació 3.12. Sigui $x \in \mathbb{Q}^\times$. Observem que

a) $v_p(x) > 0 \Leftrightarrow p$ divideix el numerador de x.

b) $v_p(x) = 0 \Leftrightarrow p$ no divideix ni el numerador ni el denominador de x.

c) $v_p(x) < 0 \Leftrightarrow p$ divideix el denominador de x.

Proposició 3.13. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Sigui p un nombre primer i sigui $P = (x, y) \in E(\mathbb{Q})$. Aleshores $v_p(x) < 0$ si i només si $v_p(y) < 0$. En aquest cas, existeix un enter positiu r tal que $v_p(x) = -2r$ i $v_p(y) = -3r$.*

Demostració. Suposem que p divideix el denominador de x, és a dir, $v_p(x) = -k$, amb k enter positiu. Per tant,

$$x = p^{-k}\frac{a}{b},$$

amb $a, b \in \mathbb{Z}$, $(a, b) = 1$ i $p \nmid ab$. Tenim

$$x^3 + Ax + B = p^{-3k}\frac{a^3}{b^3} + p^{-k}A\frac{a}{b} + B = \frac{a^3 + p^{2k}Aab^2 + p^{3k}Bb^3}{p^{3k}b^3}.$$

Com que $k > 0$ i $p \nmid a$, aleshores $p \nmid a^3+p^{2k}Aab^2+p^{3k}Bb^3$. Per tant, $v_p(x^3+Ax+B) = -3k$. Ara bé, $2v_p(y) = v_p(y^2) = v_p(x^3 + Ax + B) = -3k$. Per tant, $v_p(y) < 0$. A més, com que $2|k$, es té que $k = 2r$, amb r enter positiu. Per tant,

$$v_p(x) = -2r, \quad v_p(y) = \frac{-3k}{2} = -3r.$$

Finalment, si $v_p(x) \geq 0$, com que $A, B \in \mathbb{Z}$, es té que

$$2v_p(y) = v_p(y^2) = v_p(x^3 + Ax + B) \geq 0.$$

Per tant, $v_p(y) \geq 0$. □

La proposició anterior ens diu que si p divideix el denominador de x o y, aleshores p també divideix el denominador de l'altre, i, en aquest cas, la potència exacta de p que divideix el denominador de x és p^{2r} i la que divideix el denominador de y és p^{3r}, per a algun enter positiu r. Això motiva la següent definició.

Definició 3.14. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Sigui p un nombre primer. Per a cada nombre enter $r \geq 1$ definim*

$$E_r := \{(x, y) \in E(\mathbb{Q}) : v_p(x) \leq -2r,\ v_p(y) \leq -3r\} \cup \{\infty\}.$$

E_r és el conjunt de punts racionals $(x, y) \in E(\mathbb{Q})$ tals que p^{2r} divideix el denominador de x i p^{3r} divideix el denominador de y. Observem que, per la proposició anterior, $P = (x, y) \in E_r$ si i només si p^{2r} divideix el denominador de x, i que

$$E(\mathbb{Q}) \supset E_1 \supset E_2 \supset \cdots .$$

Recordem que al Teorema de Lutz-Nagell volem demostrar que si $P = (x, y) \in E(\mathbb{Q})$ és un punt d'ordre finit, aleshores $x, y \in \mathbb{Z}$. L'estratègia serà veure que per a tot primer p, els denominadors de x i de y no són divisibles per p, és a dir, veurem que un punt d'ordre finit de E no pot pertànyer a E_1 per a tot primer p. Provarem primer que E_r és subgrup de $E(\mathbb{Q})$ per a tot enter $r \geq 1$.

Observem que si $P = (x, y) \in E_r$, aleshores $y \neq 0$. Per tant, el canvi de coordenades

$$t = \frac{x}{y}, \quad s = \frac{1}{y}$$

està ben definit. L'equació de E es transforma sota aquest canvi en

$$E' : s = t^3 + Ats^2 + Bs^3$$

en el pla (t, s).

Si $P = (x, y) \in E(\mathbb{Q})$, denotarem la imatge de P sota aquest canvi de coordenades per

$$P' := \left(\frac{x}{y}, \frac{1}{y}\right) = (t, s) \in E'(\mathbb{Q}).$$

Fem notar que en el pla (t, s) tenim tots els punts del pla (x, y) excepte els punts amb $y = 0$. Observem també que ara l'element neutre ∞ és el punt $(0, 0)$ del pla (t, s). A més, una recta $y = mx+n$ al pla (x, y) és una recta al pla $(t.s)$. En efecte, dividint $y = mx+n$ entre ny, tenim

$$\frac{1}{n} = \frac{m}{n}\frac{x}{y} + \frac{1}{y} \quad \Rightarrow \quad s = -\frac{m}{n}t + \frac{1}{n}.$$

Per tant, podem sumar punts de $E'(\mathbb{Q})$ al pla (t, s) de la mateixa manera que al pla (x, y), però utilitzant ara el punt $(0, 0)$ com a element neutre. En aquest cas, per exemple, si $P' = (t, s) \in E'(\mathbb{Q})$, es té que $-P' = (-t, -s)$.

Estudiem ara la divisibilitat de les noves coordenades t i s per potències d'un nombre primer p. Sigui $P = (x, y) \in E_r$. Aleshores

$$x = \frac{a}{bp^{2(r+i)}}, \quad y = \frac{c}{dp^{3(r+i)}},$$

amb $i \geq 0$. Per tant,

$$t = \frac{x}{y} = \frac{ad}{bc}p^{r+i}, \quad s = \frac{1}{y} = \frac{d}{c}p^{3(r+i)}.$$

Per tant, $P' = (t, s) \in E_r$ si i només si p^r divideix el numerador de t i p^{3r} divideix el numerador de s, és a dir, tenim la següent bijecció

$$E_r \ \leftrightarrow \ E'_r := \{P' \in E'(\mathbb{Q}) : v_p(t) \geq r, \ v_p(s) \geq 3r\}.$$

Per la bijecció anterior, si provem que E'_r és subgrup de $E'(\mathbb{Q})$, tindrem que E_r és subgrup de $E(\mathbb{Q})$ per a tot $r \geq 1$.

Per veure que E'_r és subgrup de $E(\mathbb{Q})$ hem de veure que si una potència de p divideix la coordenada t de P'_1 i P'_2, amb $P'_1, P'_2 \in E'_r$, aleshores la mateixa potència de p divideix la coordenada t de $P'_1 + P'_2$, i que si una potència de p divideix la coordenada t de $P' \in E'_r$, aleshores la mateixa potència de p divideix la coordenada t de $-P'$. Això últim és fàcil de veure ja que si $P' = (t, s) \in E'_r$, aleshores $v_p(t) \geq r$ i, com que $-P' = (-t, -s)$, s'obté que $v_p(-t) \geq r$. Per tant, $-P \in E'_r$.
Veiem ara que si $P'_1 = (t_1, s_1), P'_2 = (t_2, s_2) \in E'_r$, aleshores $P'_1 + P'_2 \in E'_r$. Distingim casos:

1. $t_1 = t_2$.
   En aquest cas, la recta vertical $t = t_1$ talla E' en P'_1, P'_2 i un tercer punt $P'_3 = (t_1, s_3)$ (P'_3 pot tornar a ser P'_1 o P'_2). Aleshores, $P'_1 + P'_2 = (-t_1, s_3)$. Com que $v_p(t_1) \geq r$, obtenim que $P'_1 + P'_2 \in E'_r$.

2. $t_1 \neq t_2$.
   Considerem la recta $s = \alpha t + \beta$ que passa per P'_1 i P'_2. El pendent α de la recta ve donat per

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1}.$$

Com que (t_1, s_1) i (t_2, s_2) satisfan

$$s_1 = t_1^3 + At_1s_1^2 + Bs_1^3$$
$$s_2 = t_2^3 + At_2s_2^2 + Bs_2^3,$$

es té que

$$\begin{aligned} s_2 - s_1 &= (t_2^3 - t_1^3) + A(t_2s_2^2 - t_1s_1^2) + B(s_2^3 - s_1^3) \\ &= (t_2 - t_1)(t_1^2 + t_1t_2 + t_2^2) + As_2^2(t_2 - t_1) + At_1(s_2 - s_1)(s_2 + s_1) \\ &+ B(s_2 - s_1)(s_1^2 + s_1s_2 + s_2^2). \end{aligned}$$

Per tant,

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_1^2 + t_1t_2 + t_2^2 + As_2^2}{1 - At_1(s_2 + s_1) - B(s_1^2 + s_1s_2 + s_2^2)}. \tag{3.1}$$

Observem que si $P_1' = P_2'$, aleshores, derivant implícitament, el pendent de la recta tangent a E' per P_1 és

$$\alpha = \frac{ds}{dt}(P_1') = \frac{3t_1^2 + As_1^2}{1 - 2At_1s_1 - 3Bs_1^2},$$

que coincideix amb l'expressió (3.1) fent $t_1 = t_2$ i $s_1 = s_2$. Per tant, utilitzarem l'expressió de (3.1) en tots els casos.
Sigui $P_3' = (t_3, s_3)$ el tercer punt d'intersecció de la recta $s = \alpha t + \beta$ amb E'. Per trobar t_3 resolem

$$\begin{aligned} \alpha t + \beta &= t^3 + At(\alpha t + \beta)^2 + B(\alpha t + \beta)^3 \\ &= t^3 + A\alpha^2t^3 + 2A\alpha\beta t^2 + A\beta^2t + B\alpha^3t^3 + 3B\alpha^2t^2\beta + 3B\alpha t\beta^2 + B\beta^3 \end{aligned}$$

Per tant,

$$0 = (1 + A\alpha^2 + B\alpha^3)t^3 + (2A\alpha\beta + 3B\alpha^2\beta)t^2 + (A\beta^2 + 3B\alpha\beta^2 - \alpha)t + B\beta^3 - \beta.$$

Les soluciones de l'equació anterior són t_1, t_2, t_3. Per tant,

$$t_1 + t_2 + t_3 = -\frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + A\alpha^2 + B\alpha^3}.$$

Obtenim d'aquesta manera una expressió per a $t_1 + t_2 + t_3$ en funció de α i de β. Observem que, com que $v_p(t_1), v_p(t_2) \geq r$ i $v_p(s_1), v_p(s_2) \geq 3r$, de l'expressió de α s'obté que

$$v_p(\alpha) \geq 2r.$$

A més, com que $\beta = s_1 - \alpha t_1$, tenim que

$$v_p(\beta) \geq 3r.$$

Per tant,

$$v_p(t_1 + t_2 + t_3) \geq 5r. \tag{3.2}$$

Observem que l'expressió anterior és equivalent a $t_1 + t_2 + t_3 \equiv 0 \pmod{p^{5r}}$.
Finalment, com que $v_p(t_1), v_p(t_2) \geq r$, de (3.2) es dedueix que $v_p(t_3) \geq r$. Per tant, $v_p(-t_3) \geq r$. S'obté així que $P_1' + P_2' \in E_r'$.

El procediment anterior, juntament amb la bijecció entre E_r i E'_r, demostra el següent resultat.

Proposició 3.15. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Sigui p un nombre primer. Aleshores, per a tot nombre enter $r \geq 1$, E_r és un subgrup de $E(\mathbb{Q})$.*

Observació 3.16. Si denotem per $t(P)$ la coordenada t del punt $P \in E_r$ (és a dir, si $P = (x, y) \in E_r$, $t(P) = x/y$), de l'expressió (3.2) obtenim que, per a tot $P_1, P_2 \in E_r$,

$$t(P_1) + t(P_2) \equiv t(P_1 + P_2) \pmod{p^{4r}}.$$

Proposició 3.17. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Sigui p un nombre primer. Aleshores, per a tot nombre enter $r \geq$, l'aplicació*

$$\begin{aligned} \lambda_r \colon \frac{E_r}{E_{5r}} &\to \mathbb{Z}/p^{4r}\mathbb{Z} \\ P = (x, y) &\mapsto p^{-r}t(P) = p^{-r}\frac{x}{y} \\ \infty &\mapsto 0 \end{aligned}$$

és un morfisme de grups injectiu.

Demostració. Observem primer que, com que

$$v_p\left(p^{-r}\frac{x}{y}\right) = v_p\left(p^{-r}\right) + v_p\left(\frac{x}{y}\right) = v_p\left(p^{-r}\right) + v_p(t) \geq -r + r \geq 0,$$

l'aplicació λ_r està ben definida.
Siguin $P_1, P_2 \in E_r$. Tenim que $\lambda_r(P_1) + \lambda_r(P_2) = p^{-r}t(P_1) + p^{-r}t(P_2) \pmod{p^{4r}} \equiv p^{-r}(t(P_1) + t(P_2)) \pmod{p^{4r}} \equiv p^{-r}t(P_1 + P_2) \pmod{p^{4r}} = \lambda_r(P_1 + P_2)$. Per tant, λ_r és un morfisme de grups.
Sigui ara $P = (x, y) \in E_r$ i suposem que $\lambda_r(P) = 0 \in \mathbb{Z}/p^{4r}\mathbb{Z}$. Per tant, $v_p\left(p^{-r}\frac{x}{y}\right) = -r + v_p(t(P)) \geq 4r$. Obtenim, doncs, que $v_p(t(P)) \geq 5r$, és a dir, $P \in E_{5r}$. Per tant, λ_r és injectiu. □

El següent resultat és clau per a la demostració del Teorema de Lutz-Nagell.

Proposició 3.18. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Per a tot primer p, l'únic punt d'ordre finit de E_1 és ∞.*

Demostració. Sigui $P = (x, y) \in E_1$ un punt d'ordre n amb $n \geq 2$. Sigui p un nombre primer i suposem que $P \in E_1$. El punt P pot pertànyer a un $E_r \subset E_1$, però no pot pertànyer a infinits E_r perquè el denominador de x no pot ser divisible per potències arbitràries de p. Per tant, existeix un enter positiu $r \geq 1$ tal que $P \in E_r$ i $P \notin E_{r+1}$. Tenim, doncs, que $v_p(t(P)) = r$. Distingim casos:

1. Suposem que $p \nmid n$.
   Com que per a tot $P_1, P_2 \in E_r$ tenim que $t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{5r}}$, s'obté que $t(nP) \equiv nt(P) \pmod{p^{5r}}$. Ara bé, com que $nP = \infty$, s'obté

$$\begin{aligned} t(nP) = t(\infty) = 0 \quad &\Rightarrow \quad 0 \equiv nt(P) = np^r\lambda_r(P) \pmod{p^{5r}} \quad \Rightarrow \\ \Rightarrow \quad 0 \equiv n\lambda_r(P) \pmod{p^{4r}} \quad &\Rightarrow \quad 0 \equiv \lambda_r(P) \pmod{p^{4r}} \quad \Rightarrow \quad P \in E_{5r}, \end{aligned}$$

on en la penúltima implicació hem utilitzat que $p \nmid n$ i en l'última hem fet ús de la injectivitat de λ_r. Com que $P \in E_{5r}$, tenim que $v_p(t(P)) \geq 5r$, que contradiu $v_p(t(P)) = r$.

2. Suposem que $p|n$.
El punt $Q = (n/p)P$ té ordre p i pertany a E_1 per ser E_1 subgrup de $E(\mathbb{Q})$. Argumentant igual que a l'inici de la demostració, existeix un enter positiu $r' \geq 1$ tal que $Q \in E'_r$ i $Q \notin E_{r'+1}$. Per tant, $v_p(t(Q)) = r'$. Tenim ara

$$0 = t(\infty) = t(pQ) \equiv pt(Q) \pmod{p^{5r'}} \quad \Rightarrow \quad v_p(pt(Q)) \geq 5r'.$$

Ara bé, $v_p(pt(Q)) = v_p(p) + v_p(t(Q)) = 1 + r'$. Com que $r \geq 1$, tenim una contradicció.

□

Demostrem finalment el Teorema de Lutz-Nagell. Recordem l'enunciat.

Teorema 3.19. *(Lutz-Nagell)*
Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica amb $A, B \in \mathbb{Z}$. Sigui $P = (x, y) \in E(\mathbb{Q})$ un punt d'ordre finit. Aleshores

1. $x, y \in \mathbb{Z}$.

2. *O bé* $y = 0$ *o bé* $y^2 | \Delta_E$.

Demostració. Si $P = (x, y) \in E(\mathbb{Q})$ té ordre finit, per la proposició anterior tenim que per a tot primer p, $P \notin E_1$, és a dir, els denominadors de x i de y no són divisibles per cap primer p. Per tant, $x, y \in \mathbb{Z}$. Això prova (1).
Si P és un punt de 2-torsió, aleshores $y = 0$. Suposem, doncs, que P té ordre $n \geq 3$. Com que $2P$ també té ordre finit, les seves coordenades seran nombres enters. Ara bé, per les fórmules de l'endomorfisme de duplicació [2], la coordenada x de $2P$ és

$$\frac{9x^4 + 6Ax^2 + A^2 - 8xy^2}{4y^2} = \frac{9x^4 + 6Ax^2 + A^2 - 8x(x^3 + Ax + B)}{4y^2} = \frac{(x^2 - A)^2 - 8Bx}{4y^2}.$$

Per tant,

$$\frac{(x^2 - A)^2 - 8Bx}{4y^2} \in \mathbb{Z} \quad \Rightarrow \quad y^2 | (x^2 - A)^2 - 8Bx.$$

Com que també tenim que $y^2 | x^3 + Ax + B$, la igualtat

$$\Delta_E = -4A^3 - 27B^2 = -(3x^2 + 4A)((x^2 - A)^2 - 8Bx) + (3x^3 - 5Ax - 27B)(x^3 + Ax + B)$$

implica que $y^2 | \Delta_E$, com volíem veure. □

Corol·lari 3.20. *Sigui $E/\mathbb{Q}$ una corba el·líptica. Aleshores, el subgrup de torsió $E(\mathbb{Q})_{\text{tors}}$ és finit.*

Demostració. El canvi de variable esmentat a l'inici de la secció ens dóna una corba el·líptica amb coeficients a $\mathbb{Z}$ isomorfa a E. El Teorema de Lutz-Nagell ens diu que, en aquest cas, només tenim un nombre finit de possibilitats pels punts de torsió de E. □

4 Teorema de Mordell

En aquest capítol demostrarem el Teorema de Mordell.

Teorema 4.1. *(Mordell)*
Sigui $E/\mathbb{Q}$ una corba el·líptica. Aleshores el grup abelià $E(\mathbb{Q})$ és finitament generat, és a dir,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

on $r \geq 0$ és un nombre enter anomenat rang de E i $E(\mathbb{Q})_{\text{tors}}$ és el subgrup de torsió de E, que és finit.

Dividirem la demostració d'aquest teorema en tres parts. En la primera demostrarem un teorema conegut com a Teorema de descens. Aquest teorema ens diu que si en un grup abelià Γ tenim definida una funció, coneguda com a funció altura, que satisfà certes propietats, i, a més, el grup $\Gamma/2\Gamma$ és finit, aleshores el grup Γ és finitament generat.

En la segona part definirem una funció altura al grup abelià $E(\mathbb{Q})$ i veurem que aquesta funció satisfà les hipòtesis del Teorema de descens.

Finalment, en la tercera part, demostrarem el conegut com a Teorema feble de Mordell-Weil, que ens diu que $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit.

4.1 Teorema de descens

En aquesta secció enunciem i demostrem el Teorema de descens.

Teorema 4.2. *(Teorema de descens)*
Sigui Γ un grup abelià. Suposem que existeix una funció

$$h : \Gamma \longrightarrow [0, \infty)$$

que satisfà

(a) Per a tot nombre real M, el conjunt $\{P \in \Gamma : h(P) \leq M\}$ és finit.

(b) Per a tot $P_0 \in \Gamma$, existeix una constant k_0 tal que

$$h(P + P_0) \leq 2h(P) + k_0, \quad \text{per a tot } P \in \Gamma.$$

(c) Existeix una constant k tal que

$$h(2P) \geq 4h(P) - k, \quad \text{per a tot } P \in \Gamma.$$

Suposem, a més, que

(d) El subgrup 2Γ té índex finit en Γ.

Aleshores Γ és finitament generat.

Demostració. Per (d), el grup $\Gamma/2\Gamma$ és finit. Suposem que té ordre n. Siguin $Q_1, Q_2, \ldots, Q_n$ representants de cada classe d'equivalència de $\Gamma/2\Gamma$. Per tant, per a tot $P \in \Gamma$ existeix un índex $i_1 \in \{1, \ldots, n\}$, que depèn de P, tal que $P - Q_{i_1} \in 2\Gamma$. És a dir,

$$P - Q_{i_1} = 2P_1, \tag{4.1}$$

per a algun $P_1 \in \Gamma$. Repetint el mateix procés obtenim

$$P_1 - Q_{i_2} = 2P_2, \quad P_2 - Q_{i_3} = 2P_3, \quad \dots \quad P_{m-1} - Q_{i_m} = 2P_m,$$

on $Q_{1_2}, \dots, Q_{i_m} \in \{Q_1, \dots, Q_n\}$ i $P_2, \dots, P_m \in \Gamma$. Substituint les anteriors igualtats a l'equació (4.1) es té que

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Tenim, doncs, que P pertany al subgrup de Γ generat pels Q_i's i P_m. Veurem que, escollint un m suficientment gran, podrem fitar superiorment $h(P_m)$. Per (a), tenim que només hi ha un conjunt finit d'aquests punts. Per tant, aquest conjunt finit de punts juntament amb els Q_i's generaran Γ.
Apliquem (b) amb $P_0 = -Q_i$ per a tot $1 \leq i \leq n$ i obtenim una constant k_i tal que

$$h(P - Q_i) \leq 2h(P) + k_i, \quad \text{per a tot } P \in \Gamma.$$

Sigui k' el màxim de totes les k_i's. Per tant, per a tot $1 \leq i \leq n$, tenim que

$$h(P - Q_i) \leq 2h(P) + k', \quad \text{per a tot } P \in \Gamma.$$

Sigui k la constant donada per (c). Aleshores,

$$4h(P_j) \leq h(2P_j) + k = h(P_{j-1} - Q_{i_j}) + k \leq 2h(P_{j-1}) + k' + k.$$

Reescrivint la darrera desigualtat obtenim

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{k' + k}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (k' + k)).$$

Per tant, si $h(P_{j-1}) \geq k' + k$, es té que

$$h(P_j) \leq \frac{3}{4}h(P_{j-1}). \tag{4.2}$$

Tenim, doncs, que, en la seqüència de punts $P, P_1, P_2, \dots$, mentre que el punt P_j satisfaci $h(P_j) \geq k' + k$, aleshores el punt P_{j+1} sempre satisfrà $h(P_{j+1} \leq 3/4h(P_j)$. Ara bé, si comences amb un nombre i el multipliques reiteradament per $3/4$, el resultat se'n va cap a zero. Per tant, reiterant (4.2), obtindrem un punt $P_m \in \Gamma$ tal que $h(P_m) \leq k' + k$. S'obté així que tot $P \in \Gamma$ es pot escriure de la forma

$$P = a_1Q_1 + a_2Q_2 + \cdots + a_nQ_n + 2^m R,$$

on $a_1, \dots, a_n \in \mathbb{Z}$ i $R \in \Gamma$ satisfà $h(R) \leq k' + k$. Per tant, el conjunt

$$\{Q_1, Q_2, \dots, Q_n\} \cup \{R \in \Gamma : h(R) \leq k' + k\}$$

genera Γ. Per (a) i (d), aquest conjunt és finit, com volíem demostrar. □

El nostre objectiu serà aplicar el Teorema de descens amb $\Gamma = E(\mathbb{Q})$ i h una funció altura que definirem en la propera secció. Veurem que aquesta funció h satisfà les tres primeres hipòtesis del Teorema de descens. Per obtenir la darrera hipòtesi, demostrarem el Teorema feble de Mordell-Weil. Un cop demostrat tot això, aplicant el Teorema de descens demostrarem el Teorema de Mordell.

4.2 Altures

Introduïm en aquesta secció el concepte d'altura d'un punt de $E(\mathbb{Q})$, on $E/\mathbb{Q}$ és una corba el·líptica. Comencem definint l'altura d'un nombre racional.

Definició 4.3. *Sigui $x = \frac{m}{n} \in \mathbb{Q}$ amb $(a, b) = 1$. Es defineix l'altura de x com*

$$H(x) = H(m/n) := \max\{|m|, |n|\}.$$

Si $x = 0$, $H(x) = H(0) := 1$.
Es defineix l'altura logarítmica de x com

$$h(x) := \log H(x).$$

Definició 4.4. *Sigui $E/\mathbb{Q}$ una corba el·líptica. Sigui $P = (x, y) \in E(\mathbb{Q})$. Es defineix l'altura de P com*

$$H(P) := H(x).$$

Si $P = \infty$, $H(P) = H(\infty) := 1$.

Definició 4.5. *Sigui $E/\mathbb{Q}$ una corba el·líptica. S'anomena funció altura en $E(\mathbb{Q})$ a la funció*

$$\begin{aligned} h\colon E(\mathbb{Q}) &\to [0, \infty) \\ P &\mapsto \log H(P) \\ \infty &\mapsto 0. \end{aligned}$$

Observació 4.6. Si $E/\mathbb{Q}$ és una corba el·líptica i $P = (x, y) \in E(\mathbb{Q})$, es té que l'altura logarítmica de x coincideix amb $h(P)$, ja que $h(P) = \log H(P) = \log H(x) = h(x)$.

Lema 4.7. *Siguin $E : y^2 = x^3 + Ax + B$ una corba el·líptica definida sobre $\mathbb{Q}$ i $M \geq 0$ un nombre real. Aleshores, el conjunt $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ és finit.*

Demostració. Observem primer que el conjunt $\{x \in \mathbb{Q} : H(x) \leq M\}$ és finit. En efecte, si $x = \frac{m}{n} \in \mathbb{Q}$ amb $(m, n) = 1$, com que $H(x) = \max\{|a|, |b|\} \leq M$, tenim que $|m| \leq M$ i $|n| \leq M$. Ara bé, com que $m, n \in \mathbb{Z}$, només existeix una quantitat finita d'ells satisfent la fita anterior.
Observem que $E(\mathbb{Q})$ també té aquesta propietat, és a dir, el conjunt $\{P \in E(\mathbb{Q}) : H(P) \leq M\}$ és finit (el mateix se satisfà si canviem $H(P)$ per $h(P)$). Això és degut a que els punts del conjunt només tenen un nombre finit de possibilitats per a la seva coordenada x i per a cada x només hi ha dues possibilitats per a la coordenada y. □

Observem que el lema anterior ens diu que la funció altura h satisfà la hipòtesi (a) del Teorema de descens. A continuació veurem que també satisfà les hipòtesis (b) i (c).

Recordem que sempre podem considerar $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$. Per la Proposició 3.13 tenim que, si $P = (x, y) \in E(\mathbb{Q})$, aleshores un nombre primer p divideix el denominador de x si i només si divideix el denominador de y i que, en aquest cas, la potència exacta de p que divideix el denominador de x i de y és p^{2r} i p^{3r}, respectivament, on $r \geq 1$ és un nombre enter. Per tant, argumentant de la mateixa manera per a tot nombre primer p, obtenim que

$$P = (x, y) = \left(\frac{m}{u^2}, \frac{n}{u^3}\right),$$

amb $m, n, u \in \mathbb{Z}$, $(m, u) = 1$ i $(n, u) = 1$.

Observem que si $P = \left(\frac{m}{u^2}, \frac{n}{u^3}\right)$, aleshores $H(P) = \max\{|m|, u^2\}$. Per tant, $|m| \leq H(P)$ i $u^2 \leq H(P)$. També podem fitar n en funció de $H(P)$. Més concretament, existeix una constant $K > 0$ que depèn de A i B tal que

$$|n| \leq KH(P)^{3/2}, \quad \text{per a tot } P = \left(\frac{m}{u^2}, \frac{n}{u^3}\right) \in E(\mathbb{Q}).$$

En efecte, substituint el punt P a l'equació de E i multiplicant per u^6, s'obté

$$n^2 = m^3 + Au^4m + Bu^6.$$

Per tant,

$$|n^2| \leq |m^3| + |Au^4m| + |Bu^6| \leq H(P)^3 + |A|H(P)^3 + |B|H(P)^3 = (1 + |A| + |B|)H(P)^3.$$

Considerant $K = \sqrt{1 + |A| + |B|}$, obtenim el resultat.

Amb tot això podem demostrar que la funció altura h satisfà la hipòtesi (b) del Teorema de descens.

Lema 4.8. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$ una corba el·líptica. Aleshores, donat $P_0 \in E(\mathbb{Q})$ existeix una constant k_0, que depèn de P_0, de A i de B, tal que*

$$h(P + P_0) \leq 2h(P) + k_0, \quad \textit{per a tot } P \in E(\mathbb{Q}).$$

Demostració. Observem que el resultat és trivial si $P_0 = \infty$. Per tant, suposarem que $P_0 = (x_0, y_0) \neq \infty$. Observem també que per provar l'existència de k_0 és suficient fer-ho per a tots els punts $P \in E(\mathbb{Q})$ excepte per a un subconjunt finit d'aquests, ja que pels punts P d'aquest conjunt finit, mirem les diferències $h(P + P_0) - 2h(P)$ i agafem k_0 més gran que totes aquestes. Amb aquestes simplificacions, és suficient provar el lema pels punts $P = (x, y) \in E(\mathbb{Q}) \setminus \{P_0, -P_0, \infty\}$.
Sigui

$$P + P_0 := (\xi, \eta).$$

Necessitem calcular l'expressió de ξ per poder calcular l'altura de $P + P_0$. Com que $P \notin \{P_0, -P_0\}$, es té que $x \neq x_0$. Per les fórmules de la suma de punts, obtenim que

$$\xi = \frac{(y - y_0)^2}{(x - x_0)^2} - x - x_0 = \frac{(y - y_0)^2 - (x - x_0)^2(x + x_0)}{(x - x_0)^2}.$$

Desenvolupant el numerador veiem que apareix $y^2 - x^3$. Com que $P \in E(\mathbb{Q})$, podem substituir $y^2 - x^3$ per $Ax + B$. S'obté així que

$$\xi = \frac{ay + bx^2 + cx + d}{ex^2 + fx + g}, \tag{4.3}$$

on $a, b, c, d, e, f, g \in \mathbb{Q}$ depenen de A, B, x_0 i y_0. A l'expressió anterior, multiplicant el numerador i el denominador pel mínim comú múltiple de a, b, c, d, e, f, g podem suposar que $a, b, c, d, e, f, g \in \mathbb{Z}$. Substituint $x = m/u^2$ i $y = n/u^3$ i multplicant numerador i denominador de l'expressió (4.3) per u^4 obtenim que

$$\xi = \frac{anu + bm^2 + cmu^2 + du^4}{em^2 + fmu^2 + gu^4}.$$

La darrera expressió de ξ és un quocient de nombres enters, però no és necessàriament una fracció irreductible. A l'hora de calcular l'altura de ξ això últim no importa, ja que simplificar el numerador i el denominador pel mateix factor només fa que l'altura de ξ disminueixi. Per tant,

$$H(P+P_0) = H(\xi) \leq \max\{|anu + bm^2 + cmu^2 + du^4|, |em^2 + fmu^2 + gu^4|\}.$$

Com que $u \leq H(P)^{1/2}$, $|m| \leq H(P)$ i $|n| \leq KH(P)^{3/2}$, on $K = \sqrt{1+|A|+|B|}$, tenim que

$$|anu + bm^2 + cmu^2 + du^4| \leq |anu| + |bm^2| + |cmu^2| + |du^4| \leq (|aK| + |b| + |c| + |d|)H(P)^2$$

i

$$|em^2 + fmu^2 + gu^4| \leq |em^2| + |fmu^2| + |gu^4| \leq (|e| + |f| + |g|)H(P)^2.$$

Per tant,

$$H(P+P_0) = H(\xi) \leq \max\{|aK| + |b| + |c| + |d|, |e| + |f| + |g|\}H(P)^2.$$

Prenent logaritmes obtenim que

$$h(P+P_0) \leq 2h(P) + k_0,$$

on $k_0 = \log\max\{|aK| + |b| + |c| + |d|, |e| + |f| + |g|\}$ depèn només de A, B, x_0 i y_0. □

Veiem a continuació que la funció altura h satisfà també la hipòtesi (c) del Teorema de descens.

Lema 4.9. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$ una corba el·líptica. Aleshores, existeix una constant k, que depèn de A i B, tal que*

$$h(2P) \geq 4h(P) - k, \quad \textit{per a tot } P \in E(\mathbb{Q}).$$

Demostració. De la mateixa manera que en el Lema 4.8, podem ignorar un subconjunt finit de punts de $E(\mathbb{Q})$, perquè sempre podem agafar k més gran que $4h(P)$ per a tots els punts P d'aquest conjunt finit. En aquest cas demostrarem el lema només pels punts $P = (x, y) \in E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]$, és a dir, descartarem els punts de 2-torsió.
Tenim que $2P = (\xi, \eta)$, on, per les fórmules de l'endomorfisme de duplicació [2],

$$\xi = \frac{(3x^2 + A)^2 - 8xy^2}{4y^2}.$$

Com que $y^2 = f(x)$, on $f(x) = x^3 + Ax + B$, podem reescriure

$$\xi = \frac{(f'(x))^2 - 8xf(x)}{4f(x)} = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}. \tag{4.4}$$

Com que $2P \neq \infty$, tenim que $f(x) \neq 0$. Per tant, l'expressió (4.4) està ben definida. Observem també que, com que E és una corba el·líptica, $f(x)$ no té arrels dobles. Per tant, $f(x)$ i $f'(x)$ no tenen cap arrel en comú. Es dedueix així que ξ és un quocient de dos polinomis coprimers amb coeficients enters.
Com que $h(P) = h(x)$ i $h(2P) = h(\xi)$, el que volem provar és

$$h(\xi) \geq 4h(x) - k.$$

Aquest resultat serà conseqüència immediata del següent lema.

Lema 4.10. *Siguin $\phi(x), \psi(x) \in \mathbb{Z}[x]$ dos polinomis sense arrels en comú. Sigui d el màxim dels graus de ϕ i ψ. Aleshores,*

(a) Existeix un nombre enter $R \geq 1$, que depèn dels coeficients de ϕ i ψ, tal que per a tot $\frac{m}{n} \in \mathbb{Q}$,

$$\operatorname{mcd}\left(n^d \phi\left(\frac{m}{n}\right), n^d \psi\left(\frac{m}{n}\right)\right) \quad \textit{divideix } R.$$

(b) Existeixen constants k_1 i k_2, que depenen dels coeficients de ϕ i ψ, tals que per a tot $\frac{m}{n} \in \mathbb{Q}$ que no sigui arrel de ψ,

$$dh\left(\frac{m}{n}\right) - k_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + k_2.$$

Demostració. [1], Capítol 3, Lema 3.6. □

Fent $\frac{m}{n} = x$, $\phi(m/n) = \phi(x) = x^4 - 2Ax^2 - 8Bx + A^2$, $\psi(m/n) = \psi(x) = 4x^3 + 4Ax + 4B$, $d = 4$ i $k_2 = -k$, l'apartat (b) del lema anterior ens demostra el Lema 4.9. □

Demostrem així que la funció altura de la Definició 4.5 satisfà les tres primeres hipòtesis del Teorema de descens. Ens falta demostrar que $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit.

4.3 Teorema feble de Mordell-Weil

4.3.1 Preliminars de teoria algebraica de nombres

En aquesta secció es definiran i es presentaran conceptes i resultats d'àlgebra commutativa i de teoria algebraica de nombres que necessitarem per demostrar el Teorema feble de Mordell-Weil. Més concretament, es desenvoluparà la teoria necessària per poder enunciar dos teoremes molt importants en teoria algebraica de nombres: el Teorema de finitud del nombre de classes i el Teorema de les Unitats de Dirichlet. Comencem definint el concepte de cos de nombres.

Definició 4.11. *Un cos de nombres és una extensió finita de $\mathbb{Q}$. Es diu que K és un cos de nombres de grau n si el grau de l'extensió $K/\mathbb{Q}$ és igual a n.*

La teoria algebraica de nombres estudia l'aritmètica dels cossos de nombres. Particularment, si K és un cos de nombres, la teoria algebraica de nombres estudia l'aritmètica d'un subanell de K, que definirem més endavant, anomenat anell d'enters de K. S'estudien, entre molts altres temes, la factorització única d'aquet anell i el seu grup d'unitats.

Definició 4.12. *Siguin A, B dominis d'integritat amb $A \subseteq B$. Es diu que un element $b \in B$ és enter sobre A si b és arrel d'un polinomi mònic amb coeficients en A. El conjunt d'elements de B que són enters sobre A s'anomena la clausura entera de A en B. Es diu que B és enter sobre A si tot element de B és enter sobre A.*

Proposició 4.13. *Siguin A, B dominis d'integritat amb $A \subseteq B$. La clausura entera de A en B és un subanell de B que conté A.*

Demostració. [6], Teorema 4.1.7. □

Definició 4.14. *Un nombre complex $s \in \mathbb{C}$ s'anomena enter algebraic si s és enter sobre $\mathbb{Z}$. El conjunt dels enters algebraics es denota per Ω.*

Corol·lari 4.15. *Ω és un subanell de $\mathbb{C}$.*

Demostració. El resultat és conseqüència directa de la Proposició 4.13. □

Definim a continuació l'anell d'enters d'un cos de nombres K.

Definició 4.16. *Sigui K un cos de nombres. S'anomena anell d'enters de K a la clausura entera de K sobre $\mathbb{Z}$. L'anell d'enters d'un cos de nombres K es denota per $\mathcal{O}_K$.*

Observació 4.17. Si K és un cos de nombres, aleshores $\mathcal{O}_K = \Omega \cap K$. Observem també que, com a conseqüència de la Proposició 4.13, $\mathcal{O}_K$ és un subanell de K.

Veiem tot seguit que, si K és un cos de nombres, aleshores el cos de fraccions de $\mathcal{O}_K$ és K.

Proposició 4.18. *Sigui K un cos de nombres. Aleshores, el cos de fraccions de $\mathcal{O}_K$ és K.*

Demostració. Sigui F el cos de fraccions de $\mathcal{O}_K$. Sigui $a \in F$. Aleshores, $a = b/c$, on $b, c \in \mathcal{O}_K$ amb $c \neq 0$. Com que $\mathcal{O}_K \subseteq K$, tenim que $b, c \in K$. Finalment, com que K és un cos, es té que $a = b/c \in K$. Per tant, $F \subseteq K$.
Sigui ara $a \in K$. Com que K és una extensió finita de $\mathbb{Q}$, l'extensió $K|\mathbb{Q}$ és algebraica. Per tant, a és algebraic sobre $\mathbb{Q}$, és a dir, a és arrel d'un polinomi

$$P(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0,$$

on $c_i \in \mathbb{Q}$ per a tot $0 \leq i \leq n-1$. Sigui b el mínim comú múltiple dels denominadors de $c_0, c_1, \cdots, c_{n-1}$. Aleshores, $bc_i \in \mathbb{Z}$ per a tot $0 \leq i \leq n-1$ i

$$b^n P(a) = (ab)^n + (bc_{n-1})(ab)^{n-1} + \cdots + (b^{n-1}c_1)(ab) + b^n c_0 = 0.$$

És a dir, $ab \in K$ és un enter algebraic. Per tant, $ab \in \mathcal{O}_K$. Com que $\mathbb{Z} \subset \mathcal{O}_K$, es té que $a = (ab)/b \in F$. □

Definim a continuació els conceptes de domini d'integritat íntegrament tancat i domini noetherià i provem que l'anell d'enters d'un cos de nombres és íntegrament tancat i noetherià. Necessitarem aquest conceptes per definir posteriorment el que es coneix com a domini de Dedekind.

Definició 4.19. *Es diu que un domini d'integritat D és íntegrament tancat si els únics elements del seu cos de fraccions que són enters sobre D són els mateixos elements de D. És a dir, D és íntegrament tancat si D és la seva pròpia clausura entera en el seu cos de fraccions.*

El següent pas serà veure que l'anell d'enters d'un cos de nombres és íntegrament tancat. Per provar-ho necessitarem el següent resultat.

Lema 4.20. *Siguin A, B, C dominis d'integritat amb $A \subseteq B \subseteq C$. Si B és enter sobre A i $c \in C$ és enter sobre B, aleshores c és enter sobre A.*

Demostració. [6], Teorema 4.1.11. □

Proposició 4.21. *Sigui K un cos de nombres. Aleshores, $\mathcal{O}_K$ és íntegrament tancat.*

Demostració. Per la Proposició 4.18 sabem que el cos de fraccions de $\mathcal{O}_K$ és K. Sigui $a \in K$ enter sobre $\mathcal{O}_K$. Com que $\mathcal{O}_K$ és enter sobre $\mathbb{Z}$, pel Lema 4.20 tenim que a és enter sobre $\mathbb{Z}$, és a dir, $a \in \Omega \cap K = \mathcal{O}_K$. Per tant, $\mathcal{O}_K$ és íntegrament tancat. □

Definició 4.22. *Es diu que un domini d'integritat D és un domini noetherià si tota cadena ascendent d'ideals de D estaciona. És a dir, D és un domini noetherià si per a tota cadena d'ideals de D de la forma*

$$I_1 \subseteq I_2 \subseteq \dots I_n \subseteq \dots$$

existeix un enter positiu n_0 tal que $I_n = I_{n_0}$ per a tot $n \geq n_0$.

El següent resultat ens caracteritza els dominis noetherians.

Proposició 4.23. *Sigui D un domini d'integritat. Aleshores, D és un domini noetherià si i només si tot ideal de D és finitament generat.*

Demostració. Sigui D un domini noetherià. Suposem que hi ha un ideal I de D que no és finitament generat. Per tant, $I \neq (0)$. Sigui $a_1 \in I$ amb $a_1 \neq 0$ i sigui A_1 l'ideal generat per a_1, és a dir, $A_1 = (a_1)$. Clarament, $A_1 \subseteq I$. A més, com que A_1 és finitament generat i I no ho és, tenim que $A_1 \neq I$. Per tant, $A_1 \subset I$. Sigui ara $a_2 \in I, a_2 \notin A_1$ i sigui A_2 l'ideal $A_2 = (a_1, a_2)$. De manera anàloga als arguments anteriors, obtenim que $A_1 \subset A_2 \subset I$. Iterant aquest procés obtindríem una cadena infinita estrictament creixent d'ideals de D, $A_1 \subset A_2 \subset \dots$, contradient que D sigui un domini noetherià. Per tant, tot ideal de D és finitament generat.
Suposem ara que D és un domini d'integritat en què tot ideal és finitament generat. Sigui

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

una cadena ascendent d'ideals de D. Com que $\bigcup_{n=1}^{\infty} I_n$ també és un ideal de D, aleshores $\bigcup_{n=1}^{\infty} I_n$ és finitament generat. Per tant, existeixen $a_1, a_2, \dots, a_m \in D$ de manera que

$$\bigcup_{n=1}^{\infty} I_n = (a_1, a_2, \dots, a_m).$$

Per a tot $1 \leq i \leq m$ es té que $a_i \in \bigcup_{n=1}^{\infty} I_n$. Posem $a_i \in I_{n_i}$ i sigui $k = \max(n_1, n_2, \dots, n_m)$. Clarament, $I_k \subseteq \bigcup_{n=1}^{\infty} I_n$. Com que $n_i \leq k$, es té que $I_{n_i} \subseteq I_k$ per a tot $1 \leq i \leq m$. Per tant, per a tot $1 \leq i \leq m$ tenim que $a_i \in I_k$. S'obté, doncs, que $\bigcup_{n=1}^{\infty} I_n = (a_1, a_2, \dots, a_m) \subseteq I_k$. Això prova que $\bigcup_{n=1}^{\infty} I_n = I_k$. Per tant, $I_n = I_k$ per a tot $n \geq k$. És demostra així que D és un domini noetherià. □

Per provar que l'anell d'enters d'un cos de nombres K és un domini noetherià necessitarem el següent resultat.

Lema 4.24. *Sigui K un cos de nombres de grau n. Sigui I un ideal no nul de $\mathcal{O}_K$. Aleshores, existeixen elements $\eta_1, \dots, \eta_n \in I$ tals que tot element $\alpha \in I$ es pot expressar de manera única de la forma*

$$\alpha = \xi_1\eta_1 + \dots + \xi_n\eta_n,$$

on $\xi_1, \dots, \xi_n \in \mathbb{Z}$. En particular, I és finitament generat. Es diu que I és un $\mathbb{Z}$-mòdul finitament generat.

Demostració. La demostració es basa en el concepte de discriminant de n elements d'un cos de nombres de grau n i en algunes de les seves propietats. No desenvoluparem aquests detalls perquè no necessitarem el concepte de discriminant en la resta de la secció. La prova del resultat es pot trobar a [6], Teorema 6.5.2. □

Proposició 4.25. *Sigui K un cos de nombres. Aleshores, $\mathcal{O}_K$ és un domini noetherià.*

Demostració. El resultat és conseqüència directa de la Proposició 4.23 i el Lema 4.24. □

Sabem que un ideal maximal d'un domini d'integritat D és sempre un ideal primer. El recíproc, però, no és sempre cert, tot i que sí que ho és si D és un domini d'ideals principals. Provarem a continuació que aquest resultat també se satisfà en l'anell d'enters d'un cos de nombres K, és a dir, tot ideal primer de l'anell de nombres d'un cos de nombres K és maximal. Necessitarem el següent lema.

Lema 4.26. *Sigui K un cos de nombres. Aleshores, per a tot ideal $I \subseteq \mathcal{O}_K$ es té que l'anell quocient $\mathcal{O}_K/I$ és finit.*

Demostració. La demostració es basa en un resultat que ens diu que per a tot ideal $I \subseteq \mathcal{O}_K$ es té que $I \cap \mathbb{Z} \neq \emptyset$ i en el fet que, pel Lema 4.24, sabem que $\mathcal{O}_K$ és un $\mathbb{Z}$-mòdul finitament generat. La prova del resultat es pot trobar a [5], Proposició 12.2.3. □

Proposició 4.27. *Sigui K un cos de nombres. Aleshores, tot ideal primer no nul de $\mathcal{O}_K$ és maximal.*

Demostració. Pel Lema 4.26, si $\mathfrak{p}$ és un ideal primer no nul de $\mathcal{O}_K$, aleshores $\mathcal{O}_K/\mathfrak{p}$ és un domini d'integritat finit. Com que tot domini d'integritat finit és un cos, es té que $\mathcal{O}_K/\mathfrak{p}$ és un cos. Per tant, $\mathfrak{p}$ és maximal. □

A continuació definim el concepte de domini de Dedekind. Una de les propietats més importants dels dominis de Dedekind és que tots els seus ideals no nuls es poden expressar de manera única com a producte d'ideals primers. Veurem que l'anell d'enters d'un cos de nombres és un domini de Dedekind i, per tant, els seus ideals no nuls ademeten una factorització única com a producte d'ideals primers. Fem notar la similitud d'aquest fet amb el Teorema Fonamental de l'aritmètica, que ens diu que $\mathbb{Z}$ és un domini de factorització única. Tot i això, no tot anell d'enters d'un cos de nombres és un domini de factorització única. Definirem més endavant el nombre de classes de l'anell d'enters d'un cos de nombres K. El nombre de classes de l'anell d'enters d'un cos de nombres K ens mesura, en certa manera, quant de lluny està $\mathcal{O}_K$ de ser un domini de factorització única.

Definició 4.28. *Es diu que un domini d'integritat D és un domini de Dedekind si D satisfà les següents tres propietats:*

(i) D és íntegrament tancat.

(ii) D és un domini noetherià.

(iii) Tot ideal primer no nul de D és un ideal maximal.

Proposició 4.29. *Sigui K un cos de nombres. Aleshores, $\mathcal{O}_K$ és un domini de Dedekind.*

Demostració. El resultat és conseqüencia directa de les proposicions 4.21, 4.25 i 4.27. □

Teorema 4.30. *Sigui D un domini de Dedekind. Aleshores, tot ideal no nul $\mathfrak{a}$ de D és pot escriure de manera única com*

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n},$$

on, per a tot $1 \leq i \leq n$, $\mathfrak{p}_i$ és un ideal primer de D i a_i és un nombre enter positiu.

Demostració. [10], Teorema 3.7. □

Definim tot seguit el concepte d'ideal fraccionari d'un domini d'integritat D.

Definició 4.31. *Sigui D un domini d'integritat. Sigui F el cos de fraccions de K. Un subconjunt no buit A de F s'anomena ideal fraccionari de D si satisfà les següents tres propietats:*

(i) Si $\alpha, \beta \in A$, aleshores $\alpha + \beta \in A$.

(ii) Si $\alpha \in A$ i $r \in D$, aleshores $r\alpha \in A$.

(iii) Existeix un element $\gamma \in D \setminus \{0\}$ tal que $\gamma A \subseteq D$.

Observació 4.32. La condició (iii) de la Definició 4.31 ens diu que podem entendre γ com un múltiple dels denominadors dels elements d'un ideal fraccionari. Un ideal fraccionari d'un domini d'integritat D que és alhora un subconjunt de D és clarament un ideal de D en el sentit usual. A més, tot ideal de D és un ideal fraccionari de D que és un subconjunt de D. Normalment ens referim als ideals de D en el sentit usual com a ideals enters. Observem que si A és un ideal fraccionari de D i γ és l'element que apareix a la Definició 4.31, aleshores γA és un ideal enter de D.

Es pot veure que es pot estendre la factorització única del Teorema 4.30 a ideals fraccionaris d'un domini de Dedekind. Més en general, es pot provar que el conjunt d'ideals fraccionaris d'un domini de Dedekind forma un grup abelià amb la multiplicació d'ideals. El següent teorema recull tot això.

Teorema 4.33. *Sigui D un domini de Dedekind. Aleshores, el conjunt d'ideals fraccionaris no nuls de D té estructura de grup abelià amb la multiplicació d'ideals.*

Demostració. [6], Teorema 8.3.3. □

Corol·lari 4.34. *Sigui K un cos de nombres. Aleshores, el conjunt d'ideals fraccionaris no nuls de $\mathcal{O}_K$ té estructura de grup abelià amb la multiplicació d'ideals. Aquest grup es denota per $I(K)$.*

Demostració. El resultat és conseqüència directa de la Proposició 4.29 i del Teorema 4.33. □

Definim a continuació el grup de classes d'ideals de l'anell d'enters d'un cos de nombres. Si K és un cos de nombres, sabem pel Corol·lari 4.34 que els ideals fraccionaris no nuls de $\mathcal{O}_K$ formen un grup $I(K)$ amb la multiplicació d'ideals. Un subconjunt important de $I(K)$ són els seus ideals principals. Aquests són de la forma $(\alpha) = \{r\alpha : r \in \mathcal{O}_K\}$, on $\alpha \in K^\times$. Els ideals principals de $I(K)$ formen un subgrup de $I(K)$, que denotem per $P(K)$, ja que $(\alpha)(\beta)^{-1} = (\alpha\beta^{-1}) \in P(K)$ per a tot $(\alpha), (\beta) \in P(K)$. Com que $I(K)$ és un grup abelià, es té que $P(K)$ és un subgrup normal de $I(K)$. Per tant, el grup quocient $I(K)/P(K)$ està ben definit.

Definició 4.35. *Sigui K un cos de nombres. Sigui $I(K)$ el grup dels ideals fraccionaris no nuls de $\mathcal{O}_K$, i sigui $P(K)$ el subgrup dels ideals principals de $I(K)$. El grup quocient $I(K)/P(K)$ s'anomena grup de classes d'ideals de $\mathcal{O}_K$. Denotem el grup de classes d'ideals de $\mathcal{O}_K$ per $Cl(K)$.*

Definició 4.36. *Sigui K un cos de nombres. L'ordre del grup de classes d'ideals de $\mathcal{O}_K$ s'anomena el nombre de classes de $\mathcal{O}_K$. Denotem el nombre de classes de $\mathcal{O}_K$ per $h(K)$.*

Un dels teoremes més importants en teoria algebraica de nombres és el Teorema de finitud del nombre de classes, que ens diu que per a qualsevol cos de nombres K es té que $h(K)$ és finit. Abans, però, donem una altra interpretació del grup $Cl(K)$.

Sigui K un cos de nombres. Si dos ideals no nuls $\mathfrak{a}, \mathfrak{b}$ de $\mathcal{O}_K$ estan a la mateixa classe de $Cl(K) = I(K)/P(K)$, direm que $\mathfrak{a}$ i $\mathfrak{b}$ són equivalents. Escriurem $\mathfrak{a} \sim \mathfrak{b}$. Es té que

$$\begin{aligned}\mathfrak{a} \sim \mathfrak{b} &\Leftrightarrow \mathfrak{a}^{-1}\mathfrak{b} \in P(K) \Leftrightarrow \mathfrak{a}^{-1}\mathfrak{b} = (\alpha), \text{ per a algun } \alpha \in K^\times \\ &\Leftrightarrow \mathfrak{b} = \mathfrak{a}(\alpha), \text{ per a algun } \alpha \in K^\times \Leftrightarrow (a)\mathfrak{a} = (b)\mathfrak{b}, \text{ per a alguns } a, b \in \mathcal{O}_K \setminus \{0\}.\end{aligned}$$

El següent resultat ens diu que el nombre de classes de l'anell d'enters d'un cos de nombres K ens mesura, en certa manera, quant de lluny està $\mathcal{O}_K$ de ser un domini de factorització única.

Proposició 4.37. *Sigui K un cos de nombres. Aleshores*

$$\begin{aligned}h(K) = 1 &\Leftrightarrow \mathcal{O}_K \textit{ és un domini d'ideals principals} \\ &\Leftrightarrow \mathcal{O}_K \textit{ és un domini de factorització única.}\end{aligned}$$

Demostració. Totes les implicacions són trivials excepte el fet que si $\mathcal{O}_K$ és un domini de factorització única, aleshores $\mathcal{O}_K$ és un domini d'ideals principals. La demostració d'aquest darrer resultat es pot trobar a [10], Proposició 3.18. □

Enunciem finalment el Teorema de finitud del nombre de classes.

Teorema 4.38. *(finitud del nombre de classes)*
Sigui K un cos de nombres. Aleshores, $h(K)$ és finit.

Demostració. [6], Teorema 12.5.4. □

Per finalitzar aquesta secció, enunciarem un altre teorema molt important en teoria algebraica de nombres que, juntament amb el Teorema de finitud del nombre de classes, necessitarem per demostrar el Teorema feble de Mordell-Weil: el Teorema de les Unitats de Dirichlet.

Teorema 4.39. *(Unitats de Dirichlet)*
Sigui K un cos de nombres. Aleshores, el grup $\mathcal{O}_K^\times$ és finitament generat.

Demostració. [5], Capítol 19, §3, Lema 4. □

4.3.2 Demostració del Teorema feble de Mordell-Weil

L'objectiu d'aquesta secció és demostrar que, donada una corba el·líptica $E/\mathbb{Q}$, el grup $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit. Fent un canvi de variables, considerarem $E : y^2 = f(x)$, on $f(x) = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$.

Definim el següent anell

$$R := \mathbb{Q}(\xi) = \mathbb{Q}[x]/(f(x)),$$

on ξ denota la classe de x. Pel Teorema Xinès del Residu, es té que

$$R \cong \bigoplus_{i=1}^{n} \mathbb{Q}[x]/(f_i(x)), \tag{4.5}$$

on f_i denota un factor irreductible de f en $\mathbb{Q}[x]$. Observem que, $n = 1$ si f és irreductible sobre $\mathbb{Q}$, $n = 2$ si f té una arrel a $\mathbb{Q}$, i $n = 3$ si f té les tres arrels a $\mathbb{Q}$. Recordem que, si f és irreductible sobre $\mathbb{Q}$, aleshores $R = \mathbb{Q}(\xi) = \mathbb{Q}[x]/(f(x))$ és un cos. D'altra banda, si f té una única arrel $\alpha \in \mathbb{Q}$, aleshores $f(x) = (x - \alpha)g(x)$, on $g(x)$ és un polinomi mònic de grau 2 irreductible sobre $\mathbb{Q}[x]$, i

$$R \cong \frac{\mathbb{Q}[x]}{(x-\alpha)} \oplus \frac{\mathbb{Q}[x]}{(g(x))} \cong \mathbb{Q} \oplus \frac{\mathbb{Q}[x]}{(g(x))}.$$

Finalment, si f té les tres arrels a $\mathbb{Q}$, tenim que $R \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$.

Denotarem el grup de les unitats de R per $R^\times$. Observem que un polinomi $h(x) \in \mathbb{Q}[x]$ pertany a $R^\times$ si $h(x)$ és coprimer amb $f(x)$. Com que R és isomorf a la suma directa (4.5), es té que

$$R^\times \cong \bigoplus_{i=1}^{n} R_i^\times,$$

on $R_i = \mathbb{Q}[x]/(f_i(x))$.

Per veure que $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit, construïrem un morfisme des de $E(\mathbb{Q})$ que tingui com a nucli $2E(\mathbb{Q})$ i veurem que aquest morfisme té imatge finita. Com a conseqüència del Primer Teorema d'Isomorfia obtindrem que $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit. Per poder definir aquest morfisme necessitem introduir el següent subgrup de $R^\times$:

$$(R^\times)^2 := \{r^2 : r \in R^\times\}.$$

A la proposició següent definim el morfisme esmentat i provem que és un morfisme de grups amb nucli $2E(\mathbb{Q})$.

Proposició 4.40. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Sigui $R = \mathbb{Q}(\xi) = \mathbb{Q}[x]/(f(x))$, on $f(x) = x^3 + Ax + B$. L'aplicació*

$$\phi : E(\mathbb{Q}) \to R^\times/(R^\times)^2$$

$$\phi(P) = \phi(\alpha, \beta) = \begin{cases} 1 & \text{si } P = \infty \\ \alpha - \xi & \text{si } \beta \neq 0 \\ (f'(\alpha),\ \alpha - x \ (\mathrm{mod}(g(x))) & \text{si } \beta = 0 \end{cases},$$

on $g(x) = f(x)/(x - \alpha)$, és un morfisme de grups amb $\ker(\phi) = 2E(\mathbb{Q})$.

Demostració. Observem, primer de tot, que l'aplicació ϕ està ben definida. En efecte, si $P = (\alpha, \beta) \in E(\mathbb{Q})$ no és un punt de 2-torsió, aleshores $\alpha - x$ és coprimer amb $f(x)$. Per tant, $\alpha - \xi$ és una unitat de $R = \mathbb{Q}(\xi)$. Si $P = (\alpha, 0) \in E(\mathbb{Q})$ és un punt de 2-torsió, aleshores $f(x) = (x - \alpha)g(x)$, on $g(x)$ és un polinomi mònic de grau 2, i $R \cong \mathbb{Q}[x]/(x - \alpha) \oplus \mathbb{Q}[x]/(g(x))$. Com que $f(x)$ no té arrels dobles, es té que $f'(\alpha) \neq 0$. Finalment, com que $\alpha - x$ és coprimer amb $g(x)$, s'obté que $\phi(P) = (f'(\alpha),\ \alpha - x \pmod{g(x)})$ és una unitat de R per ser cada factor una unitat.
Veiem a continuació que ϕ és un morfisme de grups. Per a tot $P = (\alpha, \beta) \in E(\mathbb{Q})$ es té que $\phi(P) = \phi(-P)$, ja que la definició de ϕ no depèn del signe de β. Observem que si $\omega \in R^\times/(R^\times)^2$, aleshores $\omega^2 = 1$, és a dir, $\omega = \omega^{-1}$. Per veure que ϕ és morfisme de grups és suficient provar que per a tot $A, B, C \in E(\mathbb{Q})$, si $A + B + C = \infty$, aleshores $\phi(A)\phi(B)\phi(C) = \infty$. En efecte,

$$\phi(A + B) = \phi(-C) = \phi(C) = (\phi(A)\phi(B))^{-1} = \phi(A)\phi(B).$$

Posem $A = (x_1, y_1), B = (x_2, y_2), C = (x_3, y_3) \in E(\mathbb{Q})$ i suposem que $A + B + C = \infty$. Demostrarem la proposició en el cas en què els tres punts A, B i C són diferents. Els altres casos es poden provar utilitzant les fórmules de suma de punts i de duplicació. Distingim casos:

1. $x_1 = x_2$.
   Com que A, B, i C estan sobre una mateixa recta (perquè $A+B+C = \infty$), aquesta recta serà vertical. En aquest cas tenim que $B = -A$ i $C = \infty$. Per tant, $\phi(A)\phi(B)\phi(C) = \phi(A)\phi(-A)\phi(\infty) = \phi(A)^2 = 1$ mòdul quadrats de $R^\times$

2. $x_1 \neq x_2$.

   (a) Suposem que cap dels punts A, B, C és un punt de 2-torsió.
   En aquest cas es té que

   $$\phi(A)\phi(B)\phi(C) = (x_1 - \xi)(x_2 - \xi)(x_3 - \xi).$$

   Com que els tres punts estan sobre una mateixa recta $y = cx + d$, s'obté que

   $$f(x) - (cx + d)^2 = (x_1 - x)(x_2 - x)(x_3 - x). \tag{4.6}$$

   Reduïnt l'equació (4.6) mòdul $(f(x))$ s'obté que $\phi(A)\phi(B)\phi(C) = 1$ a $R^\times/(R^\times)^2$.

   (b) Suposem que només $A = (\alpha, 0)$ és un punt d'ordre 2.
   En aquest cas hem de veure que se satisfà $\phi(A)\phi(B)\phi(C) = 1$ en les dues components de

   $$R \cong \frac{\mathbb{Q}[x]}{(x - \alpha)} \oplus \frac{\mathbb{Q}[x]}{(g(x))} \cong \mathbb{Q} \oplus \frac{\mathbb{Q}[x]}{(g(x))}$$

   A la segona component, reduïnt l'equació (4.6) mòdul $(g(x))$ i mirant el resultat a $R^\times/(R^\times)^2$, es té que

   $$1 = (\alpha - x)(x_2 - x)(x_3 - x) \pmod{g(x)} = \phi(A)\phi(B)\phi(C).$$

   Per veure que el resultat també se satisfà en la primera component, derivem la igualtat (4.6) respecte de x i fem $x = \alpha$. Aleshores, $f'(\alpha) = (x_2 - \alpha)(x_3 - \alpha)$. Ara bé, com que $\phi(A) = f'(\alpha) \pmod{(x - \alpha)}$, $\phi(B) = x_2 - \alpha \pmod{(x - \alpha)}$ i $\phi(C) = x_3 - \alpha \pmod{(x - \alpha)}$, obtenim que

   $$\phi(A)\phi(B)\phi(C) = f'(\alpha)(x_2 - \alpha)(x_3 - \alpha) = (f'(\alpha))^2 = 1.$$

(c) Suposem que els tres punts A, B i C són punts de 2-torsió.
Posem $A = (\theta_1, 0), B = (\theta_2, 0), C = (\theta_3, 0)$. En aquest cas hem de veure que se satisfà $\phi(A)\phi(B)\phi(C) = 1$ en les tres components de

$$R \cong \frac{\mathbb{Q}[x]}{(x-\theta_1)} \oplus \frac{\mathbb{Q}[x]}{(x-\theta_2)} \oplus \frac{\mathbb{Q}[x]}{(x-\theta_3)} \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}.$$

Derivant una altra vegada (4.6) respecte de x i fent $x = \theta_i$, es té que

$$f'(\theta_i) = \prod_{\substack{j=1 \\ j \neq i}}^{n} (x_j - \theta_i),$$

per a $1 \leq i \leq 3$. Ara bé, com que

$$\begin{aligned} \phi(A) &= (f'(\theta_1), x_1 - \theta_2, x_1 - \theta_3) \\ \phi(B) &= (x_2 - \theta_1, f'(\theta_2), x_2 - \theta_3) \\ \phi(C) &= (x_3 - \theta_1, x_3 - \theta_2, f'(\theta_3)), \end{aligned}$$

obtenim que

$$\phi(A)\phi(B)\phi(C) = ((f'(\theta_1))^2, (f'(\theta_2))^2, (f'(\theta_3))^2) = (1, 1, 1).$$

Es demostra així que ϕ és morfisme de grups.

Provem ara que $\ker(\phi) = 2E(\mathbb{Q})$. Com que $\phi(2P) = \phi(P)^2 = 1$ per a tot $P \in E(\mathbb{Q})$, tenim que $2E(\mathbb{Q}) \subset \ker(\phi)$. Sigui ara $P = (\alpha, \beta) \in \ker(\phi)$, $P \neq \infty$. Aleshores, $\phi(P) = 1$. És a dir, $\phi(P)$ és un quadrat a $R = \mathbb{Q}(\xi)$. Es dedueix, doncs, que $\alpha - \xi$ també és un quadrat a R. En efecte, si $\beta \neq 0$, és a dir, si P no és un punt de 2-torsió, es té que $\alpha - \xi = \phi(P) = 1$. Si P és un punt de 2-torsió, tenim que $\phi(P) = (f'(\alpha),\ \alpha - x \pmod{(g(x))}) = (1, 1)$. Ara bé, com que

$$\begin{aligned} \alpha - \xi &= (\alpha - x \pmod{(x-\alpha)},\ \alpha - x \pmod{(g(x))}) \\ &= (0,\ \alpha - x \pmod{(g(x))}) \in \mathbb{Q}(\xi) \cong \frac{\mathbb{Q}[x]}{(x-\alpha)} \oplus \frac{\mathbb{Q}[x]}{(g(x))}, \end{aligned}$$

del fet que 0 i $\alpha - x \pmod{(g(x))}$ siguin quadrats a $R^\times$, es dedueix que $\alpha - \xi$ també ho és.
Com que $\alpha - \xi$ és un quadrat a $R = \mathbb{Q}(\xi)$ i $\{1, \xi, \xi^2\}$ és una base de $\mathbb{Q}(\xi)$ com a $\mathbb{Q}$-espai vectorial, es té que

$$\alpha - \xi = (\alpha_1 \xi^2 + \alpha_2 \xi + \alpha_3)^2, \tag{4.7}$$

on $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$. Com que $f(\xi) = 0$, tenim que $\xi^3 = -A\xi - B$. Per tant,

$$e_1 \xi + f_1 = (\alpha_1 \xi^2 + \alpha_2 \xi + \alpha_3)(-\alpha_1 \xi + \alpha_2), \tag{4.8}$$

on $e_1, f_1 \in \mathbb{Q}$. Observem que $\alpha_1 \neq 0$ perquè, altrament, la independència lineal de $1, \xi, \xi^2$ ens donaria una contradicció a la igualtat (4.7).
Elevant al quadrat la igualtat (4.8), substituint a (4.7), i dividint entre α_1^2 s'obté

$$(a\xi + b)^2 = (\alpha - \xi)(h - \xi)^2,$$

on $h, a, b \in \mathbb{Q}$. Per tant, el polinomi $(ax+b)^2 - (\alpha - x)(h-x)^2$ és un múltiple de $f(x)$. Ara bé, com que els dos polinomis tenen el mateix grau i són mònics, es té la igualtat $f(x) = (ax+b)^2 - (\alpha - x)(h-x)^2$. Interpretant aquesta darrera igualtat geomètricament es dedueix que la recta $y = ax + b$ talla E en el punt (α, β) o $(\alpha, -\beta)$ i és tangent a E en el punt (h, t), on $t = ah + b \in \mathbb{Q}$. Per tant,

$$(\alpha, \pm\beta) + 2(h, t) = \infty,$$

on el signe de β s'escull adequadament. Per tant,

$$P = (\alpha, \beta) = 2Q,$$

on $Q = (h, \mp t) \in E(\mathbb{Q})$, escollint el signe adequat per a t. Es demostra així que $\ker(\phi) \subset 2E(\mathbb{Q})$. Per tant, $\ker(\phi) = 2E(\mathbb{Q})$. □

Pel Primer Teorema d'Isomorfia tenim que $E(\mathbb{Q})/2E(\mathbb{Q}) \cong \phi(E(\mathbb{Q})) \subset R^\times/(R^\times)^2$. Per tant, per acabar de demostrar que $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit, hem de veure que $\phi(E(\mathbb{Q}))$ és finit. Recordem que podem escriure $R = \mathbb{Q}[x]/((f(x))$ com la suma directa dels cossos $R_i = \mathbb{Q}[x]/(f_i(x))$ i $R^\times$ com la suma directa de $R_i^\times$. Per tant, la imatge $\phi(E(\mathbb{Q}))$ es pot veure com un subgrup de la suma directa de $R_i^\times/(R_i^\times)^2$. Observem que, amb aquestes identificacions, provar que la imatge $\phi(E(\mathbb{Q}))$ és finita és equivalent a veure que, per a tot $P \in E(\mathbb{Q})$, la component i-èssima de $\phi(P)$ pertany a un subgrup finit de $R_i^\times/(R_i^\times)^2$. Com que el conjunt de punts de 2-torsió de E és un conjunt finit, no ens preocuparem en calcular les imatges per ϕ d'aquests punts. Suposem, doncs, que $P = (\alpha, \beta) \in E(\mathbb{Q})$, amb $\beta \neq 0$. Com que sempre podem considerar la corba el·líptica E definida sobre $\mathbb{Z}$, podem suposar, doncs, que $\alpha = m/u^2$, amb $m, u \in \mathbb{Z}$ i $(m, u) = 1$. Observem que, com que no estem considerant les imatges dels punts de 2-torsió, es té que, per a tot $P \in E(\mathbb{Q})$, $\phi(P) = \alpha - \xi \in R = \mathbb{Q}(\xi)$. És a dir, ϕ es comporta igual en totes les components de $R_i^\times/(R_i^\times)^2$. Sense pèrdua de generalitat, treballarem, doncs, en la component i-èssima de $R_i^\times/(R_i^\times)^2$. Sigui $\theta := \theta_i$ una arrel de $f(x)$. Posem $K := \mathbb{Q}(\theta_i) = \mathbb{Q}(\theta)$. Podem escriure $f(x) = (x-\theta)g(x)$, on $g(x) = x^2 + \theta x + A + \theta^2$. Com que $f(x) \in \mathbb{Z}[x]$ i $f(\theta) = 0$, tenim que θ és un enter algebraic. També són enters algebraics $m - u^2\theta$ i $g(m/u^2)u^4$, perquè $\theta \in \mathcal{O}_K$ i $\mathbb{Z} \subset \mathcal{O}_K$. Mantindrem tota aquesta notació fins al final d'aquesta secció. Procedim a provar tres lemes que necessitarem per demostrar el Teorema feble de Mordel-Weil.

Lema 4.41. *Sigui $E : y^2 = f(x)$, amb $f(x) = x^3 + Ax + B \in \mathbb{Z}[x]$, una corba el·líptica. Sigui $P = (\alpha, \beta) \in E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]$, on $\alpha = m/u^2$, amb $m, u \in \mathbb{Z}$ i $(m, u) = 1$. Es defineix l'ideal*

$$I(P) := (m - u^2, g(m/u^2)u^4) \subset \mathcal{O}_K.$$

Aleshores, el conjunt d'ideals $I(P)$ és finit, és a dir,

$$\{I(P) : P \in E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]\}$$

és finit.

Demostració. Tenim que

$$\begin{aligned} g(x) - g(\theta) &= x^2 + \theta x + A + \theta^2 - 2\theta^2 - A - \theta^2 \\ &= x^2 + \theta x - 2\theta^2 = (x - \theta)(x + 2\theta). \end{aligned}$$

Substituint $x = m/u^2$ i multiplicant per u^4 es té que

$$g(m/u^2)u^4 - g(\theta)u^4 = (m - u^2\theta)(m + 2\theta u^2).$$

Per tant, $g(\theta)u^4 \in I(P)$. També es té que

$$\begin{aligned} g(\theta)x^2 - g(x)\theta^2 &= g(\theta)(x^2 - \theta^2) + \theta^2(g(\theta) - g(x)) \\ &= g(\theta)(x - \theta)(x + \theta) - \theta^2(x - \theta)(x + 2\theta) \\ &= (x - \theta)(g(\theta)(x + \theta) - \theta^2(x + 2\theta)) \end{aligned}$$

Substituint $x = m/u^2$ i multiplicant per u^4 s'obté

$$g(\theta)m^2 - \theta^2 g(m/u^2)u^4 = (m - u^2\theta)u^2(g(\theta)(m/u^2 + \theta) - \theta^2(m/u^2 + 2\theta)).$$

Per tant, $g(\theta)m^2 \in I(P)$.
Es dedueix, doncs, que $(g(\theta)m^2, g(\theta)u^4) \subset I(P)$. Ara bé, com que m^2 i u^4 són coprimers, tenim que $(g(\theta)) \subset (g(\theta)m^2, g(\theta)u^4) \subset I(P)$. És a dir, $I(P)$ divideix $(g(\theta))$. Com que $\mathcal{O}_K$ és un domini de Dedekind, l'ideal $(g(\theta))$ té un nombre finit de divisors. Per tant, el nombre d'ideals $I(P)$ és finit. □

Lema 4.42. *Sigui $E : y^2 = f(x)$, amb $f(x) = x^3 + Ax + B \in \mathbb{Z}[x]$, una corba el·líptica. Sigui $P = (\alpha, \beta) \in E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]$, on $\alpha = m/u^2$ i $\beta = n/u^4$, amb $m, n, u \in \mathbb{Z}$, $(m, u) = 1$ i $(n, u) = 1$. Sigui $I(P) = (m - u^2, g(m/u^2)u^4) \subset \mathcal{O}_K$. Aleshores, existeix un ideal $C \subset \mathcal{O}_K$ tal que*

$$(m - u^2\theta) = I(P)C^2.$$

Demostració. Observem que podem escriure $(m - u^\theta) = I(P)I_1$ i $(g(m/u^2)u^4) = I(P)I_2$, on $I_1, I_2 \subset \mathcal{O}_K$ són ideals coprimers. Com que $\beta^2 = f(\alpha)$, es té que $n^2/u^6 = (m/u^2 - \theta)g(m/u^2)$. Multiplicant aquesta darrera igualtat per u^6 es té que $n^2 = (m - u^2\theta)g(m/u^2)u^4$. Per tant $(n^2) = I(P)^2 I_1 I_2$. És a dir, $I_1 I_2$ ha de ser el quadrat d'algun ideal de $\mathcal{O}_K$. Ara bé, com que I_1 i I_2 són coprimers, tant I_1 com I_2 han de ser quadrats d'ideals de $\mathcal{O}_K$. Per tant, existeix un ideal $C \subset \mathcal{O}_K$ tal que $I_1 = C^2$. □

Lema 4.43. *Sigui $E : y^2 = f(x)$, amb $f(x) = x^3 + Ax + B \in \mathbb{Z}[x]$, una corba el·líptica. Sigui $P = (\alpha, \beta) \in E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]$, on $\alpha = m/u^2$, amb $m, u \in \mathbb{Z}$ i $(m, u) = 1$. Aleshores existeix un conjunt finit d'enters algebraics $S \subset \mathcal{O}_K$ de manera que podem escriure*

$$m - u^2\theta = u\gamma\tau^2,$$

on $u \in \mathcal{O}_K^\times$, $\tau \in K$ i $\gamma \in S$

Demostració. Siguin $C_1, C_2, \ldots, C_n$ representants del grup de classes d'ideals de $\mathcal{O}_K$ (recordem que el grup de classes d'ideals de l'anell d'enters d'un cos de nombres és finit pel Teorema de finitud del nombre de classes (Teorema 4.38)). Sigui $C \subset \mathcal{O}_K$ un ideal tal que $(m - u^2\theta) = I(P)C^2$. Es té que $C \sim C_s$, on $C_s \in \{C_1, C_2, \ldots, C_n\}$. És a dir, existeixen $\rho_1, \rho_2 \in \mathcal{O}_K$ tals que $(\rho_1)C = (\rho_2)C_s$. Per tant, $I(P)C_s^2 \sim I(P)C^2 = (m - u^2\theta)$. És a dir, l'ideal $I(P)C_s^2$ és principal. Posem $I(P)C_s^2 = (\gamma)$, on $\gamma \in \mathcal{O}_K$. Com que el conjunt d'ideals $I(P)$ és finit, existeix una quantitat finita d'expressions de la forma $I(P)C_s^2$. Per a cadascuna d'aquestes expressions considerem un $\gamma \in \mathcal{O}_K$ tal que $I(P)C_s^2 = (\gamma)$. Obtenim així el conjunt finit S de l'enunciat. De les igualtats $(\rho_1^2(m - u^2\theta)) = I(P)(\rho_2^2)C_s^2 = (\gamma\rho_2^2)$, es dedueix que existeix $u \in \mathcal{O}_K$ tal que $\rho_1^2(m - u^2\theta) = u\gamma\rho_2^2$. Finalment, recordant que el cos de fraccions de $\mathcal{O}_K$ és K, s'obté el resultat posant $\tau = \rho_2/\rho_1 \in K$ □

Demostrem a continuació el Teorema feble de Mordell-Weil.

Teorema 4.44. *(feble de Mordell-Weil)*
Sigui $E/\mathbb{Q}$ una corba el·líptica. Aleshores, el grup $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit.

Demostració. Fent un canvi de variables, considerem E definida sobre $\mathbb{Z}$. Recordem que és suficient provar que la imatge $\phi(E(\mathbb{Q}))$ és finita, on ϕ és el morfisme de la Proposició 4.40. Recordem també que provar això últim és equivalent a provar que per a tot $P = (\alpha, \beta) \in E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]$, la component i-èssima de $\phi(P)$ pertany a un subgrup finit de $R_i^\times/(R_i^\times)^2$. Posem $\alpha = m/u^2$, on $m, u \in \mathbb{Z}$ i $(m, u) = 1$. Es té que $\phi(P) = m/u^2 - \xi$ mòdul quadrats de $R^\times$. A la component i-èssima $K := \mathbb{Q}(\theta_i) = \mathbb{Q}(\theta)$ de $R = \mathbb{Q}[x]/(f(x))$ es té que $\phi(P)$ val $m/u^2 - \theta$. Pel lema anterior, s'obté que $m/u^2 - \theta = (1/u^2)(m - u^2\theta) = (1/u^2)u\gamma\tau^2 = u\gamma$ a $R_i^\times/(R_i^\times)^2$, on γ pertany a un conjunt finit d'enters algebraics $S \subset \mathcal{O}_K$ i $u \in \mathcal{O}_K^\times$. Pel Teorema de les Unitats de Dirichlet (Teorema 4.39), $\mathcal{O}_K^\times$ és finitament generat. Sigui $u_1, u_2, \ldots, u_t$ una base de $\mathcal{O}_K^\times$. Aleshores, mòdul $(R_i^\times)^2$, la component i-èssima de $\phi(P)$ té un representant de la forma $u_1^{\epsilon_1}u_2^{\epsilon_2}\cdots u_t^{\epsilon_t}\gamma$, on $\epsilon_i \in \{0, 1\}$ per a tot $1 \leq i \leq t$. Com que només hi ha una quantitat finita de γ, s'obté que la component i-èssima de $\phi(P)$ té un nombre finit de representants a $R_i^\times/(R_i^\times)^2$. □

Demostrem finalment el Teorema de Mordell (Teorema 4.1)

Demostració. (Mordell)
El Teorema feble de Mordell-Weil (Teorema 4.44) ens diu que $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit. Pels lemes 4.7, 4.8 i 4.9 tenim que la funció altura de la definició 4.5 satisfà les tres hipòtesis del Teorema de descens (Teorema 4.2). Aplicant el Teorema de descens, es té que $E(\mathbb{Q})$ és finitament generat. □

4.3.3 Teorema feble de Mordell-Weil i cohomologia de Galois

L'objectiu d'aquesta darrera secció és presentar breument una versió alternativa a la demostració del Teorema feble de Mordell-Weil de la secció anterior. La demostració que exposarem es basa en conceptes i resultats de cohomologia de grups (en particular, de cohomologia de Galois) que anirem presentant al llarg de la secció. Necessitarem només introduir els grups de cohomologia H^0 i H^1. A més a més, presentarem també dos grups molt importants en l'estudi de corbes el·líptiques: el grup de Selmer i el grup de Shafarevich-Tate.

La cohomologia de grups és una eina per estudiar l'estructura d'un grup a través de les accions que aquest té sobre altres grups o conjunts. La cohomologia de Galois, en particular, estudia l'estructura del grup de Galois d'una extensió de cossos L/K a través, per exemple, de l'acció de $\mathrm{Gal}(L/K)$ sobre L o $L^\times$.

Comencem presentant el concepte de G-mòdul i de morfisme de G-mòduls.

Definició 4.45. *Siguin G un grup i M un grup abelià sobre el qual G actua. Es diu que M és un G-mòdul.*

Definició 4.46. *Siguin G un grup i M, N dos G-mòduls. Un morfisme de grups $\phi : M \longrightarrow N$ és diu que és un morfisme de G-mòduls si és un morfisme de grups compatible amb l'acció de G, és a dir, si*

$$\phi(gm) = g\phi(m)$$

per a tot $g \in G$ i tot $m \in M$.

En cohomologia de grups, donat un grup G i un G-mòdul M, s'acostuma a parlar de grups topològics (grups dotats d'una topologia de manera que l'operació del grup i el pas a l'invers siguin aplicacions contínues). És en aquest context on habitualment es demana que l'acció de G en M sigui contínua. Si el grup G és finit, dotem G amb la topologia discreta i tenim així que tota acció i tota aplicació és contínua. En canvi, si G és infinit, necessitem dotar G d'una topologia més precisa. Un exemple de grup infinit molt important és el grup de Galois de la clausura algebraica d'un cos. Aquest grup es pot dotar d'una topologia concreta, coneguda com a topologia de Krull, de manera que les accions i les aplicacions del grup siguin contínues. La teoria infinita de Galois estudia aquestes extensions de Galois infintes. No és objectiu d'aquest treball desenvolupar tota aquesta teoria. Suposarem, doncs, que totes les accions i aplicaciones de la resta de la secció són contínues.

Recordem el concepte de successió exacta de grups.

Definició 4.47. *Siguin M, N, P grups i $\alpha : M \longrightarrow N$ i $\beta : N \longrightarrow P$ morfismes de grups. La successió de grups*

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

es diu que és una successió exacta curta si α i β són morfismes de grups, α és injectiu, β és exhaustiu i $\ker(\beta) = \mathrm{Im}(\alpha)$.
Més en general, es diu que una successió de grups

$$\cdots \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to \cdots \tag{4.9}$$

és exacta a N si $\ker(\beta) = \mathrm{Im}(\alpha)$. Es diu que la successió (4.9) és exacta si és exacta a cada grup de la successió.

Presentem a continuació el grup de cohomologia H^0.

Definició 4.48. *Siguin G un grup i M un G-mòdul. Es defineix el grup de cohomologia $H^0(G, M)$ com*

$$H^0(G, M) := M^G = \{m \in M : gm = m \text{ per a tot } g \in G\}.$$

Observació 4.49. Siguin G un grup i M un G-mòdul. Observem que si l'acció de G en M és trivial, aleshores $H^0(G, M) = M$.

Per poder definir el grup de cohomologia necessitem introduir el grup dels 1-cocicles i el grup de les 1-covores.

Definició 4.50. *Siguin G un grup i M un G-mòdul. El conjunt*

$$Z^1(G, M) := \{\text{aplicacions } f : G \to M : f(g_1 g_2) = f(g_1) + g_1 f(g_2) \text{ per a tot } g_1, g_2 \in G\}$$

s'anomena conjunt dels 1-cocicles.

El conjunt dels 1-cocicles $Z^1(G, M)$ de la definició anterir també és coneix amb el nom de conjunt dels morfismes creuats, i és un grup amb la suma d'aplicacions.

Observació 4.51. Siguin G un grup i M un G-mòdul. Si l'acció de G en M és trivial, aleshores $Z^1(G, M) = \mathrm{Hom}(G, M)$ és el conjunt dels morfismes de grups de G en M.

Donat un grup G i un G-mòdul M, hi ha una manera de construir elements de $Z^1(G,M)$. Sigui $m \in M$. Definim $f_m(g) := gm - m$. Clarament, f_m és una aplicació de G en M. A més,

$$f_m(g_1g_2) = g_1(g_2m) - m = g_1m - m + g_1(g_2m - m) = f_m(g_1) + g_1f_m(g_2).$$

Per tant, $f_m \in Z^1(G,M)$. Aquest fet motiva la següent definició.

Definició 4.52. *Siguin G un grup i M un G-mòdul. El conjunt*

$$B^1(G,M) := \{f \in Z^1(G,M) : \text{ existeix un } m \in M \text{ tal que } f(g) = gm - m \text{ per a tot } g \in G\}$$

s'anomena conjunt de les 1-covores.

Definim a continuació el grup de cohomologia H^1.

Definició 4.53. *Siguin G un grup i M un G-mòdul. Es defineix el grup de cohomologia $H^1(G,M)$ com*

$$H^1(G,M) := \frac{Z^1(G,M)}{B^1(G,M)}.$$

Observació 4.54. Siguin G un grup i M un G-mòdul. Si l'acció de G en M és trivial, aleshores $B^1(G,M) = 0$, perquè $gm - m = 0$ per a tot $g \in G$ i tot $m \in M$. Com que també es té que $Z^1(G,M) = \mathrm{Hom}(G,M)$, s'obté que $H^1(G,M) \cong \mathrm{Hom}(G,M)$.

Donats un grup G i dos G-mòduls M i N, un morfisme de G-mòduls $\phi : M \longrightarrow N$ indueix una aplicació

$$\phi^* : H^j(G.M) \longrightarrow H^j(G,N)$$

entre grups de cohomologia, on $j \in \{0,1\}$. Per a H^0, l'aplicació ϕ^* és la restricció de ϕ a $H^0(G,M) = M^G$. En efecte, si $gm = m$ per a $g \in G$ i $m \in M$, aleshores $g\phi(m) = \phi(gm) = \phi(m)$ i, per tant, ϕ^* és una aplicació de $H^0(G,M) = M^G$ en $H^0(G,N) = N^G$. Per a H^1, l'aplicació ϕ^* s'obté agafant un element $f \in Z^1(G,M)$ i definint $(\phi^*(f))(g) := \phi(f(g))$.

Necessitarem el següent resultat d'àlgebra homològica durant la resta de la secció.

Proposició 4.55. *Siguin G un grup i M, N, P G-mòduls. Si*

$$0 \to M \to N \to P \to 0$$

és una successió exacta curta, aleshores

$$\begin{aligned} 0 \to H^0(G,M) \to H^0(G,N) \to H^0(G,P) \to \\ \to H^1(G,M) \to H^1(G,N) \to H^1(G,P) \end{aligned}$$

és una successió exacta.

Demostració. [12], Capítol 4, §1. □

Reflectim ara tots aquests resultats amb corbes el·líptiques. Sigui $E/\mathbb{Q}$ una corba el·líptica. Per la Proposició 2.15 tenim que l'endomorfisme $[n]$ és exhaustiu. Com que $\ker([n]) = E[n]$, es té que la successió

$$0 \to E[n] \to E(\overline{\mathbb{Q}}) \xrightarrow{[n]} E(\overline{\mathbb{Q}}) \to 0 \tag{4.10}$$

és una successió exacta curta.

Sigui $G := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Si $P = (x, y) \in E(\overline{\mathbb{Q}})$, G actua sobre $E(\overline{\mathbb{Q}})$ coordenada a coordenada, és a dir, si $g \in G$, aleshores $gP = (gx, gy)$. Observem que, per la teoria de Galois, es té que

$$H^0(G, E(\overline{\mathbb{Q}})) = E(\overline{\mathbb{Q}})^G = E(\mathbb{Q}).$$

Per tant, per la Proposició 4.55, obtenim la següent successió exacta:

$$\begin{aligned} 0 \to E(\mathbb{Q})[n] \to E(\mathbb{Q}) \xrightarrow{[n]} E(\mathbb{Q}) \to \\ \to H^1(G, E[n]) \to H^1(G, E(\overline{\mathbb{Q}})) \to H^1(G, E(\overline{\mathbb{Q}})). \end{aligned}$$

De la sucessió anterior podem extreure la següent successió exacta curta:

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to H^1(G, E[n]) \to H^1(G, E(\overline{\mathbb{Q}})[n] \to 0, \tag{4.11}$$

on $H^1(G, E(\overline{\mathbb{Q}})[n]$ denota el subgrup d'elements de $H^1(G, E(\overline{\mathbb{Q}}))$ anul·lats per $[n]$, és a dir, el subgrup de n-torsió de $H^1(G, E(\overline{\mathbb{Q}}))$.

Observem que, fent $n = 2$ a la successió (4.11), si el grup $H^1(G, E[2])$ fos finit, tindríem que $E(\mathbb{Q})/2E(\mathbb{Q})$ seria finit, demostrant així el Teorema feble de Mordell-Weil. Malauradament, això no sempre passa. Un contraexemple es pot trobar a [7], pp 109, on es prova que si $E[2] \subseteq E(\mathbb{Q})$, aleshores $H^1(G, E[2]) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \oplus \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Una solució a això vindrà de considerar corbes el·líptiques definides sobre un cos p-àdic $\mathbb{Q}_p$.

Sigui $E/\mathbb{Q}_p$ una corba el·líptica. Reescrivint la successió (4.11) en termes de $\mathbb{Q}_p$ obtenim la successió exacta

$$0 \to E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) \to H^1(G_p, E[n]) \to H^1(G_p, E(\overline{\mathbb{Q}_p})[n] \to 0,$$

on $G_p := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. La injecció de $\mathbb{Q}$ en $\mathbb{Q}_p$ indueix aplicacions $E(\mathbb{Q})/nE(\mathbb{Q}) \to E(\mathbb{Q}_p)/nE(\mathbb{Q}_p)$, $H^1(G, E[n]) \to H^1(G_p, E[n])$, $H^1(G, E(\overline{\mathbb{Q}})[n] \to H^1(G_p, E(\overline{\mathbb{Q}_p})[n]$ de manera que el següent diagrama commuta:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \longrightarrow & H^1(G, E[n]) & \longrightarrow & H^1(G, E(\overline{\mathbb{Q}})[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) & \longrightarrow & H^1(G_p, E[n]) & \longrightarrow & H^1(G_p, E(\overline{\mathbb{Q}_p})[n] & \longrightarrow & 0. \end{array}$$

Observem que l'objectiu és canviar $H^1(G, E[n])$ per un subconjunt seu de manera que aquest sigui finit i contingui la imatge de $E(\mathbb{Q})/nE(\mathbb{Q})$. Procedim de la següent manera: si $\phi \in H^1(G, E[n])$ prové d'un element de $E(\mathbb{Q})$, aleshores la seva imatge ϕ_p en $H^1(G_p, E[n])$ prové d'un element de $E(\mathbb{Q}_p)$. Aquest fet motiva la definició del grup de Selmer.

Definició 4.56. *Sigui $E/\mathbb{Q}$ una corba el·líptica i sigui $n \geq 1$ un nombre enter. Es defineix el grup de n-Selmer de E com*

$$S_n(E/\mathbb{Q}) := \ker\left(H^1(G, E[n]) \longrightarrow \prod_{p \leq \infty} H^1(G_p, E(\overline{\mathbb{Q}_p}))\right),$$

on $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $G_p = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ i $\mathbb{Q}_\infty$ denota la compleció de $\mathbb{Q}$ respecte la norma euclidiana, és a dir, $\mathbb{Q}_\infty = \mathbb{R}$.

Mantenint la mateixa notació que en la definició anterior definim el grup de Shafarevich-Tate.

Definició 4.57. *Sigui $E/\mathbb{Q}$ una corba el·líptica. Es defineix el grup de Shafarevich-Tate de E com*

$$Ш(E/\mathbb{Q}) := \ker\left(H^1(G, E(\overline{\mathbb{Q}}) \longrightarrow \prod_{p\leq\infty} H^1(G_p, E(\overline{\mathbb{Q}_p}))\right).$$

Sigui $E/\mathbb{Q}$ una corba el·líptica. A partir de les definicions de $S_n(E/\mathbb{Q})$ i $Ш(E/\mathbb{Q})$ es dedueix la següent successió exacta:

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S_n(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0, \tag{4.12}$$

on $Ш(E/\mathbb{Q})[n]$ denota el subgrup de n-torsió de $Ш(E/\mathbb{Q})$.

Fent $n = 2$ a la successió (5.12), es té que, si $S_2(E/\mathbb{Q})$ fos finit, aleshores $E(\mathbb{Q})/2E(\mathbb{Q})$ també ho seria, provant així el Teorema feble de Mordell-Weil. Per sort, en aquest cas, sí que es té que el grup $S_2(E/\mathbb{Q})$ és finit. Més en general, està demostrat que per a tot $n \geq 1$ el grup de n-Selmer $S_n(E/\mathbb{Q})$ és finit (veure [7], Capítol 4, Teorema 3.1). Es demostra així el Teorema feble de Mordell-Weil.

5 Funció L i Conjectura de Birch i Swinnerton-Dyer

En aquest darrer capítol del treball definirem la funció L d'una corba el·líptica $E/\mathbb{Q}$ i enunciarem la Conjectura de Birch i Swinnerton-Dyer.

5.1 Funció L d'una corba el·líptica $E/\mathbb{Q}$

Per poder definir la funció L d'una corba el·lítpica $E/\mathbb{Q}$, necessitem estudiar les diferents reduccions mòdul un nombre primer p de l'equació que defineix E.

Recordem que podem considerar tota corba el·líptica $E/\mathbb{Q}$ definida sobre $\mathbb{Z}$. Ara bé, podem tenir moltes possibles equacions diferents que defineixen E amb $A, B \in \mathbb{Z}$. Per tenir les millors propietats possibles al reduir l'equació de E mòdul un nombre primer p, seria ideal que el discriminant de E fos divisible per les potències més petites possibles de p. Es pot demostrar que podem obtenir una equació de E d'aquest tipus mitjançant el canvi de variable $(x, y) \mapsto (\mu^2 x, \mu^3 y)$, amb $\mu \in \overline{\mathbb{Q}}^{\times}$. Aquesta equació de E es coneix amb el nom d'equació minimal de E. Suposarem que totes les corbes el·líptiques d'aquest capítol venen donades per equacions minimals.

Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Sigui p un nombre primer. Reduïnt l'equació de E mòdul p obtenim

$$E_p : y^2 = x^3 + \overline{A}x + \overline{B},$$

on $\overline{A}, \overline{B} \in \mathbb{F}_p$ són les reduccions de A i B mòdul p. Tindríem un problema si la nova corba E_p no fos una corba el·líptica. Afortunadament, això últim només passa en un nombre finit de casos. En efecte, $\Delta_{E_p} = -4\overline{A}^3 - 27\overline{B}^2 = 0$ si i només si $p|\Delta_E$, on $\Delta_E = -4A^3 - 27B^2 \neq 0$. Aquest fet motiva la següent definició.

Definició 5.1. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Sigui p un nombre primer. Es diu que E té bona reducció a p si $p \nmid \Delta_E$. Altrament, es diu que E no té bona reducció a p.*

Si $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, és una corba el·líptica que no té bona reducció a p, aleshores la nova corba E_p no és una corba el·líptica. En aquest cas es classifica el tipus de reducció de la manera següent.

Definició 5.2. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Sigui p un nombre primer tal que E no té bona reducció a p. Denotem per $\overline{A}, \overline{B} \in \mathbb{F}_p$ les reduccions de A i B mòdul p. Es diu que*

1. *E té reducció additiva a p si el polinomi $x^3 + \overline{A}x + \overline{B}$ té una arrel triple.*
2. *E té reducció multiplicativa a p si el polinomi $x^3 + \overline{A}x + \overline{B}$ té una arrel doble. En aquest cas es distingeixen els següents dos casos. Sigui x_0 l'arrel doble de $x^3 + \overline{A}x + \overline{B}$. Es diu que*
   a) *E té reducció multiplicativa split a p si els pendents de les rectes tangents a E per $(x_0, 0)$ pertanyen a $\mathbb{F}_p$.*
   b) *E té reducció multiplicativa no split a p si algun dels pendents de les rectes tangents a E per $(x_0, 0)$ no pertany a $\mathbb{F}_p$.*

Definim a continuació la funció L d'una corba el·líptica $E/\mathbb{Q}$. Suposarem que E ve definida sobre $\mathbb{Z}$. Definim abans el següent nombre enter a_p per a cada nombre primer p.

$$a_p = \begin{cases} 0 & \text{si } E \text{ té reducció additiva a } p \\ 1 & \text{si } E \text{ té reducció multiplicativa split a } p \\ -1 & \text{si } E \text{ té reducció multiplicativa no split a } p \\ p+1-\#E_p(\mathbb{F}_p) & \text{si } E \text{ té bona reducció a } p \end{cases}$$

Definició 5.3. *Sigui $E : y^2 = x^3+Ax+B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. Es defineix la funció L de E com*

$$L_E(s) = \prod_{p|\Delta_E} (1 - a_p p^{-s})^{-1} \prod_{p\nmid\Delta_E} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

on p recorre el conjunt dels nombres primers.

Pel Teorema de Hasse (Teorema 2.21) tenim que, si E té bona reducció a p, aleshores $|a_p| < 2\sqrt{p}$. Utilitzarem aquest resultat a continuació per provar que la funció L d'una corba el·líptica $E/\mathbb{Q}$ convergeix en un semiplà concret del pla complex.

Teorema 5.4. *Sigui $E : y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{Z}$, una corba el·líptica. La funció L de E convergeix al semiplà $\{s \in \mathbb{C} : \mathrm{Re}(s) > 3/2\}$.*

Demostració. Com que el producte

$$\prod_{p|\Delta_E} (1 - a_p p^{-s})^{-1}$$

és un producte finit, per provar la convergència de $L_E(s)$ hem de provar la convergència del producte

$$\prod_{p\nmid\Delta_E} (1 - a_p p^{-s} + p^{1-2s})^{-1}. \tag{5.1}$$

Observem que el producte (5.1) convergeix si i només si el producte

$$\prod_{p\nmid\Delta_E} (1 - a_p p^{-s} + p^{1-2s}) \tag{5.2}$$

convergeix.
Sigui $(z_n)_{n\geq 0}$ una successió de nombres complexos. Un resultat conegut sobre convergència de productes infinits ens diu que si la sèrie $\sum_{n\geq 0} |z_n|$ convergeix, aleshores el producte $\prod_{n\geq 0}(1 + z_n)$ també convergeix. La demostració d'aquest fet es basa en dos resultats: el primer diu que el producte $\prod_{n\geq 0} z_n$ convergeix si i només si la sèrie $\sum_{n\geq 0} \log z_n$ convergeix (veure [9], Capítol 7, Proposició 5.2); el segon diu que la sèrie $\sum_{n\geq 0} \log(1 + z_n)$ és absolutament convergent si i només si la sèrie $\sum_{n\geq 0} z_n$ és absolutament convergent (veure [9], Capítol 7, Proposició 5.4). Per tant, per provar la convergència del producte (5.2), és suficient veure que la sèrie

$$\sum_{p\nmid\Delta_E} | - a_p p^{-s} + p^{1-2s}|$$

és convergent. Ara bé,

$$\begin{aligned}\sum_{p\nmid\Delta_E} |-a_p p^{-s}+p^{1-2s}| &\leq \sum_{p\nmid\Delta_E} |a_p p^{-s}|+|p^{1-2s}| \leq \sum_{p\nmid\Delta_E} 2|p^{\frac{1}{2}-s}|+|p^{1-2s}| \\ &\leq \sum_{p\nmid\Delta_E} 2p^{\mathrm{Re}(-s+\frac{1}{2})}+p^{\mathrm{Re}(1-2s)} = \sum_{p\nmid\Delta_E} 2p^{\mathrm{Re}(-s+\frac{1}{2})}+(p^2)^{\mathrm{Re}(-s+\frac{1}{2})} \\ &\leq \sum_{p\nmid\Delta_E} 2p^{\mathrm{Re}(-s+\frac{1}{2})}+p^{\mathrm{Re}(-s+\frac{1}{2})} = 3\sum_{p\nmid\Delta_E} p^{\mathrm{Re}(-s+\frac{1}{2})} \\ &\leq 3\sum_{n\geq 0} n^{\mathrm{Re}(-s+\frac{1}{2})} \leq \sum_{n\geq 0} n^{\mathrm{Re}(-s+\frac{1}{2})},\end{aligned}$$

on en la segona desigualtat hem utilitzat el Teorema de Hasse. El resultat segueix del fet que la sèrie

$$\sum_{n\geq 0} n^{\mathrm{Re}(-s+\frac{1}{2})}$$

convergeix si i només si $\mathrm{Re}(s) > 3/2$. □

5.2 Conjectura de Birch i Swinnerton-Dyer

Com a conseqüència del Teorema de Modularitat, un dels teoremes més importants en teoria de nombres, demostrat per C. Breuil, B. Conrad, F.Diamond i R.Taylor l'any 2001, s'obté que la funció L d'una corba el·líptica $E/\mathbb{Q}$ admet una extensió holomorfa a tot el pla complex. Més concretament, el Teorema de Modularitat afirma que $L_E(s) = L_f(s)$, on $L_f(s)$ és una funció associada a una forma modular f. Tot i que l'estudi de les formes modulars no és un dels objectius d'aquest treball, dir que una forma modular f és una funció $f : H \to \mathbb{C}$ holomorfa en el semiplà superior $H = \{s : \mathrm{Im}(s) > 0\}$ que satisfà certes propietats. A una forma modular f també se li pot associar una funció L, que denotem per $L_f(s)$. Es pot demostrar que $L_f(s)$ es pot estendre a una funció holomorfa a tot el pla complex, obtenint així l'extensió de $L_E(s)$ mencionada abans. Comentat això, observem que té sentit, doncs, parlar del valor que pren la funció $L_E(s)$ a $s = 1$.

Enunciarem a continuació la Conjectura de Birch i Swinnerton-Dyer. Recordem abans que, pel Teorema de Mordell, donada una corba el·líptica $E/\mathbb{Q}$ es té que

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^r,$$

on $r \geq 0$ és un nombre enter anomenat rang de E i $E(\mathbb{Q})_{\mathrm{tors}}$ és el subgrup de torsió de E, que és finit. Escriurem $r(E)$ per denotar el rang de E.

Conjectura 5.5. *(Birch i Swinnerton-Dyer)*
Sigui $E/\mathbb{Q}$ una corba el·líptica i sigui $r = r(E)$. Aleshores, r és igual a l'ordre d'anul·lació de $L_E(s)$ en $s = 1$. És a dir, el desenvolupament de Taylor de la funció $L_E(s)$ en $s = 1$ és

$$L_E(s) = c(s-1)^r \ + \ \textit{termes d'ordre superior},$$

on $c \neq 0$ és una constant i $r = r(E)$.

Donada una corba el·líptica $E/\mathbb{Q}$, l'ordre d'anul·lació de $L_E(s)$ en $s = 1$ es coneix amb el nom de rang analític de E.

Tot i que la Conjectura de Birch i Swinnerton-Dyer encara no està demostrada, sí que es coneix un cas particular d'aquesta, que correspon als casos en què el rang analític de la corba el·líptica és 0 o 1.

Teorema 5.6. *(Gross-Zagier, Kolyvagin)*
Sigui $E/\mathbb{Q}$ una corba el·líptica. Aleshores,

(1) Si $L_E(1) \neq 0$, aleshores $r(E) = 0$. En particular, $\#E(\mathbb{Q}) < \infty$.

(2) Si $L_E(1) = 0$ i $L'_E(1) \neq 0$, aleshores $r(E) = 1$.

És a dir, si el rang analític de E és 0 o 1, aleshores se satisfà la Conjectura de Birch i Swinnerton-Dyer.

6 Conclusions

Fent servir coneixements i resultats assolits durant aquests quatre anys, aprofundint en altres no tan coneguts com la teoria algebraica de nombres i aprenent alguns de nous com la cohomologia de Galois, hem pogut assolir els dos objectius que ens vam plantejar a l'inici del treball: demostrar el Teorema de Mordell i enunciar de manera autocontinguda la Conjectura de Birch i Swinnerton-Dyer.

Aquest treball mostra clarament que, en teoria de nombres, per tractar un problema tan simple a primera vista com és trobar solucions d'una equació, necessitem treballar amb moltes altres branques de les matemàtiques. És per això que crec que aquest treball ha estat una manera molt idònia de concloure el grau, perquè utilitza i lliga resultats de diferents assignatures cursades durant aquests quatre anys.

Referències

[1] J. H. Silverman and J. T. Tate. *Rational Points on Elliptic Curves*. 2a Edició. Undergraduate Texts in Mathematics. Springer, 2015.

[2] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. 2a Edició. Chapman & Hall/CRC, 2008.

[3] J. H. Silverman. *The Arithmetic of Elliptic Curves*. 2a Edició. Graduate Texts in Mathematics. Springer, 2009.

[4] Á. Lozano-Robledo. *Elliptic Curves, Modular Forms and their L-functions*. Student Mathematical Library, Vol. 58. American Mathematical Society, 2011.

[5] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer, 1990.

[6] S. Alaca and K. S. Williams. *Introductory Algebraic Number Theory*. Cambridge University Press, 2004.

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

[8] K. Butt. *Elliptic Curves and the Mordell-Weil Theorem*. `http://math.uchicago.edu/~may/REU2016/REUPapers/Butt.pdf`

[9] J. B. Conway. *Functions of One Complex Variable*. Graduate Texts in Mathematics. Springer, 1973.

[10] J. S. Milne. *Algebraic Number Theory*. Versió 3.08. `https://www.jmilne.org/math/CourseNotes/ANT.pdf`, 2020.

[11] A. Wiles. *The Birch and Swinnerton-Dyer Conjecture*. `https://www.claymath.org/sites/default/files/birchswin.pdf`.

[12] M. F. Atiyah and C. T. C. Wall. *Algebraic Number Theory*. Proceedings of an Instructional Conference, Brighton, 1965. pp 94–115 (*Cohomology of groups*). Thompson Book Company Inc. Washington, D.C., 1967.