Universitat Autònoma de Barcelona

Treball de Fi de Grau

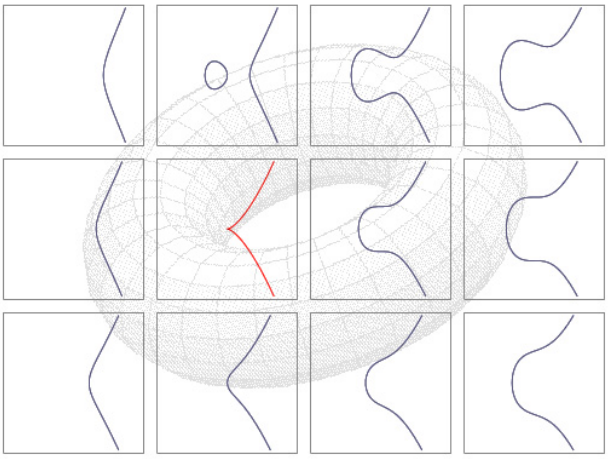
La formulació de la conjectura de Birch i Swinnerton-Dyer, un dels problemes del mil·leni de l'Institut Clay

Autor:

Jordi Ribes González

Tutor:

Dr.Francesc Bars Cortina



Obra presentada al premi Évariste Galois de la Societat Catalana de Matemàtiques

"This remarkable conjecture relates the behaviour of a function L, at a point where it is not at present known to be defined[1], to the order of a group Ш, which is not known to be finite."

-John Tate (1974)

[1] Un seguit de publicacions, començant per la d'Andrew Wiles (1999) sobre l'últim teorema de Fermat, conjuntament amb treballs posteriors i finalitzant amb l'article de Breuil, Conrand, Diamond i Taylor (2001), demostren que la funció L està definida a $s = 1$ (veieu el teorema 4.78). Aquest fet és conseqüència de la prova de la conjectura de Shimura-Taniyama-Weil (que assegura que tota corba el·líptica $E/\mathbb{Q}$ és modular, i per tant la seva funció L és la d'una forma modular, la continuació analítica de la qual és coneguda).

Índex

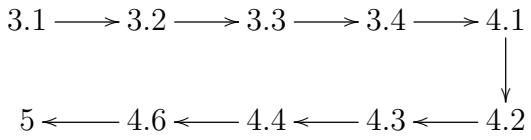
1 Prefaci

Atesa la manca de referències en català que exposin la conjectura de Birch i Swinnerton-Dyer, aquest treball pretén oferir-ne un text clar i directe, assumint només els coneixements d'un estudiant d'últim curs de grau de matemàtiques.

El primer capítol, de caràcter eminentment introductori, s'ocupa d'iniciar el lector a la teoria bàsica sobre corbes el·líptiques, i estableix les bases pel desenvolupament de la resta del treball. Posteriorment, s'exhibeixen els diversos objectes que intervenen en la conjectura i se'n comenten els conceptes relacionats. Finalment es presenta la conjectura en el context en què es va formular, acompanyada dels resultats més recents.

El treball conclueix amb tres apèndixs que complementen el cos del treball allà on s'indica, i que segur que seran d'ajuda als lectors menys familiaritzats amb la geometria algebraica, l'àlgebra commutativa o la cohomologia de grups.

Atesa la longitud del treball, proposem el següent recorregut de lectura (on és recomanable revisar els apèndixs i les referències quan el lector ho cregui convenient):



Voldria expressar el meu més sincer agraïment al tutor d'aquest treball de fi de grau, Francesc Bars Cortina, per la seva dedicació i la inestimable ajuda que ha suposat en l'elaboració d'aquest text.

2 Introducció

Una corba el·líptica E sobre $\mathbb{Q}$ és, essencialment, una corba plana al pla projectiu a la qual se li pot associar una operació (definida per funcions racionals) que en converteix el conjunt de punts amb coordenades racionals, $E(\mathbb{Q})$, en un grup.

El teorema de Mordell (demostrat el 1922 per Louis Mordell) afirma que $E(\mathbb{Q})$ és finitament generat. En l'intent de descriure aquest grup, això ens deixa amb el difícil problema d'explicitar l'anomenat rang algebraic de $E(\mathbb{Q})$ (que és el nombre d'elements d'ordre infinit d'una base per $E(\mathbb{Q})$).

A principis dels anys cinquanta (i imitant les idees d'un treball anterior sobre formes quadràtiques degut a Siegel) Peter Swinnerton-Dyer i Bryan Birch decideixen examinar el nombre de punts N_p dels diferents objectes que resulten de reduïr les coordenades dels punts de $E(\mathbb{Q})$ mòdul l'enter primer p. Amb l'ajut de la computadora EDSAC de la universitat de Cambridge, recullen certes evidències numèriques que relacionen el comportament dels nombres N_p amb el rang algebraic r del grup $E(\mathbb{Q})$.

Al seu torn, això els porta a formular una conjectura més general que utilitza la funció L de Hasse-Weil de la corba (una funció conjecturalment meromorfa al pla complex, definida a partir dels nombres N_p). La conjectura de Birch i Swinnerton-Dyer afirma que el rang algebraic de $E(\mathbb{Q})$ és exactament l'ordre del zero de la funció L al punt $s = 1$. A més, com veurem, la conjectura lliga elegantment una colla d'invariants associats a corba E amb el primer coeficient no nul del desenvolupament en sèrie de Taylor de L a $s = 1$.

La barreja d'àlgebra, geometria, anàlisi, topologia i teoria de nombres (algebraica i analítica) que observem en aquest treball és una mostra de la potent unió de diverses àrees de les matemàtiques que representa l'estudi de les corbes el·líptiques. La conjectura de Birch i Swinnerton-Dyer n'és un exemple, ja que està a mig pas entre la geometria algebraica i l'anàlisi. Això, la dificultat inqüestionable que planteja i l'esperança que una prova aclareixi l'estructura de $E(\mathbb{Q})$ han estat motius suficients perquè el Clay Mathematics Institute (CMI) la inclogui a la seva llista de problemes del mil·leni, premiant la seva demostració amb un milió de dòlars.

Notació i fets fonamentals

- Durant tot el treball k, K denoten cossos, i $\overline{k}$ denota una clausura algebraica fixada de k.

- p denota sempre un primer de $\mathbb{Z}$.

- Recordem la definició de l'**ordre p-àdic**

$$\mathrm{ord}_p(a) = n, \quad \text{on } a = p^n \frac{r}{l},\ (r,p) = (l,p) = 1.$$

  Llavors $\mathbb{Q}_p$ és la completació de $\mathbb{Q}$ amb el **valor absolut no arquimedià**

$$|a|_p = \frac{1}{p^{\mathrm{ord}_p(a)}}.$$

  A més, denotem per $\mathbb{Z}_p$ el conjunt de $x \in \mathbb{Q}_p$ tals que $\mathrm{ord}_p(x) \geq 0$, i l'anomenem el conjunt dels **enters p-àdics**. Qualsevol $\alpha \in \mathbb{Z}_p$ es pot escriure de la forma $\alpha = \sum_{i=0}^{\infty} a_i p^i$ on $0 \leq a_i \leq p-1$. Tenim que $\mathbb{Q}_p$ és el cos de fraccions de $\mathbb{Z}_p$, i que $\mathbb{Z}_p$ és un domini de factorització única.

- Donat un conjunt finit S, $\#S$ denota el nombre d'elements de S.

- Donat un grup G i un $n \in \mathbb{N}$, diem **element de torsió** de G a qualsevol element d'ordre finit de G, i **part de torsió** al subgrup d'elements de torsió de G. Anomenem **subgrup de n-torsió** al subgrup G_n d'elements de G d'ordre divisor de n. A més, diem **grup de torsió** a tot grup on cada element té ordre finit.

- Denotem $\mathbb{F}_q$ el cos finit de q elements, on $q = p^n$ per cert enter $n > 1$.

Els següents punts poden no ser coneguts per un lector poc avesat en geometria algebraica. En aquest cas, s'aconsella revisar l'apèndix A.

- Si C és una corba algebraica (definida per un conjunt de polinomis amb coeficients a k), denotem per $C(K)$ els punts de C definits a un cos $k \subseteq K$ (i.e., les arrels a K dels polinomis que defineixen C), i C/K si volem fer explícit que C està **definida** sobre el cos K (és a dir, pensem polinomis amb coeficients a K que defineixin la corba C).

- E denota una corba el·líptica, i anomenem $E(k)$ al conjunt de punts de E definits sobre k (veiem al teorema 3.8 que és un grup abelià).
- E^{aff} denota la **projecció afí** de la corba projectiva $E : Y^2Z = f(X, Y, Z)$ donada per la deshomogeneïtzació respecte la variable Z.
- Denotem el **gènere** d'una corba no singular C per $g(C)$, o per g si volem obviar la corba.
- $C^{\text{ns}}(k)$ denota el conjunt de punts no singulars de C definits sobre k.

3 Teoria bàsica de corbes el·líptiques

En aquesta secció exposem fets bàsics sobre corbes el·líptiques, necessaris per definir els objectes que intervenen en la conjectura de Birch i Swinnerton-Dyer (sobre $\mathbb{Q}$).

3.1 Definició de corba el·líptica

Sigui k un cos. Donada C una corba algebraica sobre k, $C(k)$ denota el conjunt de punts de C definits a k (veieu l'apèndix A per una explicació més distesa).

Definició 3.1. Una corba projectiva[2] E sobre k s'anomena **corba el·líptica** si compleix qualsevol de les definicions següents:

(a) una corba plana projectiva no-singular sobre k de la forma (anomenada **forma estàndard**)

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1}$$

amb $a_i \in k$;

(b) una corba plana projectiva no-singular E sobre k de grau 3 (veieu l'apartat A.8), juntament amb un punt d'inflexió[3] $O \in E(k)$;

(c) una corba plana projectiva no-singular E sobre k de grau 3, juntament amb un punt $O \in E(k)$;

(d) una corba projectiva E sobre k de gènere 1 juntament amb un punt $O \in E(k)$;

(e) una corba projectiva no-singular sobre k amb una estructura de grup definida per funcions regulars (consulteu l'apartat A.8).

[2] Veieu l'apartat A.2

[3] Si E és una corba plana i L és la recta tangent a un punt no-singular $P \in E(k)$, P s'anomena **punt d'inflexió** quan $I(P, L \cap C) \geq 3$ (veieu la definició A.7).

Usualment denotem una corba el·líptica E per E/k per explicitar el cos base on E està definida, o $(E,O)/k$ si volem explicitar també el punt distingit (quan volem obviar k, escrivim (E,O)).

Exemple 3.2. Si $k=\mathbb{C}$, llavors $E(k)\cong\mathbb{C}/\Lambda$, que és un tor complex (consulteu l'apèndix C).

Tot seguit veiem l'equivalència de les definicions (excepte per a (e), que es pot trobar a [AV] pàg.8):

(a) $\longrightarrow$ (b): Si E és com es defineix a (1), en tenim prou amb veure que $O=(0:1:0)\in E(k)$ és un punt d'inflexió. Centrant la corba a O obtenim l'equació:

$$\begin{aligned} ZY^2-2ZY+Z+a_1XZY-a_1XZ+a_3Z^2Y-a_3Z^2 \\ =X^3+a_2X^2Z+a_4XZ^2+a_6Z^3. \end{aligned}$$

Veiem doncs que l'espai tangent (sempre en el sentit de Zariski, veieu l'apartat A.2) de E a O és $L_\infty: Z=0$, que només toca a E al punt O. Per tant, la multiplicitat de la recta tangent a E al punt O és $I(O,L_\infty\cap E)=I(Z,X^3)=3$, i aleshores O és un punt d'inflexió.

(b) $\longrightarrow$ (c): Obvi.

(c) $\longrightarrow$ (d): Sigui E com (a); atès que E és no-singular i usant [FUL] §8 3.5 s'obté

$$\text{gènere de } E=\frac{(\deg E-1)(\deg E-2)}{2}=1.$$

(d) $\longrightarrow$ (a): Segons el teorema de Riemann-Roch (veieu l'apartat A.9), la dimensió de $L(m[O])$ (i.e., del $\overline{k}$-espai vectorial de les funcions racionals a $E(\overline{k})$ sense pols llevat de a O, i amb ordre del pol com a màxim $m\geq 1$) és m. Observem que les funcions constants són a $L([O])$, i són un $\overline{k}$-espai vectorial de dimensió 1, així que $\{1\}$ genera $L([O])$. Com que E/k i $2[O],3[O]$ són divisors definits a k, gràcies a la proposició [SIL] II 5.8 i pel lema d'espais vectorials de sota, podem triar $x,y\in k(E)$ generadors de $L(2[O])$

i de $L(3[O])$ respectivament. Llavors, $\{1, x, y\}$ és una $\overline{k}$-base de $L(3[O])$ formada per elements de $k(E)$.

Aleshores $x^2 \in L(4[O])$ serà $\overline{k}$-linealment independent de $1, x, y$ (si no, no podria tindre un pol d'ordre 4), i per tant $\{1, x, y, x^2\}$ és una $\overline{k}$-base de $L(4[O])$. De la mateixa manera $\{1, x, y, x^2, xy\}$ és $\overline{k}$-base de $L(5[O])$, i $\{1, x, y, x^2, xy, x^3\}$ ho és de $L(6[O])$.

Observem que $\{1, x, y, x^2, xy, x^3, y^2\}$ són $\overline{k}$-linealment dependents a $L(6[O])$, per tant

$$y^2 = -a_1xy - a_3y + a_0x^3 + a_2x^2 + a_4x + a_6. \tag{2}$$

Però com que $x, y \in k(E)$, tenim $y^\sigma = y, x^\sigma = x$ per tot $\sigma \in \mathrm{Gal}(\overline{k}/k)$. Per tant, aplicant σ a (2), obtenim

$$y^2 = (y^\sigma)^2 = -a_1^\sigma xy - a_3^\sigma y + a_0^\sigma x^3 + a_2^\sigma x^2 + a_4^\sigma x + a_6^\sigma,$$

d'on veiem $a_j = a_j^\sigma$ per tot $\sigma \in \mathrm{Gal}(\overline{k}/k)$, ja que $\{1, xy, y, x^3, x^2, x\}$ és $\overline{k}$-base de $L(6[O])$. Per tant, $a_j \in k$ per tot j.

Ara, fent els canvis $x \mapsto x/a_0$ i $y \mapsto y/a_0$ (on $a_0 \neq 0$ ja que traure x^2 de la $\overline{k}$-base de $L(6[O])$ ens deixa un conjunt linealment dependent) veiem que l'aplicació $P \mapsto (x(P), y(P))$ envia $E(k)\backslash\{O\}$ als punts definits sobre k de la corba afí

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

La funció $x \in L(2[O])$ té un pol d'ordre dos a O i cap altre pol, i per tant té només dos zeros. Per aquest motiu $x + c$ té dos zeros per tot $c \in k$, i l'aplicació

$$E(k)\backslash\{O\} \to C(k) \to \mathbb{A}^1(k) : P \mapsto (x(P), y(P)) \mapsto x(P)$$

té grau 2, ja que un element té dues antiimatges llevat de quan el discriminant del polinomi en y a (2) dins $\overline{k}(x)[y]$ s'anul·la (i això passa a un nombre finit de punts, veieu [MIL] §I 4.26(a) per més detall). Similarment, l'aplicació

$$E(k)\backslash\{O\} \to C(k) \to \mathbb{A}^1(k) : P \mapsto (x(P), y(P)) \mapsto y(P)$$

té grau 3. En conseqüència, el grau de $E(k)\backslash\{O\} \to C(k)$ divideix 2 i 3, i per tant és 1. Gràcies a [MIL] §I 4.24 i tenint en compte que C és no singular (ja que si ho fos tindria un únic punt singular doble pel teorema de Bézout, i el gènere seria 0 per [FUL] §8 3.5) obtenim que és un isomorfisme, i estén naturalment a un isomorfisme de $E(k)$ als punts sobre k de la corba projectiva

$$C' : Y^2Z + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

□

Lema 3.3. *Sigui V un $\overline{k}$-espai vectorial, i assumim que $Gal(\overline{k}/k)$ actua contínuament a V de forma compatible amb la seva acció a $\overline{k}$. Sigui*

$$V_k = V^{\mathrm{Gal}(\overline{k}/k)} = \{v \in V \mid v^\sigma = v \text{ per tot } \sigma \in \mathrm{Gal}(\overline{k}/k)\}.$$

Llavors

$$V \cong \overline{k} \otimes_k V_k,$$

i.e., l'espai vectorial V té una base de vectors $\mathrm{Gal}(\overline{k}/k)$*-invariants.*

Demostració. Consulteu [SIL] §II 5.8.1 . □

3.2 Equacions de Weierstrass d'una corba el·líptica

Sigui E una corba el·líptica sobre un cos k de característica $\neq 2, 3$. Tot seguit reescrivim la corba (1) via una **equació de Weierstrass**.

Teorema 3.4. (*a*) *Qualsevol corba el·líptica (E, O) és isomorfa sobre k a una corba descrita per una equació*

$$E(a, b) : Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in k \tag{3}$$

anomenada **equació de Weierstrass** *per a E, amb punt destacat $(0:1:0)$. D'altra banda, si $\Delta := -4a^3 - 27b^2 \neq 0$, llavors $E(a,b)$ defineix una corba el·líptica.*

(*b*) *Existeix un isomorfisme φ sobre k de $E(a',b')$ a $E(a,b)$ preservant el punt destacat si i només si existeix un element $c \in k^\times$ tal que $a' = c^4 a$, $b' = c^6 b$. En aquest cas, tenim l'isomorfisme $(x:y:z) \mapsto (c^2x : c^3y : z)$.*

(*c*) *Si $(E,O)/k$ és isomorf sobre k a $E(a,b)$ amb $a,b \in k$, definim el* **j-invariant** *de E com*

$$j(E) = \frac{1728(4a^3)}{4a^3 + 27b^2}.$$

Aleshores $j(E)$ està ben definit, i dues corbes E, E' sobre k esdevenen isomorfes sobre $\overline{k}$ si i només si $j(E) = j(E')$.

Demostració. (a) Si $char(k) \neq 2, 3$, el canvi de variables

$$X' = X + \tfrac{a_2}{3}, \quad Y' = Y + \tfrac{a_1}{2}X + \tfrac{a_3}{2}, \quad Z' = Z$$

porta a l'equació

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

que té el punt no-singular $(0:1:0)$ a k. Observeu que l'equació defineix una corba no-singular si i només si $\Delta := -4a^3 - 27b^2 \neq 0$.

(b) Suposem un tal morfisme φ; llavors (usant el raonament de l'última demostració a 3.1) $x \circ \varphi \in L(2[O]) \backslash L([O])$ i $y \circ \varphi \in L(3[O]) \backslash L(2[O])$[4], i per tant existeix una k-combinació lineal

$$x \circ \varphi = u_1 x' + r, \quad y \circ \varphi = u_2 y' + s x' + t$$

on $u_1, u_2 \in k^\times$. Ara, com que $f \mapsto f \circ \varphi : k[x,y] \longrightarrow k[x',y']$ (on $k[x,y] := k[X,Y]/\langle Y^2 - X^3 - aX - b\rangle$ és l'**anell de coordenades afí** de $E(a,b)$) és un morfisme d'anells ben definit, l'apliquem a $Y^2 = X^3 + aX + b$ per trobar que

$$(u_2y' + sx' + t)^2 = (u_1x' + r)^3 + a(u_1x' + r) + b.$$

[4]Noteu que aquí $\backslash$ denota la resta de conjunts.

Però qualsevol polinomi satisfet per x', y' és múltiple de $Y^2 - X^3 - a'X - b'$, d'on se segueix que $u_2^2 = u_1^3$, $r, s, t = 0$, (i posant $c = u_2/u_1 \in k^\times$) $a' = c^4 a$ i $b' = c^6 b$, i amb això φ queda definida sobre k. L'afirmació contrària és obvia.

(c) La primera implicació és directa per l'apartat anterior. Per veure l'oposada, si $j(E) = j(E')$ aleshores $a^3 b'^2 = a'^3 b^2$. Com que la corba $y^2 = x^3$ és singular (a L_∞), trobar una u adequada en els casos $a = 0$ i $b = 0$ és directe utilitzant la igualtat anterior (més detalls a [SIL] III 1.4(b)). Quan $ab \neq 0$, per la no-singularitat de E' (sobre $\overline{k}$) també tenim $a'b' \neq 0$ per la igualtat anterior, i per tant agafar $c = (a/a')^{1/4}$ al darrer apartat ens dóna el morfisme desitjat.

□

Observació 3.5. Aquest teorema també té un anàleg per $\mathrm{char}(k) = 2, 3$, i $j(E)$ i φ també s'hi poden definir (veieu [MIL] §II 2.4).

Observació 3.6. Dues corbes poden tenir el mateix j-invariant i no ser isomorfes sobre k. En aquest cas una s'anomena un **twist** de l'altra. La classe de les corbes sobre k que esdevenen isomorfes a E sobre $\overline{k}$ es pot descriure mitjançant cohomologia i espais homogenis, i és $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}_{\overline{k}}(E))$ (consulteu [MIL] §IV 7.12 a 7.15).

Observació 3.7. Donat $j \in k$ podem trobar una corba el·líptica sobre k amb $j(E) = j$:

$$Y^2Z = X^3 + Z^3, \quad j = 0,$$

$$Y^2Z = X^3 + XZ^2, \quad j = 1728,$$

$$Y^2Z = X^3 - \tfrac{27}{4}\tfrac{j}{j-1728}XZ^2 - \tfrac{27}{4}\tfrac{j}{j-1728}Z^3, \quad j \neq 0, 1728.$$

Fórmules de duplicació i d'addició

Considerem una corba el·líptica E/k . Tot seguit dotem $E(k)$ d'una estructura de grup abelià (això es pot fer més en general per corbes cúbiques, veieu l'apartat A.7). Definim la operació a $E(k)$ com segueix:

Siguin $P, Q \in E$, L la recta projectiva a través de P i Q (si $P = Q$ prenem la recta tangent) i definim PQ el tercer punt d'intersecció de L amb E (que existeix per [HAR]

§I 7.8, un cas especial del teorema de Bézout). Sigui L' la recta que passa per O i PQ. Definim $P+Q$ com l'altre punt d'intersecció de la recta L' amb E.

Teorema 3.8. *$E(k)$ és un grup abelià, i s'anomena* **grup de Mordell-Weil** *de E/k.*

Demostració. E/k és una corba plana projectiva no-singular de grau tres. Consulteu el teorema A.16. □

Explicitem la fórmula de la suma per la projecció afí del model (1):

Siguin $P_1, P_2 \in E(k)\backslash\{O\}$, i posem $P_3 := P_1P_2 = -(P_1+P_2)$. Denotem, amb coordenades afins (deshomogeneïtzant per Z), $P_i = (x_i, y_i)$. Per descriure la recta $L : y = \lambda x$ distingim tres casos:

$\underline{P_1 \neq P_2}$: Si $x_1 \neq x_2$ tenim $\lambda = \frac{y_1-y_2}{x_1-x_2}$ i $\beta = y_1 - \lambda x_1$.
En l'altre cas (que obviem per trobar les fórmules), $x_1 = x_2$, i L és la recta $X = x_1$ (per tant $P_2 = -P_1$ i $-P_3 = O$).

$\underline{P_1 = P_2}$: Derivant implícitament respecte X la projecció afí del model (1),

$$\lambda = \left(\frac{\partial Y}{\partial X}\right)_{(x_1,y_1)} = \frac{f'(x_1) - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \beta = y_1 - \lambda x_1.$$

Per trobar P_3 susbstituïm $Y = \lambda X + \beta$ al model i usem que el coeficient de X^2 és la suma de x_1, x_2 i x_3 (denotem $x_1 =: x_2$ si $P_1 = P_2$). Després d'obtenir així $P_3 = (x_3, \lambda x_3 + \beta)$, veiem que $-P_3 = P_1 + P_2 = (x_1, y_1) + (x_2, y_2)$ té coordenades:

$$(\lambda^2 + \lambda a_1 - a_2 - x_1 - x_2, -(\lambda + a_1)(\lambda^2 + \lambda a_1 - a_2 - x_1 - x_2) - a_1x_3 - a_3 - \beta).$$

En particular, si realitzem el mateix procediment amb $P_1 = P_2 = (x, y)$ i amb la projecció afí del model (3), obtenim les **fórmules de duplicació**

$$x_3 = \frac{(3x^2 + a)^2 - 8x(x^3 + ax + b))}{4(x^3 + ax + b)} \tag{4}$$

$$y_3 = \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{(2y)^3}. \tag{5}$$

3.3 Reducció d'una corba el·líptica mòdul p

Com que la conjectura de Birch i Swinnerton-Dyer es formula inicialment per a $E/\mathbb{Q}$, fem aquest apartat pensant $k = \mathbb{Q}$.

Considerem una corba el·líptica

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in \mathbb{Q}, \quad \Delta := -4a^3 - 27b^2 \neq 0.$$

Tal com hem vist al teorema 3.4b, tota corba el·líptica E' isomorfa a E sobre $\mathbb{Q}$ s'obté mitjançant un canvi $X' = X/c^2, Y' = Y/c^3$ per cert $c \in \mathbb{Q}^\times$. Amb aquest canvi, tenim

$$c^{12}\Delta' = \Delta, \quad c^4a' = a, \quad c^6b' = b.$$

D'un model de Weierstrass obtingut d'aquesta manera, que minimitzi $|\Delta|$ i tal que $a, b \in \mathbb{Z}$ en diem model **minimal global**.

Teorema 3.9. *Per a qualsevol corba el·líptica $E/\mathbb{Q}$ aquest model minimal global existeix i és únic.*

Demostració. Per una demostració, veieu [SIL] §VIII 8.2, 8.3 . □

Observació 3.10. En el cas que $k/\mathbb{Q}$ sigui una extensió finita, el model minimal global no necessàriament és únic; aquest fet depèn de ser o no domini de factorització única l'anomenat anell d'enters de k (veieu [HUS] §15.2 1.3).

Observació 3.11. En el cas que E/k amb k cos local (per exemple $k = \mathbb{Q}_p$, cas que treballem a la secció 3.4) l'anell d'enters de k és domini de factorització única i existeix el model minimal en aquest anell d'enters, amb $a, b \in \mathbb{Z}_p$ (consulteu [HUS] §5 1.4). Aquest model minimal s'anomena **local**.

A partir del model minimal global i d'un primer $p \neq 2, 3$, construïm la **reducció de** E **mòdul** p

$$\overline{E}/\mathbb{F}_p : Y^2Z = X^3 + \overline{a}XZ^2 + \overline{b}Z^3, \quad \overline{a}, \overline{b} \in \mathbb{F}_p, \tag{6}$$

on $\overline{a}, \overline{b}$ són les imatges de a i de b a $\mathbb{F}_p$ (per $p = 2, 3$ consulteu [MIL] §II.3). De la definició 3.1 i del fet que una corba donada per una equació de Weierstrass és el·líptica (i.e., no singular) si i només si $\Delta \neq 0$, n'extreiem el següent

Corol·lari 3.12. *Sigui $E/\mathbb{Q}$ una corba el·líptica. Si Δ és el discriminant associat al model minimal global de E, llavors $p \nmid \Delta$ si i només si $\overline{E}/\mathbb{F}_p$ és una corba el·líptica.*

Teorema 3.13 (Tate)**.** *Sigui $E/\mathbb{Q}$ una corba el·líptica i sigui $\Delta \in \mathbb{Z}$ el discriminant associat al model minimal global de E. Llavors $\Delta \neq 1$* [5].

Observació 3.14. Si $E/\mathbb{Q}$ és una corba el·líptica i $p \geq 5$ és un primer que divideix al discriminant Δ del model global minimal de E, llavors $\overline{E}/\mathbb{F}_p$ (a (6)) és una corba singular. Tot seguit estudiem corbes singulars sobre cossos finits.

Classificació de corbes planes projectives singulars de grau 3

Sigui $C : f = 0$ una corba plana projectiva singular de grau 3 sobre un cos M amb característica $\neq 2, 3$. Pel teorema de Bézout i per [FUL] §3 3(5), C tindrà només un punt singular doble $S = (a : b : c)$ [6]. A més a més aquest punt és també a coordenades sobre M, ja que si el suposem a coordenades sobre una extensió de Galois L/M, tenim, per tot automorfisme $\sigma \in \mathrm{Gal}(L/M)$:

$$f(S) = 0 \Rightarrow 0 = \sigma(f(a : b : c)) = \sum a_{ijk}(\sigma a)^i(\sigma b)^j(\sigma c)^k = f(\sigma a, \sigma b, \sigma c),$$

i.e., σ estabilitza els punts de C. Aplicant la mateixa observació a $\frac{\partial f}{\partial X} = 0$, $\frac{\partial f}{\partial Y} = 0$ i $\frac{\partial f}{\partial Z} = 0$ veiem que σ també estabilitza S, per tant $S \in \mathbb{P}^2(M)$.

Assumim que $C(M)$ conté un punt $O \neq S$. Llavors, una llei de composició similar a la definida per $C(M)$ converteix $C^{\mathrm{ns}}(M) := C(M)\backslash\{S\}$ en un grup abelià amb zero O: per [FUL] §3 3(5) i pel Teorema de Bézout, si L talla C^{ns} per dos punts P i Q, també tallarà C per un tercer punt PQ que no pot ser singular. Definim $P+Q$ com el tercer punt d'intersecció entre C i la recta que passa per O i per PQ (que pel mateix motiu tampoc és singular).

[5] Consulteu [COM] per resultats sobre el discriminant associat al model minimal global per E/k amb $[k : Q]$ finit.

[6] Si L és la recta que passa per la singularitat S i per qualsevol altre punt $P \in C$, tenim $I(S, C \cap L) \geq 2$. Per Bézout, P complirà $I(P, C \cap L) \leq 1$, i per tant no serà singular.

La singularitat S pot ser un **node** (si l'espai tangent a S són dues rectes diferents de multiplicitat 1; i.e., si S és un punt doble ordinari), o una **cúspide** (si té una sola recta tangent de multiplicitat 2). La següent proposició classifica el grup $C^{\mathrm{ns}}(M)$ segons com sigui el punt singular.

Proposició 3.15. *Sigui C/M donada per una equació del tipus* (3) *amb $char(M) \neq 2, 3$ i $\Delta = -4a^3 - 27b^2 = 0$, on C té un punt singular $S \neq O$ ($O = (0:1:0)$ és el punt distingit de l'equació* (3)*). Obtenim:*

- *Suposem que S és un node, siguin $y = \alpha_1 x + \beta_1$,$y = \alpha_2 x + \beta_2$ les rectes tangents a S. Aleshores:*
  - *Si $\alpha_1 \in M$, llavors $\alpha_2 \in M$, i*
  $$C^{ns}(M) \cong M^{\times}.$$
  - *Si $\alpha_1 \notin M$, llavors $L := M(\alpha_1, \alpha_2)$ és una extensió quadràtica de M (pel punt anterior tenim $C^{ns}(M) \subset C^{ns}(L) \cong L^{\times}$), i*
  $$C^{ns}(M) \cong \left\{ t \in L^{\times} \mid Nm_{L/M}(t) = 1 \right\},$$
  on $Nm_{L/M}(t)$ és la norma de L a M evaluada a t, definida com el determinant de l'aplicació M-lineal $a \mapsto at : L \to L$.
- *Suposem que S és una cúspide. Aleshores*
$$C^{ns}(M) \cong M^{+},$$
on M^{+} és el grup additiu M amb l'operació $(x, y) \mapsto x + y : M \times M \to M$.

Demostració. Pel cas $\overline{M} = M$ veure [SIL] §III.2 2.5. Per una discussió sobre la resta de casos, consultar [CAS] §9. □

Exemple 3.16. Per qualsevol cos M amb $char(M) \neq 2$, la corba plana projectiva
$$C/M : Y^2 Z = X^3$$

té una cúspide a $S = (0 : 0 : 1)$ amb tangent $Y = 0$ de multiplicitat 2. Com que $C \cap \{Y = 0\} = S$, és clar que $C_1 := C \cap \{Y \neq 0\} = C^{\mathrm{ns}}$, i podem deshomogeneïtzar per Y. Encara que ja ho sabem pel teorema, anem a explicitar que $C_1 : Z = X^3$ és isomorf a M^+.

Si tres punts $P_i = (x_i, z_i) \in C_1$ passen per una recta $Z = \alpha X + \beta$ (i.e., $P_1 + P_2 + P_3 = 0$), seran arrels del polinomi $X^3 - \alpha X - \beta$, i per tant n'obtenim $x_1 + x_2 + x_3 = 0$. A més, com que $O = (0, 0)$, el pas a l'invers a C^{ns} serà $(x, z) \mapsto (-x, -z)$ (en conseqüència $x(-P) = -x(P)$). Tot això implica que $P \mapsto x(P) : C^{\mathrm{ns}}(M) \to M$ és un homomorfisme, que és clarament un isomorfisme de grups.

Tot seguit donem un criteri que classifica corbes el·líptiques singulars segons la singularitat que hi apareix (pels casos a o b nuls, consulteu [MIL] §II.3).

Proposició 3.17. *Sigui M un cos amb $\mathrm{char}(M) \neq 2, 3$ i considerem una corba singular*

$$C/k : Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in M^\times, \Delta = -4a^3 - 27b^2 = 0$$

Si escrivim $t = -\frac{3b}{2a}$, llavors $S = (t : 0 : 1)$ és el punt singular de C. A més, S és una cúspide si $3t = 0$, un node amb tangents racionals sobre M si $3t$ és un quadrat a $M^\times$, i un node amb tangents no racionals sober M si $3t$ no és un quadrat a $M^\times$.

Demostració. Com que el punt $C \cap \{Z = 0\} = (0 : 1 : 0)$ és sempre no-singular, necessitem estudiar la corba afí

$$Y^2 = X^3 + aX + b.$$

L'escrivim de la forma

$$Y^2 = 3t(X - t)^2 + (X - t)^3,$$

que té una singularitat a $(t, 0)$ i on

$$-2ab = (2t^2)^2(3t),$$

d'on veiem que $3t$ és quadrat o no quadrat a M, nul o no nul, en funció de si ho és o no $-2ab$. Aquesta última observació funciona amb corbes singulars si a o b són nuls, perquè la única corba singular amb a o b nuls (assumint $\mathrm{char}(M) \neq 2, 3$) és $Y^2 = X^3$ (que té una singularitat cuspidal). □

Reducció d'una corba el·líptica mòdul p

D'acord amb les conclusions de l'apartat anterior, distingim els següents casos per la reducció (6) del model global minimal de $E/\mathbb{Q}$ mòdul $p \neq 2, 3$:

(a) **Bona reducció.** Si p no divideix Δ, aleshores $\overline{E}/\mathbb{F}_p$ és una corba el·líptica sobre $\mathbb{F}_p$. Per qualsevol punt $P = (x : y : z) \in E(\mathbb{Q})$ podem triar un representant amb x, y i z enters sense cap factor en comú, i fent-ho així $\overline{P} := (\overline{x} : \overline{y} : \overline{z})$ és un punt ben definit a $\overline{E}(\mathbb{F}_p)$. Com que les rectes redueixen a rectes i $(0 : 1 : 0)$ redueix a $(0 : 1 : 0)$, la funció reducció $E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$ és un homomorfisme de grups (es pot veure procedint com a l'exemple 3.16).

(b) **Reducció cuspidal o additiva.** Si p divideix Δ i divideix també $-2ab$, la corba reduïda $\overline{E}/\mathbb{F}_p$ té una cúspide. Per tant, $\overline{E}^{\text{ns}}(\mathbb{F}_p) \cong \mathbb{F}_p^+$.

(c) **Reducció nodal o multiplicativa.** Si p divideix Δ però no divideix $-2ab$, la corba reduïda $\overline{E}/\mathbb{F}_p$ té un node.

- Parlem de **reducció multiplicativa racional** quan $-2ab$ és un quadrat a $\mathbb{F}_p$. En aquest cas es pot veure que

$$\overline{E}^{\text{ns}}(\mathbb{F}_p) \cong \mathbb{F}_p^{\times}.$$

Parlem de **reducció multiplicativa irracional** quan $-2ab$ no és un quadrat a $\mathbb{F}_p$. Llavors, per les últimes observacions de l'apartat anterior es pot comprovar que

$$\overline{E}^{\text{ns}}(\mathbb{F}_p) \cong \left\{ t \in \mathbb{F}_p\left(\sqrt{-2\overline{ab}}\right)^{\times} \mid Nm_{\mathbb{F}_p\left(\sqrt{-2\overline{ab}}\right)/\mathbb{F}_p}(t) = 1 \right\}. \tag{7}$$

Observació 3.18. Si $E/\mathbb{Q}$ té reducció bona o nodal a p i $K/\mathbb{Q}$ finita, $E/\mathbb{Q}$ i E/K tenen la mateixa equació minimal, i la reducció de E/K a p no canvia de tipus ([SIL] §VII 5.4b). En canvi això no passa en general quan $E/\mathbb{Q}$ té reducció cuspidal a p ([SIL] §VII 5.4c). Per això, si E té reducció bona o nodal a p es diu que té reducció **semiestable** a p.

La següent taula resumeix els resultats d'aquest apartat per a $p \neq 2, 3$:

Tipus	tangents	$\Delta \mod p$	$-2ab \mod p$	$\overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$	$\#\overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$
bona	-	$\neq 0$	-	$\overline{E}(\mathbb{F}_p)$	§4.6
cuspidal	-	0	0	$\mathbb{F}_p^+$	p
nodal	racionals	0	$\square$	$\mathbb{F}_p^\times$	$p-1$
nodal	no racionals	0	$\neq \square$	(7)	$p+1$

Veiem que quan la reducció no és bona (diem que és **dolenta**) el grup $\overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$ és més o menys senzill, com també ho és $\#\overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$ (veieu [MIL] §II 3.1 pel cas no trivial del cardinal de (7)).

Observació 3.19 (Cas $p = 2$ o $p = 3$). Cal utilitzar la forma estàndard (1) per trobar una equació minimal local adequada per $\mathbb{F}_2$ o $\mathbb{F}_3$ (consulteu [SIL] §VII 5). Per exemple, qualsevol corba sobre $\mathbb{F}_2$ de la forma (3) és singular (ja que $(a, a+b)$ és arrel de $y^2 = f(x)$ i de $f'(x)$), però per exemple $Y^2 + Y = X^3 - X^2$ defineix una corba no-singular sobre $\mathbb{F}_2$.

3.4 Corbes el·líptiques sobre $\mathbb{Q}_p$

Lema (Hensel) 3.20. *Considerem $f(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$, i sigui $\underline{a} \in \mathbb{Z}^n$ tal que, per algun $m \geq 0$,*

$$f(\underline{a}) \equiv 0 \mod p^{2m+1}$$

però, per algun i,

$$\left(\frac{\partial f}{\partial X_i}(\underline{a}) \not\equiv 0 \mod p^{m+1}\right).$$

Llavors, existeix un $\underline{b} \in \mathbb{Z}_p^n$ tal que $f(\underline{b}) = 0$ i $f(\underline{b}) \equiv f(\underline{a}) \mod p^{m+1}$.

Demostració. Veure [MIL] §I 2.10-2.12. □

Sigui E una corba el·líptica sobre $\mathbb{Q}_p$:

$$E/\mathbb{Q}_p : Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in \mathbb{Q}_p, \quad \Delta := -4a^3 - 27b^2 \neq 0.$$

Fent el canvi $X' = X/c^2, Y' = Y/c^3, Z' = Z$ podem suposar $a, b \in \mathbb{Z}_p$ i $\mathrm{ord}_p(\Delta)$ minimal[7] [8]. Com a l'apartat anterior, n'obtenim $\overline{E}/\mathbb{F}_p$, la reducció de E mòdul p (observem que només té sentit reduïr el model amb aquest primer p). Triant unes **coordenades primitives** per a cada $P \in E(\mathbb{Q}_p)$ (amb $x(P), y(P), z(P) \in \mathbb{Z}_p$ però no tots a $p\mathbb{Z}_p$) tenim també una **funció de reducció** (component a component)

$$P \mapsto \overline{P} : E(\mathbb{Q}_p) \to \overline{E}(\mathbb{F}_p).$$

Construïm una filtració descendent

$$E(\mathbb{Q}_p) \supseteq E^0(\mathbb{Q}_p) \supseteq E^1(\mathbb{Q}_p) \supseteq \cdots \supseteq E^n(\mathbb{Q}_p) \supseteq \cdots .$$

Per començar, definim

$$E^0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \overline{P} \text{ no és singular}\}, \tag{8}$$

que és subgrup[9] de $E(\mathbb{Q}_p)$.

Adaptant la demostració de [HUS] §5 3.4 amb la observació a peu de pàgina, veiem que la restricció de la funció reducció

$$P \mapsto \overline{P} : E^0(\mathbb{Q}_p) \to \overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$$

és un homomorfisme. Definim $E^1(\mathbb{Q}_p)$ com seu nucli,

$$E^1(\mathbb{Q}_p) := \big\{P = (x(P) : y(P) : z(P)) \in E^0(\mathbb{Q}_p) \mid \\ x(P) \text{ i } z(P) \text{ divisibles per } p \text{ però } y(P) \text{ no divisible per } p\big\},$$

[7] Obtenint un model local minimal de Weierstrass sobre $\mathbb{Q}_p$. Recordem que la unicitat del model local minimal sobre un cos k necessita que l'anell d'enters $\mathcal{O}_k$ de k sigui domini de factorització única, i l'anell d'enters de $\mathbb{Q}_p$ (que és $\mathbb{Z}_p$) és domini de factorització única.

[8] Si $E/\mathbb{Q}$ i $p \neq 2, 3$ on E té model minimal global, llavors el mateix model és minimal local per $E/\mathbb{Q}_p$

[9] Si la recta que passa per $P, Q \in E^0(\mathbb{Q}_p)$ tallés E a un punt R que reduït fos singular, llavors, com que les rectes redueixen a rectes, la recta que passa per $\overline{P}$ i $\overline{Q}$ tallaria $\overline{E}$ per $\overline{R}$, que és absurd. A més, $(0 : 1 : 0)$ és sempre no-singular. (Si $P = Q$ s'utilitza [SIL] §VII 2.1.1 per veure que la tangent a $\overline{P}$ talla $\overline{E}$ amb multiplicitat 2)

i posem

$$E^n(\mathbb{Q}_p) = \left\{ P \in E^1(\mathbb{Q}_p) \;\middle|\; \frac{x(P)}{y(P)} \in p^n\mathbb{Z}_p \right\}.$$

Teorema 3.21. *La filtració que acabem de definir té les propietats següents*

(*a*) *El quocient $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ és finit.*

(*b*) *La funció $P \mapsto \overline{P}$ defineix un isomorfisme $E^0(\mathbb{Q}_p)/E^1(\mathbb{Q}_p) \mapsto \overline{E}^{ns}(\mathbb{F}_p)$.*

(*c*) *Per a tot $n \geq 1$, $E^n(\mathbb{Q}_p)$ és un subgrup de $E(\mathbb{Q}_p)$, i la funció $P \mapsto p^{-n}\frac{x(P)}{y(P)} \mod p$ és un isomorfisme de grups $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \to \mathbb{F}_p$.*

(*d*) *La filtració és exhaustiva, i.e., $\bigcap_n E^n(\mathbb{Q}_p) = \{0\}$.*

Demostració. (a) Consulteu [MIL] §2 4.1 .

(b) El lema de Hensel implica que la funció de reducció $E^0(\mathbb{Q}_p) \to \overline{E}^{\mathrm{ns}}(\mathbb{F}_p)$ és exhaustiva, i hem definit $E^1(\mathbb{Q}_p)$ com el seu nucli.

(c) Assumim la primera afirmació ([HUS] §4 4.5). Per la segona afirmació, multiplicant convenientment per $p^{-\mathrm{ord}_p(z)}$, considerem $P = (x' : y' : 1) \in E^1(\mathbb{Q}_p)$. Posem $x' = p^{-m}x_0$ i $y' = p^{-m'}y_0$ amb x_0, y_0 unitats a $\mathbb{Z}_p$ (tenim doncs $m' \geq 1$).

Evaluant P a l'equació de Weierstrass de E n'obtenim $2m' = 3m$, que implica que existeix un enter n tal que $m = 2n$ i $m' = 3n$. És a dir, si $P = (x : y : z) \in E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p)$ amb $n \geq 1$ (això passa si i només si $n = m' - m$), obtenim

$$\begin{cases} \mathrm{ord}_p(x) = \mathrm{ord}_p(z) - 2n \\ \mathrm{ord}_p(y) = \mathrm{ord}_p(z) - 3n \end{cases},$$

i per tant podem escriure $P = (p^n x_0 : y_0 : p^{3n} z_0)$ amb $x_0, z_0 \in \mathbb{Z}_p$ i y_0 unitat. Evaluant altre cop a l'equació de Weierstrass de E, simplificant potències de p i considerant la reducció $\overline{E_0} : Y^2Z = X^3$ de E mòdul p, veiem que $P_0 := (\overline{x_0} : \overline{y_0} : \overline{z_0})$ pertany a $\overline{E}_0^{\mathrm{ns}}(\mathbb{F}_p)$. Per una observació anterior i com que $E^n(\mathbb{Q}_p)$ és un subgrup de $E^0(\mathbb{Q}_p)$, tenim que

$$P \mapsto P_0 : E^n(\mathbb{Q}_p) \to \overline{E}_0^{\mathrm{ns}}(\mathbb{F}_p)$$

és un epimorfisme de grups amb nucli $E^{n+1}(\mathbb{Q}_p)$ (per la descripció de P). De [MIL] §II 3, obtenim un isomorfisme $Q \mapsto \frac{x(Q)}{y(Q)} : \overline{E_0}^{\text{ns}}(\mathbb{F}_p) \to \mathbb{F}_p$, que ens dóna l'isomorfisme desitjat per composició.

(d) Si $P \in \bigcap_n E^n(\mathbb{Q}_p)$, per estar dins de $E^1(\mathbb{Q}_p)$ tenim $y(P) \neq 0$, i per definició de $E^n(\mathbb{Q}_p)$ observem que $x(P) = 0$. Evaluant P a l'equació de Weierstrass de E és clar que, o bé $z(P) = 0$, o bé $y(P)^2 = bz(P)^3$. L'últim cas contradiu $P \in E^1(\mathbb{Q}_p)$, ja que $z(P)$ ha de ser divisible per p però $y(P)$ no ho és. Per tant, $P = (0 : 1 : 0)$.

□

Corol·lari 3.22. *Per tot $m \in \mathbb{Z}$, amb $p \nmid m$, l'homomorfisme*

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

és bijectiu.

Demostració. Si $P \neq O$, llavors $P \in E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p)$ per algun n (per (d)), i $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \cong \mathbb{F}_p$ (per (c)), així que la imatge de P a $\mathbb{F}_p$ és no nul·la i $mP \neq O$. Per tant l'aplicació és injectiva.

Per veure que és exhaustiva, notem que com que $p \nmid m$, el producte per m és un automorfisme de $E^1(\mathbb{Q}_p)/E^2(\mathbb{Q}_p) \cong \mathbb{F}_p$. Per tant, existeix un $Q_1 \in E^1(\mathbb{Q}_p)$ tal que

$$P = mQ_1 \mod E^2(\mathbb{Q}_p).$$

De la mateixa manera, existeix un $Q_2 \in E^2(\mathbb{Q}_p)$ tal que

$$P - mQ_1 = mQ_2 \mod E^3(\mathbb{Q}_p).$$

Continuant, obtenim una seqüència de punts $Q_i \in E^i(\mathbb{Q}_p)$ tals que $P - m\sum_n Q_i \in E^{n+1}(\mathbb{Q}_p)$; per ser $E(\mathbb{Q}_p)$ compacte, $\sum_n Q_i$ convergeix a un cert $Q \in E^1(\mathbb{Q}_p)$, i per (d) tenim $P = mQ$. □

Teorema 3.23. *$E^1(\mathbb{Q}_p)$ és lliure de torsió (i.e., no té elements d'ordre finit).*

Idea. Després de l'últim corol·lari només cal provar que $pP \neq O$ per a tot $P \in E^1(\mathbb{Q}_p)$ (consulteu [MIL] §II 5.4 per la prova). □

4 L'Aritmètica de les corbes el·líptiques

En aquesta secció definim els objectes necessaris per enunciar la conjectura de Birch i Swinnerton-Dyer (sobre $\mathbb{Q}$), tot assenyalant-ne les propietats i exposant la seva relació amb la problemàtica lligada amb la conjectura.

4.1 Grups de Selmer i de Tate-Shafarevich

Un lector no familiaritzat amb la teoria de cohomologia de grups hauria de consultar tot l'apèndix B, i la part final els que tan sols estiguin familiaritzats amb cohomologia de grups finits.

Definició 4.1. Per una corba el·líptica $E/\overline{k}$ i per $i \in \mathbb{N} \cup \{0\}$, definim $H^i(k, E) := H^i(\mathrm{Gal}(\overline{k}/k), E(\overline{k}))$ (que té estructura de grup abelià ja que $E(\overline{k})$ és abelià).

Lema 4.2. *Sigui k un cos, $E/\overline{k}$ una corba el·líptica, i $n \in \mathbb{Z}$ un enter. Llavors $P \mapsto nP : E(\overline{k}) \to E(\overline{k})$ és un epimorfisme de grups.*

Demostració. Consulteu [MIL] §IV 2.1 . □

Fixem un $n \in \mathbb{Z}$.

Del lema 4.2 tenim en particular la successió exacta

$$0 \to E_n(\overline{\mathbb{Q}}) \overset{\text{incl}}{\hookrightarrow} E(\overline{\mathbb{Q}}) \overset{\cdot n}{\twoheadrightarrow} E(\overline{\mathbb{Q}}) \to 0,$$

i per la proposició B.21 obtenim la successió exacta

$$0 \to E_n(\mathbb{Q}) \overset{\text{incl}}{\hookrightarrow} E(\mathbb{Q}) \overset{(\cdot n)}{\to} E(\mathbb{Q}) \overset{\delta}{\to} H^1(\mathbb{Q}, E_n) \overset{\text{incl}_1}{\to} H^1(\mathbb{Q}, E) \overset{(\cdot n)_1}{\to} H^1(\mathbb{Q}, E).$$

Ara utilitzem el primer teorema d'isomorfia i restringim a la imatge de la penúltima aplicació (gràcies a l'exactitud d'aquesta) per a obtenir la successió exacta curta

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \overset{\delta}{\to} H^1(\mathbb{Q}, E_n) \to H^1(\mathbb{Q}, E)_n \to 0.$$

Tot seguit, tenint en compte que l'acció de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ a $\overline{\mathbb{Q}}$ defineix un homomorfisme $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, composant-lo amb qualsevol 1-cocicle de $Z^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}}))$ i amb la inclusió a $E(\overline{\mathbb{Q}}_p)$, s'obté un homomorfisme

$$H^1(\mathbb{Q}, E) \to H^1(\mathbb{Q}_p, E). \tag{9}$$

Per tot primer p, amb aquest homomorfisme (veure [MIL] §IV 1.9 per una explicació més detallada) i la inclusió $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ s'obté el diagrama commutatiu

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, E_n) & \xrightarrow{f'} & H^1(\mathbb{Q}, E)_n & \longrightarrow & 0\,. \\
 & & \downarrow & & \downarrow & \searrow^{f=f''\circ f'} & \downarrow{\scriptstyle f''} & & \\
0 & \longrightarrow & \prod_p E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) & \longrightarrow & \prod_p H^1(\mathbb{Q}_p, E_n) & \longrightarrow & \prod_p H^1(\mathbb{Q}_p, E)_n & \longrightarrow & 0
\end{array}$$

Definició 4.3. Anomenem **grup de Selmer** al grup

$$S^{(n)}(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(\mathbb{Q}, E_n) \xrightarrow{f} \prod_{p=2,3,5\ldots} H^1(\mathbb{Q}_p, E)\right).$$

Definició 4.4. Definim el **grup de Tate-Shafarevich** com el grup

$$Ш(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(\mathbb{Q}, E) \overset{(9)}{\to} \prod_{p=2,3,5,\ldots} H^1(\mathbb{Q}_p, E)\right).$$

Teorema 4.5. *$Ш(E/\mathbb{Q})$ és un grup de torsió.*

Demostració. Veieu [HUS] §3 3.8. □

Observació 4.6. Si un element de $Ш(E/\mathbb{Q})$ té ordre n, llavors també pertany a $\mathrm{Ker}\left(H^1(\mathbb{Q}, E)_n \overset{(9)}{\to} \prod_{p=2,3,5,\ldots} H^1(\mathbb{Q}_p, E)_n\right) = \mathrm{Ker}\,(f'')$, i la inclusió contrària també es compleix gràcies al teorema 4.6. Concluïm,

$$Ш(E/\mathbb{Q})_n = \mathrm{Ker}\left(H^1(\mathbb{Q}, E)_n \overset{(9)}{\to} \prod_{p=2,3,5,\ldots} H^1(\mathbb{Q}_p, E)_n\right) = \mathrm{Ker}\,(f'').$$

Conjectura 4.7. *Per a qualsevol corba el·líptica $E/\mathbb{Q}$, el grup de Tate-Shafarevich $Ш(E/\mathbb{Q})$ és finit.*

Recordem el següent lema d'àlgebra homològica.

Lema 4.8. *Per qualsevol parell d'homomorfismes de grups abelians o R-mòduls (amb R anell)*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

es té la successió exacta (anomenada **nucli-conucli**[10]*)*

$$0 \longrightarrow \mathrm{Ker}(\alpha) \longrightarrow \mathrm{Ker}(\beta \circ \alpha) \longrightarrow \mathrm{Ker}(\beta) \longrightarrow$$

$$\longrightarrow \mathrm{Coker}(\alpha) \longrightarrow \mathrm{Coker}(\beta \circ \alpha) \longrightarrow \mathrm{Coker}(\beta) \longrightarrow 0.$$

Aplicant aquest lema als homomorfismes

$$H^1(\mathbb{Q}, E_n) \xrightarrow{f'} (\mathbb{Q}, E)_n \xrightarrow{f''} \prod_p H^1(\mathbb{Q}_p, E)_n,$$

com que f' és epimorfisme (el conucli és 0), s'obté la successió exacta:

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S^{(n)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})_n \to 0. \tag{10}$$

Teorema 4.9. *Per qualsevol corba el·líptica $E/\mathbb{Q}$ i qualsevol enter n, el grup de Selmer $S^{(n)}(E/\mathbb{Q})$ és finit*[11] *.*

Demostració. Veieu [MIL] §IV.3. □

Teorema 4.10 (Mordell-Weil dèbil)**.** *Per qualsevol corba el·líptica $E/\mathbb{Q}$ i qualsevol enter n, el grup $E(\mathbb{Q})/nE(\mathbb{Q})$ és finit.*

Demostració. És directe a partir de la successió exacta (10) i del teorema 4.9. Per $n = 2$ és possible desenvolupar una demostració elemental d'aquest fet. Veieu [SIL-TATE] §III.4, §III.5. □

[10] $\mathrm{Coker}(X \xrightarrow{f} Y) = Y/\mathrm{Im}(f)$.

[11] De fet fins i tot es pot calcular en un nombre finit de passos, ja que és possible descriure els elements del grup finit $H^1(\mathbb{Q}, E_n)$ i decidir quins d'ells pertanyen a $S^{(n)}(E/\mathbb{Q})$ (consulteu [SIL] §X 4.5.1).

4.2 Altures

Definició 4.11. Sigui $P \in \mathbb{P}^n(\mathbb{Q})$, i $(a_0, \ldots, a_n)$ un representant primitiu[12] de P. Definim l'**altura** $H(P)$ de P com

$$H(P) = \max_i |a_i|.$$

A més, escrivim $h(P) = \log H(P)$, i l'anomenem **altura logarítmica**.

Altures a $\mathbb{P}^1$

Proposició 4.12. *Siguin $F(X,Y), G(X,Y) \in \mathbb{Q}[X,Y]$ polinomis homogenis de grau m sense zeros en comú a $\mathbb{P}^1(\overline{\mathbb{Q}})$, i considerem l'aplicació $\varphi : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$, $(x : y) \mapsto (F(x,y) : G(x,y))$. Llavors, existeix una constant B tal que*

$$|h(\varphi(P)) - mh(P)| \leq B, \qquad \textit{per tot } P \in \mathbb{P}^1(\mathbb{Q}).$$

Demostració. Com que multiplicar F i G per una constant no nul·la no canvia φ, podem suposar que F i G tenen coeficients enters. Sigui $(a : b)$ un representant primitiu de P. Per qualsevol monomi cX^iY^{m-i} de F o de G tenim $|ca^ib^{m-i}| \leq |c| \max(|a|^m, |b|^m)$ (gràcies a la homogeneïtat de F i de G), i per tant

$$|F(a,b)|, |G(a,b)| \leq C(\max(|a|, |b|))^m,$$

on

$$C = (m+1)\max(|\text{coef. d'}F \text{ o de } G|).$$

En conseqüència

$$\begin{aligned} H(\varphi(P)) &\leq \max(|F(a,b)|, |G(a,b)|) \\ &\leq C \cdot \max(|a|, |b|)^m = C \cdot H(P)^m, \end{aligned}$$

[12] Diem que $(a_0, \ldots, a_n)$ és un **representant primitiu** per P si $P = (a_0 : \ldots : a_n)$

$$a_i \in \mathbb{Z} \quad \text{mcd}(a_0, \ldots, a_n) = 1.$$

i prenent logaritmes, s'obté

$$h(\varphi(P)) \leq mh(P) + \log C. \tag{11}$$

Per veure l'altra desigualtat, considerem $F(\frac{X}{Y}, 1) = Y^{-m}F(X,Y)$ i $G(\frac{X}{Y}, 1) = Y^{-m}G(X,Y)$. Tenint en compte que F i G no tenen zeros en comú, la teoria de resultants afirma que existeixen dos polinomis $U(\frac{X}{Y}), V(\frac{X}{Y}) \in \mathbb{Z}[\frac{X}{Y}]$ de grau $m-1$ tals que

$$U\left(\frac{X}{Y}\right)F\left(\frac{X}{Y},1\right) + V\left(\frac{X}{Y}\right)G\left(\frac{X}{Y},1\right) = R \quad R \in \mathbb{Z}, R \neq 0.$$

Multiplicant per Y^{2m-1} i redefinint $U(X,Y) := Y^{m-1}U(\frac{X}{Y})$, $V(X,Y) := Y^{m-1}V(\frac{X}{Y})$,

$$U(X,Y)F(X,Y) + V(X,Y)G(X,Y) = RY^{2m-1}.$$

Repetint el mateix argument (intercanviant les variables) obtenim

$$U(X,Y)F(X,Y) + V(X,Y)G(X,Y) = RX^{2m-1}.$$

Evaluant aquestes dues equacions a $P = (a:b)$

$$U(a,b)F(a,b) + V(a,b)G(a,b) = Rb^{2m-1} \tag{12}$$

$$U'(a,b)F(a,b) + V'(a,b)G(a,b) = Ra^{2m-1}, \tag{13}$$

i a partir d'aquí observem

$$\text{mcd}(F(a,b), G(a,b)) \text{ divideix } \text{mcd}(Ra^{2m-1}, Rb^{2m-1}) = R.$$

Ara, tenint en compte que hem definit $U, U', V, V' \in \mathbb{Z}[X,Y]$ com a polinomis homogenis, la primera part de la prova ens diu que existeix una constant positiva $C \in \mathbb{Z}$ tal que

$$U(X,Y), U'(X,Y), V(X,Y), V'(X,Y) \leq C \max(|a|,|b|)^{m-1},$$

i si ho apliquem a les equacions (12) i (13) veiem

$$|R||a|^{2m-1}, |R||b|^{2m-1} \leq 2C \max(|a|,|b|)^{m-1} H(\varphi(P)).$$

Utilitzant primer $\mathrm{mcd}(F(a,b),G(a,b))|R$ i després les dues últimes desigualtats

$$H(\varphi(P)) \geq \frac{1}{R}\max(|F(a,b)|,|G(a,b)|) \geq \frac{1}{2C}H(P)^m,$$

i prenent logaritmes concluïm

$$h(\varphi(P)) \geq mh(P) - \log(2C).$$

□

Altures a $E/\mathbb{Q}$ i l'aparellament de Néron-Tate

Definició 4.13. Sigui $E/\mathbb{Q}$ una corba el·líptica donada per una equació de Weierstrass (3), i $P \in E(\mathbb{Q})$. Definim l'**altura** $H(P)$ (a E) de P com

$$H(P) = \begin{cases} H((x(P) : z(P))), & \text{si } z(P) \neq 0, \\ 1, & \text{si } P = (0:1:0). \end{cases}$$

A més, escrivim $h(P) := \log H(P)$, i l'anomenem **altura logarítmica** (a E).

Observació 4.14. Hi ha diverses maneres de definir h. Més precisament, donada una funció racional $f \in \overline{\mathbb{Q}}(E)$, definim

$$g : E \to \mathbb{P}^1, \quad P \mapsto \begin{cases} (1:0), & \text{si } P \text{ és un pol de } f, \\ (f(P):1), & \text{altrament .} \end{cases}$$

I posem $h_f(P) := h(g(P))$. Nosaltres utilitzem la funció parella $g(P) = x(P)/z(P)$.

Dues funcions parelles $f_1, f_2 \in \mathbb{Q}(E)$ dónen dues altures equivalents, en el sentit que la diferència $(\deg f_2)h_{f_1} - (\deg f_1)h_{f_2}$ està acotada sobre $E(\mathbb{Q})$ (veieu [SIL] §VIII 6.3).

Lema 4.15. *Per qualsevol $B \in \mathbb{R}$, el conjunt $\{P \in E(\mathbb{Q}) \mid h(P) < B\}$ és finit.*

Demostració. Està clar que el conjunt $\{P \in \mathbb{P}^1(\mathbb{Q}) \mid H(P) < e^B\}$ és finit (ja que hi ha finites possibilitats per a cada coordenada d'un representant primitiu de P). No obstant, per a cada punt $(x_0 : z_0) \in \mathbb{P}^1(\mathbb{Q})$ només hi ha dos possibles punts $(x_0 : y : z_0) \in E(\mathbb{Q})$ (gràcies a la forma de l'equació (3)). Per tant $\{P \in E(\mathbb{Q}) \mid H(P) < e^B\}$ és finit, d'on treiem el resultat tenint en compte que $H(P) > 0$ i aplicant logaritmes. □

Proposició 4.16. *Existeix una constant A tal que*

$$|h(2P) - 4h(P)| \leq A \quad \forall P \in E(\mathbb{Q}).$$

Demostració. Sigui $P = (x : y : z)$ i $2P = (x_2 : y_2 : z_2)$. Segons la fórmula de duplicació

$$(x_2 : z_2) = (F(x) : G(x))$$

amb

$$F(x) = (3x^2 + a)^2 - 8x(x^3 + ax + b)$$
$$G(x) = 4(x^3 + ab + b).$$

Definim ara els polinomis homogenis $F(X, Z) := Z^4 F(X/Z)$ i $G(X, Z) := Z^4 G(X/Z)$ de grau quatre. Com que $E/\mathbb{Q}$ és una corba el·líptica d'equació $y^2 z = x^3 + ax + b$, el polinomi $x^3 + ax + b$ i la seva derivada $3x^2 + a$ no tenen arrels en comú a $\mathbb{P}^1(\overline{\mathbb{Q}})$, per la qual cosa $F(X, 1)$ i $G(X, 1)$ tampoc no en tenen cap. És clar, analitzant el cas $Z = 0$, que $F(X, Z)$ i $G(X, Z)$ no tenen arrels en comú a $\mathbb{P}^1(\overline{\mathbb{Q}})$, i via la proposició 4.12 obtenim el resultat. □

Proposició 4.17. *Existeix com a molt una funció $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ satisfent les condicions següents:*

(a) $P \mapsto \hat{h}(P) - h(P)$ *és acotada a* $E(\mathbb{Q})$,

(b) $\hat{h}(2P) = 4\hat{(}h)(P)$.

Demostració. La primera condició ens permet trobar una constant B tal que

$$\left|\hat{h}(2^n P) - h(2^n P)\right| \leq B \quad \forall n \in \mathbb{N}.$$

Aplicant la segona condició,

$$\left|\hat{h}(P) - \frac{h(2^n P)}{4^n}\right| \leq \frac{B}{4^n},$$

i per tant, si $(\frac{h(2^n P)}{4^n})_n$ convergeix, ho fa cap a $\hat{h}(P)$. □

Lema 4.18. *Per tot $P \in E(\mathbb{Q})$, la successió $(h(2^n P)/4^n)_n$ és Cauchy a $\mathbb{R}$.*

Demostració. De la proposició 4.16 sabem que existeix una constant A tal que

$$|h(2P) - 4h(P)| \leq A \quad \forall P \in E(\mathbb{Q}).$$

Ara, per $N, M \in \mathbb{N}$ amb $N > M \geq 0$, i per tot $P \in E(\mathbb{Q})$ tenim

$$\begin{aligned}
\left|\frac{h(2^N P)}{4^N} - \frac{h(2^M P)}{4^M}\right| &= \left|\sum_{n=M}^{N-1} \frac{h(2^{n+1}P)}{4^{n+1}} - \frac{h(2^n P)}{4^n}\right| \\
&\overset{\text{desig.triang.}}{\leq} \sum_{n=M}^{N-1} \frac{1}{4^{n+1}} |h(2^{n+1}P) - 4h(2^n P)| \\
&\overset{\text{prop. 4.16}}{\leq} \sum_{n=M}^{N-1} \frac{1}{4^{n+1}} A \\
&\leq \frac{A}{4^{M+1}} \left(1 + \frac{1}{4} + \frac{1}{4^2} + \cdots\right) \\
&= \frac{A}{3 \cdot 4^M}
\end{aligned}$$

I per tant la successió $(h(2^n P)/4^n)_n$ és de Cauchy. □

Definició 4.19. L'**altura canònica** (o **de Néron-Tate**) a $E/\mathbb{Q}$, denotada per $\hat{h}$ o $\hat{h}_E$, és la funció $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ definida per

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h(2^n P)}{4^n}$$

Observació 4.20. Com hem notat a la observació 4.14, hi ha diverses maneres equivalents de definir h mitjançant funcions parelles. Totes elles indueixen també la mateixa funció d'altura canònica $\hat{h}$ (veieu [SIL] §VIII 9.1).

Teorema 4.21. *La funció $\hat{h}$ compleix les dues condicions de la proposició 4.17. A més:*

(a) *$\hat{h}(P) \geq 0$, i es té $\hat{h}(P) = 0$ si i només si P és un punt de torsió (i.e., P té ordre finit);*

(b) *Per tot $C \geq 0$, el conjunt $\{P \in E(\mathbb{Q}) \mid \hat{h}(P) \leq C\}$ és finit.*

Demostració. Si prenem $M = 0$ a la demostració del lema 4.18, tenim, per tot $N \geq 0$ i per tot $P \in E(\mathbb{Q})$,

$$\left| \frac{h(2^N P)}{4^N} - h(P) \right| \leq \frac{A}{3},$$

i fent tendir $N \to \infty$ obtenim la condició 4.17(a). La condició (b) es segueix de:

$$\hat{h}(2P) = \lim_{n\to\infty} \frac{h(2^{n+1}P)}{4^n} = 4 \cdot \lim_{n\to\infty} \frac{h(2^{n+1}P)}{4^{n+1}} = 4\hat{h}(P).$$

(a) Per definició $H(P) \geq 1$, d'on $h(P) \geq 0$ i per tant $\hat{h}(P) \geq 0$.

D'una banda, si P és de torsió, el conjunt $\{2^n P \mid n \geq 0\}$ és finit, per la qual cosa $\hat{h}$ hi està acotat per una constant $D \geq 0$. Gràcies a la condició 4.17(b) tenim, per a tot $n \in \mathbb{N}$ i $P \in E(\mathbb{Q})$

$$\hat{h}(P) = \hat{h}(2^n P)/4^n \leq D/4^n,$$

d'on obtenim $\hat{h}(P) = 0$.

D'altra banda, si $P \in E(\mathbb{Q})$ té ordre infinit, el conjunt $\{2^n P \mid n \geq 0\}$ és infinit i per tant $\hat{h}$ no hi està acotada (ja que, si ho estigués, tindríem una restricció sobre les coordenades d'un representant primitiu de P que ens restringiria a finites possibilitats per P). Aleshores, $\hat{h}(2^n P) > 1$ per algun n, i concluïm que $\hat{h}(P) = \hat{h}(2^n P)/4^n > 4^{-n} > 0$.

(b) Sabem gràcies a la condició 4.17(a) que, per tot $P \in E(\mathbb{Q})$, la diferència $\hat{h}(P) - h(P)$ està acotada superiorment per una constant $B \geq 0$, on $\hat{h}(P) \leq B + h(P)$. Com que, per tota constant $C \geq 0$ el conjunt $\{P \in E(\mathbb{Q}) \mid B + h(P) \leq C\}$ és finit, també ho és el conjunt de (b).

□

Lema 4.22. *Existeix una constant C tal que, per a tot $P_1, P_2 \in E(\mathbb{Q})$,*

$$|h(P_1 + P_2) + h(P_1 - P_2) - 2h(P_1) - 2h(P_2)| \leq C.$$

Demostració. Veieu [SIL] §VIII 6.2 . □

Lema 4.23. *L'altura de Néron-Tate satisfà la llei del paral·lelogram*

$$\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q).$$

Demostració. Prenent logaritmes al lema anterior, substituïm P i Q per 2^nP i 2^nQ, ho dividim tot per 4^n, i fem tendir $n\to\infty$, obtenim

$$\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q).$$

□

Proposició 4.24. *L'altura de Néron-Tate és una* **forma quadràtica**, *i.e., compleix* $\hat{h}(2P)=4\hat{h}(P)$ *per tot* $P\in E(\mathbb{Q})$, *i*

$$B(P,Q):=\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q)$$

és bi-additiva.

Demostració. Es deriva fàcilment del lema anterior (veieu [MIL] §IV 4.8). □

Definició 4.25. L'**aparellament canònic** (o **de Néron-Tate**) a $E/\mathbb{Q}$ és la forma bilineal

$$\langle\cdot,\cdot\rangle : E(\mathbb{Q})\times E(\mathbb{Q})\to\mathbb{R}$$

definida per

$$\langle P,Q\rangle := B(P,Q)=\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q).$$

Definició 4.26. Sigui $E_{\text{tors}}(\mathbb{Q})$ la part de torsió de $E(\mathbb{Q})$[13], i $P_1,\dots,P_r\in E(\mathbb{Q})$ representants de generadors de $E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$ [14]. El **regulador el·líptic** de $E/\mathbb{Q}$, denotat per $R_{E/\mathbb{Q}}$, vé donat per[15]

$$R_{E/\mathbb{Q}}=\begin{cases}\det((\langle P_i,P_j\rangle)_{1\le i,j\le r}) & r>0\\ 1 & r=0\end{cases} \tag{14}$$

[13] Veieu l'apartat 4.4 més a sota per detalls sobre $E_{\text{tors}}(\mathbb{Q})$.

[14] Ho podem fer gràcies al teorema 4.36 de mes avall.

[15] Es podria entendre com el volum d'un domini fonamental (com a concepte anàleg al definit a C.2) de $E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$, computat utilitzant la forma quadràtica $\hat{h}$. Es pot veure que està ben definit, i.e., que és independent de la tria de generadors $P_1,\dots,P_r$.

4.3 El diferencial invariant

Definició 4.27. Sigui E/k una corba el·líptica sobre un cos k. L'**espai de formes diferencials (meromorfes)** a E, denotat per Ω_E, és el $\overline{k}$-espai vectorial generat pels símbols de la forma dx per $x \in \overline{k}(E)$, subjectes a les relacions usuals:

(a) $d(\alpha+\beta) = d\alpha + d\beta$ per tot $\alpha, \beta \in \overline{k}(E)$;

(b) $d(\alpha\beta) = \alpha d\beta + \beta d\alpha$ per tot $\alpha, \beta \in \overline{k}(E)$;

(c) $da = 0$ per tot $a \in \overline{k}$.

Definició 4.28. Sigui E/k una corba el·líptica, i $P \in E(k)$ un punt. Una funció racional $u \in \overline{k}(E)$ amb $u(P) = 0$ s'anomena **uniformitzant** a P si per tot $r \in \overline{k}(E)^\times$ podem escriure

$$r = u^d \cdot s,$$

amb $d \in \mathbb{Z}$, i $s \in \overline{k}(E)$ finita a P amb $s(P) \neq 0$.

Exemple 4.29. Si $P = (a : b : 1) \in E(k)$ no té ordre dos, la funció $u(x, y) = x - a$ és un uniformitzant a P. En canvi, si P té ordre dos, un uniformitzant a P és $u(x, y) = y$. I si $P = O$, la funció $u(x, y) = x/y$ hi és un uniformitzant (cap d'aquests exemples és trivial de verificar).

Proposició 4.30. *Considerem E/k una corba el·líptica i $P \in E(k)$, i sigui $t \in \overline{k}(E)$ un uniformitzant a P.*

(a) *El diferencial dt és una $\overline{k}(E)$-base per Ω_E. És a dir, per tot $\omega \in \Omega_E$ existeix una única funció $g \in \overline{k}(E)$ (que depèn de ω i de t) satisfent*

$$\omega = g dt.$$

Denotem g per ω/dt.

(b) *Si $f \in \overline{k}(E)$ està definida a P, llavors df/dt també hi està.*

(c) *Sigui $\omega \in \Omega_E$ diferent de zero. La quantitat*

$$ord_P(\omega/dt)$$

depèn només de ω i P. L'anomenem **ordre** *de ω a P, i la denotem $ord_P(\omega)$.*

(d) *Siguin $x, f \in \overline{k}(E)$ amb $x(P) = 0$, i suposem que $char(k) = 0$. Llavors,*

$$ord_P(fdx) = ord_P(f) + ord_P(x) - 1.$$

(e) *Sigui $\omega \in \Omega_E$ amb $\omega \neq 0$. Llavors, per tot $P \in E(k)$ llevat d'un nombre finit,*

$$ord_P(\omega) = 0.$$

Demostració. Veieu [SIL] §II 4.3. □

Definició 4.31. Sigui $\omega \in \Omega_E$. El **divisor associat a** ω és

$$\mathrm{div}(\omega) = \sum_{P \in E} \mathrm{ord}_P(\omega)[P] \in \mathrm{Div}(C).$$

A més, diem que el diferencial $\omega \in \Omega_E$ és **regular** (o **holomorf**) si

$$\mathrm{ord}_P(\omega) \geq 0 \quad \text{per tot } P \in E(k),$$

i diem que **no s'anul·la** si

$$\mathrm{ord}_P(\omega) \leq 0 \quad \text{per tot } P \in E(k).$$

Tot seguit definim un diferencial d'importància cabdal en l'estudi de les corbes el·líptiques, i en destaquem un parell de propietats.

Definició 4.32. Sigui E/k una corba el·líptica donada en la forma estàndard (1). El **diferencial invariant** associat a la forma normal $F(x, y) = 0$, denotat per ω, vé donat per

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$

Proposició 4.33. *El diferencial invariant ω definit a 4.32 és holomorf i no s'anul·la (i.e., $div(\omega) = 0$).*

A més, donada qualsevol translació a $E(k)$ de la forma $\tau_Q(P) = P+Q$ (amb $Q \in E(k)$), el diferencial ω és invariant per τ_Q, i.e.,

$$\tau_Q(\omega) = \omega.$$

Demostració. [SIL] §III 1.5, §III 5.1 . □

Definició 4.34. Donada una corba el·líptica $E/\mathbb{Q}$, definim la quantitat

$$\Omega^+ = \int_{E(\mathbb{R})} |\omega|,$$

que és conjecturalment transcendent sobre $\mathbb{Q}$.

Observació 4.35. Tenim que Ω^+ és, o bé el període real (quan $E(\mathbb{R})$ és connex), o bé el doble del període real (quan $E(\mathbb{R})$ té dues components connexes).

4.4 El grup $E(\mathbb{Q})$ i el teorema de Mordell-Weil

Teorema de Mordell-Weil sobre $\mathbb{Q}$

Teorema (Mordell-Weil) 4.36. *Sigui $E/\mathbb{Q}$ una corba el·líptica. El grup $E(\mathbb{Q})$ és finitament generat.*

Demostració. Prenem $Q_1, \ldots, Q_n \in E(\mathbb{Q})$ un conjunt finit (en virtut del teorema 4.10) de representants per les classes de $E(\mathbb{Q})/2E(\mathbb{Q})$, i considerem $C = \max_{1 \leq i \leq n} \hat{h}(Q_i)$. Afirmem que el conjunt següent genera $E(\mathbb{Q})$:

$$S := \{P \in E(\mathbb{Q}) \ \mid \ \hat{h}(P) \leq C\}.$$

Per reducció a l'absurd, suposem que existeix un punt $P \in E(\mathbb{Q})$ que no està al subgrup generat per S. Recordem que $\hat{h}$ pren valors discrets (ja que pren finits valors a qualsevol interval $[0, c]$, pel teorema 4.21(a)), i per tant podem triar P tal que $\hat{h}(P)$ sigui mínim.

Ara, per la definició de S, existeix un $Q_i \in S$ tal que $P = Q_i + 2R$ per algun $R \in E(\mathbb{Q})$. Clarament, R no pot estar al subgrup generat per S, i aleshores $\hat{h}(R) \geq \hat{h}(P)$. Per tant, per la regla del paral·lelogram i per les propietats que hem donat de $\hat{h}$,

$$\begin{aligned} 2\hat{h}(Q_i) &= \hat{h}(Q_i + P) + \hat{h}(Q_i - P) - 2\hat{h}(P) \\ &\geq 0 + \hat{h}(2R) - 2\hat{h}(P) \\ &= 4\hat{h}(R) - 2\hat{h}(P) \\ &\geq 2\hat{h}(P), \end{aligned}$$

que és una contradicció, ja que $Q_i \in \langle S \rangle$ (és a dir, $\hat{h}(Q_i) \leq C$) i per contra $P \notin \langle S \rangle$ (ja que $\hat{h}(P) > C$). □

Observació 4.37. Trobar un mètode efectiu que computi (en general i en un nombre finit de passos) una base per $E(\mathbb{Q})$ és encara un problema obert, que es resoldria demostrant la conjectura 4.7 o la conjectura 4.54.

Observació 4.38. Gràcies al teorema de Mordell-Weil podem aplicar el teorema fonamental dels grups abelians finitament generats per obtenir una descomposició en suma directa

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

on la part de torsió $E(\mathbb{Q})_{\text{tors}}$ és la suma directa de grups cíclics (d'ordre certes potències de primers).

Definició 4.39. Amb les notacions de la observació anterior, anomenem **rang** (algebraic) del grup de Mordell-Weil $E(\mathbb{Q})$ (o de E) a la quantitat r, i denotem $\text{rang}(E(\mathbb{Q}))$.

De fet, una de les fites més remarcables de la conjectura de Birch i Swinnerton-Dyer és l'obtenció d'una relació entre el rang de E i altres conceptes definits en aquest treball. A la resta de l'apartat veiem que descriure la part de torsió de $E(\mathbb{Q})$ és factible, i donem les diverses eines que permeten fer-ho.

Punts de torsió de $E(\mathbb{Q})$

En aquest apartat ens ocupem de descriure breument els possibles subgrups de torsió $E(\mathbb{Q})_{\text{tors}}$ del grup de Mordell-Weil $E(\mathbb{Q})$ per $E/\mathbb{Q}$.

Teorema (Lutz-Nagell) 4.40. *Si $P = (x : y : 1) \in E(\mathbb{Q})_{tors}$, llavors $x, y \in \mathbb{Z}$ i es té que $y = 0$ o $y \mid \Delta$.*

Demostració. Si x o $y \notin \mathbb{Z}$, fixem p un primer tal que $\mathrm{ord}_p(x)$ o $\mathrm{ord}_p(y) < 0$. Si pensem $P = (x : y : 1) \in E(\mathbb{Q}_p)_{\mathrm{tors}}$, llavors es té que x o y no pertanyen a $\mathbb{Z}_p$ per aquest primer p que hem fixat, i qualssevol coordenades primitives compliran $z(P) \in p\mathbb{Z}_p$. Reduïnt P mòdul p obtenim $z(\overline{P}) = 0$, i l'únic punt de $\overline{E}(\mathbb{F}_p)$ d'aquesta forma és $(0 : 1 : 0)$. Hem demostrat, doncs, que x o $y \notin \mathbb{Z}$ implica $P = (x : y : 1) \in E^1(\mathbb{Q}_p)$. Com que $E^1(\mathbb{Q}_p)$ és lliure de torsió (teorema 3.23), obtenim que $P = (x : y : 1) \in E(\mathbb{Q}_p)_{\mathrm{tors}}$ implica $x, y \in \mathbb{Z}$.

Ara, si $x, y \in \mathbb{Z}$, P i $2P$ tenen coordenades enteres per la fórmula d'addició, i pel lema següent finalitzem. □

Lema 4.41. *Sigui $P = (x_1 : y_1 : 1) \in E(\mathbb{Q})$. Si P, $2P$ tenen coordenades enteres (imposant $z_1 = 1$), o bé $y_1 = 0$ o bé $y_1 \mid \Delta$.*

Demostració. Suposem $y_1 \neq 0$, i escrivim $2P = (x_2 : y_2 : 1)$. Si la projecció afí de E vé definida per $Y^2 = X^3 + aX + b =: f(X)$, la recta tangent a E al punt P és $Y = \alpha X + \beta$, on $\alpha = \frac{f'(x_1)}{2y_1}$, i per tant la primera coordenada de $2P$ compleix

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

Això ens diu, doncs, que $\alpha^2 = 2x_1 + x_2 \in \mathbb{Z}$ (per hipòtesi), i aleshores $\alpha, \alpha^2 \in \mathbb{Z}$. En conclusió, per la definició de α veiem que $y_1 \mid f'(x_1)$, i com que $y_1^2 = f(x_1)$ tenim que $y_1 \mid f'(x_1)$. Ara, com que $\mathrm{Res}(f, f') = (-1)^{\deg(f)(\deg(f)-1)/2}\Delta = -\Delta$, la teoria de resultants ens diu

$$\exists r(X), s(X) \in \mathbb{Z}[X] \ \mid \ -\Delta = r(X)f(X) + s(X)f'(X),$$

per tant $y_1 \mid \Delta$. □

Observació 4.42. Notem que el teorema de Lutz-Nagell dóna una llista finita de candidats a elements de torsió, ja que per a cada $y \mid \Delta$ o $y = 0$ la coordenada x compleix $x^3+ax+b-y^2 = 0$ (per tant, divideix $b - y^2$).

Tot i això ens podem trobar amb que tots els múltiples consecutius tenen coordenades enteres i cap es repeteix. Necessitem un resultat que acoti l'ordre del grup, com és el següent.

Corol·lari 4.43. *Si $E(\mathbb{Q})$ té bona reducció a p, l'aplicació de reducció*

$$E(\mathbb{Q})_{tors} \hookrightarrow \overline{E}(\mathbb{F}_p)$$

és injectiva.

Demostració. Com que E té bona reducció, $E^0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$. El morfisme de reducció $E(\mathbb{Q}_p) \to \overline{E}(\mathbb{F}_p)$ té nucli $E^1(\mathbb{Q}_p)$, que són els punts P amb $x(P), z(P) \in p\mathbb{Z}_p$ i $y(P) \in \mathbb{Z}_p^\times$. Per la demostració del teorema de Lutz-Nagell, $E^1(\mathbb{Q}_p) \cap E(\mathbb{Q})_{\text{tors}} = \{O\}$. □

Observació 4.44. La hipòtesi de Riemann (veieu l'apartat 4.6) ens dóna en particular una cota superior pel cardinal de $\overline{E}(\mathbb{F}_p)$.

Durant tot l'apartat hem desenvolupat un algorisme per trobar punts de torsió i una restricció sobre la mida del subgrup de torsió. La caracterització definitiva dels subgrups de torsió sobre $\mathbb{Q}$, però, vé donada pel següent teorema (conjecturat per Levi el 1906 i demostrat per Mazur el 1975):

Teorema 4.45 (Mazur)**.** *Sigui E una corba el·líptica sobre $\mathbb{Q}$. El subgrup de torsió $E(\mathbb{Q})_{tors}$ de $E(\mathbb{Q})$ és isomorf a un dels quinze grups següents:*

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} \qquad & amb \quad 1 \leq N \leq 10 \ o \ N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad & amb \quad 1 \leq N \leq 4. \end{aligned}$$

A més, cada un d'aquests grups és subgrup de torsió d'alguna corba el·líptica sobre $\mathbb{Q}$.

Demostració. Podeu trobar la demostració a [MAZ]. □

Observació 4.46. Pel cas d'una extensió finita de $\mathbb{Q}$ hi ha resultats per cossos cúbics (consulteu [JKS]), i existeix un resultat general que acota l'ordre del subgrup de torsió respecte al grau del cos de nombres on E està definit (veieu [MER]).

4.5 Sobre el rang de $E(\mathbb{Q})$

Com hem vist, podem considerar la descomposició del grup de Mordell-Weil d'una corba el·líptica

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

i ja som capaços de descriure'n efectivament la part de torsió en un nombre finit de passos. Per acabar de computar el grup $E(\mathbb{Q})$ ens resta trobar el rang r (o millor, una base de $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$). Tot seguit discutim aquest problema.

Conjectura 4.47 (del rang)**.** *Donat $n \in \mathbb{N}$, existeix una corba el·líptica $E/\mathbb{Q}$ amb rang$(E) > n$.*

Observació 4.48. La corba el·líptica $E/\mathbb{Q}$ de rang més gran coneguda actualment (consulteu `http://web.math.hr/~duje/tors/rankhist.html`). té rang superior a 28, i és deguda a Elkies.

Observació 4.49. La conjectura és provada per Ulmer per $E/\mathbb{F}_q(T)$ (on $\mathbb{F}_q(T)$ és el cos de fraccions de l'anell de polinomis en la variable T a coeficients al cos finit $\mathbb{F}_q$) l'any 2010.

Observació 4.50. Utilitzant la successió exacta (10):

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S^{(2)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})_2 \to 0,$$

podem donar una cota superior per r utilitzant el cardinal de $S^{(2)}(E/\mathbb{Q})$ (i $Ш(E/\mathbb{Q})_2$ ens dóna un error aproximat).

Observem que

$$(E_{tors} \oplus \mathbb{Z}^r)/2(E_{tors} \oplus \mathbb{Z}^r) = E_{tors}/2E_{tors} \oplus \mathbb{Z}^r/2\mathbb{Z}^r \subseteq S^{(2)}.$$

Atès que $\#(\mathbb{Z}^r/2\mathbb{Z}^r) = 2^r$, això implica que $\#S^{(2)} \geq 2^r \cdot \#(E_{tors}/2E_{tors})$, i obtenim la cota $r \leq \frac{\log((\#S^{(2)})/(\#(E_{tors}/2E_{tors})))}{\log(2)}$.

A partir dela successió exacta (10) podem construïr un diagrama commutatiu (on les

fletxes horitzontals formen successions exactes)

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/2E(\mathbb{Q}) & \xrightarrow{\delta} & S^{(2)}(E/\mathbb{Q}) & \xrightarrow{\text{incl}_\circ} & Ш(E/\mathbb{Q})_2 & \longrightarrow & 0 \\
 & & \text{proj}\uparrow & & \cdot 2\uparrow & & \cdot 2\uparrow & & \\
0 & \longrightarrow & E(\mathbb{Q})/4E(\mathbb{Q}) & \xrightarrow{\delta} & S^{(4)}(E/\mathbb{Q}) & \xrightarrow{\text{incl}_\circ} & Ш(E/\mathbb{Q})_4 & \longrightarrow & 0 \\
 & & \text{proj}\uparrow & & \cdot 2\uparrow & & \cdot 2\uparrow & & \\
 & & \vdots & & \vdots & & \vdots & & \\
 & & \text{proj}\uparrow & & \cdot 2\uparrow & & \cdot 2\uparrow & & \\
0 & \longrightarrow & E(\mathbb{Q})/2^nE(\mathbb{Q}) & \xrightarrow{\delta} & S^{(2^n)}(E/\mathbb{Q}) & \xrightarrow{\text{incl}_\circ} & Ш(E/\mathbb{Q})_{2^n} & \longrightarrow & 0
\end{array}$$

Definició 4.51. Denotem $S^{(2,n)}(E/\mathbb{Q})$ com la imatge de $S^{(2^n)}(E/\mathbb{Q})$ dins de $S^2(E/\mathbb{Q})$ (i.e., com $2^{n-1}S^{2n}(E/\mathbb{Q})$).

Proposició 4.52. *El grup $E(\mathbb{Q})/2E(\mathbb{Q})$ està contingut a $\cup_n S^{(2,n)}(E/\mathbb{Q})$. A més, si no existeix cap element no nul de $Ш(E/\mathbb{Q})$ divisible per totes les potències de 2, llavors tenim igualtat .*

Demostració. Com que les projeccions (que són les naturals de pas a quocient) són exhaustives, la imatge de $E(\mathbb{Q})/2E(\mathbb{Q})$ a $S^{(2)}(E/\mathbb{Q})$ és igual a la imatge de $E(\mathbb{Q})/2^nE(\mathbb{Q})$, que està continguda dins de $S^{(2,n)}(E/\mathbb{Q})$ per la commutativitat del diagrama.

Recíprocament, sigui $\gamma \in \cup_n S^{(2,n)}(E/\mathbb{Q})$, de manera que per a cada n existeix un element $\gamma_n \in S^{(2n)}(E/\mathbb{Q})$ que s'aplica a γ. Sigui δ_n la imatge de γ_n a $Ш(E/\mathbb{Q})_{2^n}$. Llavors, per la commutativitat del diagrama, $2^{n-1}\delta_n = \delta_1$ per tot n, i δ_1 és divisible per totes les potències de dos. Utilitzant l'exactitud de la primera successió horitzontal, veiem que γ pertany a la imatge de $E(\mathbb{Q})/2E(\mathbb{Q})$ si i només si $\delta_1 = 0$, que és el que buscavem. □

Lema 4.53. *Suposem que no existeix un element no nul de $Ш(E/\mathbb{Q})$ divisible per tota potència de 2. Llavors la component 2-primària[16] de $Ш(E/\mathbb{Q})$ és finita.*

[16]Sigui G un grup abelià finit, i $p \in \mathbb{N}$ un primer. La component p-primària de G és el subgrup de tots els elements d'ordre una potència de p.

Sota l'assumpció que $Ш(E/\mathbb{Q})$ és finit, parlem de component p-primària. Fora d'aquesta assumpció, el mateix paper el prèn el p-subgrup de Sylow (únic pel tercer teorema de Sylow utilitzant la commutativitat de $Ш(E/\mathbb{Q})$).

Demostració. Atès que, per tot $m \in \mathbb{N}\backslash\{0\}$, $Ш(E/\mathbb{Q})_{2^m} \subseteq Ш(E/\mathbb{Q})_{2^{m+1}}$, i que $Ш(E/\mathbb{Q})_{2^m}$ és finit (utilitzant la successió exacta (10) i el teorema 4.9), podem assegurar que

$$\text{Component 2-primària de } Ш(E/\mathbb{Q}) = \cup_{m\in\mathbb{N}\backslash\{0\}} Ш(E/\mathbb{Q})_{2^m}.$$

Demostrem el contrarrecíproc. Suposem que la component 2-primària de $Ш(E/\mathbb{Q})$ no és finita. Per la observació anterior podem triar una successió (n_i) (de nombres naturals no nuls estrictament creixent) tal que la següent cadena és estricta, no estabilitza, i $Ш(E/\mathbb{Q})_{2^{n_k-1}} \subset Ш(E/\mathbb{Q})_{2^{n_k}}$:

$$Ш(E/\mathbb{Q})_2 \subset Ш(E/\mathbb{Q})_{2^{n_1}} \subset Ш(E/\mathbb{Q})_{2^{n_2}} \subset \cdots .$$

Denotem $Ш_1 := Ш(E/\mathbb{Q})_2$ i $Ш_i = Ш(E/\mathbb{Q})_{2^{n_{i-1}}}$. Ara, veiem que per tot $\alpha_i \in Ш_i - Ш_{i-1}$ tenim $2^{n_i}\alpha_i = 0$ però $2^{n_i-1}\alpha_i \neq 0$, és a dir, $2^{n_i-1}\alpha_i \in Ш_1$ és divisible per 2^{n_i-k} amb $k = 1, \ldots, n_i - 1$. Fent el mateix amb i arbitrariament gran, trobem elements de $Ш_1$ divisibles per potències de 2 cada cop més grans, i tenint en compte que $Ш_1$ és finit concluïm que existeix un element no nul de $Ш(E/\mathbb{Q})$ divisible per tota potència de 2. □

Conjectura 4.54. *No existeix cap element no nul de* $Ш(E/\mathbb{Q})$ *divisible per tota potència de* 2.[17]

Sota la conjectura anterior, qualsevol cadena com la de la demostració del lema anterior estabilitza, i podem trobar un $n_0 \in \mathbb{N}$ de manera que $2^{n_0-1}Ш(E/\mathbb{Q})_{2^{n_0}} = 0$. Aleshores, observant que δ esdevenen epimorfismes per tot índex superior a n_0, i que les projeccions són exhaustives, tenim

$$S^{(2,n_0)}(E/\mathbb{Q}) = S^{(2,n_0+1)}(E/\mathbb{Q}) = \cdots \cong E(\mathbb{Q})/2E(\mathbb{Q}).$$

Observació 4.55. Aquest fet dóna un algorisme (degut a Mazur) per trobar un conjunt de generadors de $E(\mathbb{Q})$ en un nombre finit de passos. Per $n \in \mathbb{N}$, denotem $T(n)$ com el subgrup

$$T(n) = \langle \{P \in E(\mathbb{Q}) \mid h(P) \leq 10^n\} \rangle .$$

[17] Aquesta conjectura és més dèbil que la conjectura 4.7.

Primer calculem $T(1)$ i $S^{(2)}(E/\mathbb{Q})$ (computable per [SIL]§X.4.5). Si $T(1) \xrightarrow{\delta} S^{(2)}(E/\mathbb{Q})$ és epimorfisme, $T(1)$ genera $E(\mathbb{Q})/2E(\mathbb{Q})$.

Si no, calculem $T(2)$, $S^{(2^2)}(E/\mathbb{Q})$ i $S^{(2,2)}(E/\mathbb{Q})$. Si la imatge de $T(2) \xrightarrow{\delta} S^{(2^2)}(E/\mathbb{Q})$ és $S^{(2,2)}(E/\mathbb{Q})$, $T(2)$ genera $E(\mathbb{Q})/2E(\mathbb{Q})$.

Si no, calculem $T(3)$, $S^{(2^3)}(E/\mathbb{Q})$ i $S^{(2,3)}(E/\mathbb{Q})$, i procedim com en el pas anterior. Aquest mètode acabarà quan arribem a l'índex n_0 anterior. Després de trobar un conjunt de generadors de $E(\mathbb{Q})/2E(\mathbb{Q})$, la demostració de 4.36 ens habilita per computar un conjunt de generadors de $E(\mathbb{Q})$.

La següent proposició ens permet calcular el rang r d'algunes corbes el·líptiques (per exemples, veieu [MIL] §IV 5.7).

Proposició 4.56. (*a*) *El rang r de $E(\mathbb{Q})$ satisfà la desigualtat*

$$r \leq 2 \cdot \#\{p \text{ primer } \mid p \text{ divideix } 2\Delta\}.$$

(*b*) *Sigui*

$$t_1 = \#\{p \text{ primer } \mid p \text{ divideix a } \Delta \text{ i } E \text{ té reducció nodal a } p\},$$
$$t_2 = \#\{p \text{ primer } \mid p \text{ divideix a } \Delta \text{ i } E \text{ té reducció cuspidal a } p\}.$$

Llavors, el rang r de $E(\mathbb{Q})$ satisfà la desigualtat

$$r \leq t_1 + 2t_2 - 1.$$

Demostració. Consulteu [MIL] §IV 5.5, 5.6. □

Observació 4.57. Observem que, si sabem computar el rang r de $E(\mathbb{Q})$, també sabem trobar un conjunt de generadors de $E(\mathbb{Q})$.

Després de calcular $s = \dim E(\mathbb{Q})/2E(\mathbb{Q}) = 2^r \cdot \dim E_{\text{tors}}(\mathbb{Q})/2E_{\text{tors}}(\mathbb{Q})$, comencem a buscar punts $P_i \in E(\mathbb{Q})$ (ordenats, per exemple, per altura). Per cada P_i, examinem si $P_i = 2Q$ per algun $Q \in E(\mathbb{Q})$ (resolent la fórmula de duplicació). Si és el cas, substituïm P_i per Q i ho repetim. Aquest procés s'acabarà ja que $E(\mathbb{Q})$ és finitament generat, i n'obtenim un conjunt de punts que no són el doble de cap altre punt.

Examinant si cada un d'aquests punts defineix una classe independent a les de la resta de punts a $E(\mathbb{Q})/2E(\mathbb{Q})$, aconseguim un conjunt de representants P_i del grup $E(\mathbb{Q})/2E(\mathbb{Q})$. Si agafem prou punts, tard o d'hora obtenim s representants de classes diferents, i la demostració de 4.36 ens faculta per calcular un conjunt de generadors de $E(\mathbb{Q})$.

4.6 Funcions zeta

Funcions zeta de cossos de nombres

Recordem que la funció **zeta de Riemann** es pot definir, de maneres equivalents, com

$$\zeta(s) = \prod_{p \text{ primer}} \frac{1}{1-p^{-s}} = \sum_{n\geq 1} n^{-s}, \quad s \in \mathbb{C}, \quad \mathrm{Re}(s) = 1. \tag{15}$$

Observació 4.58. Tant la suma com el producte a (15) convergeixen per $\mathrm{Re}(s) > 1$, així que $\zeta(s)$ és holomorfa i no nul·la al semipla $\mathrm{Re}(s) > 1$. A més, $\zeta(s)$ admet una continuació analítica a $\mathbb{C}$, i té un pol simple a $s = 1$. I gràcies a la igualtat $\zeta(1-n) = -B_n/n$[18]. (per tot $n \in \mathbb{N}\backslash\{0\}$), veiem que ζ té un zeros a $-2n$ per tot $n \in \mathbb{N}\backslash\{0\}$ (aquests zeros s'anomenen **zeros trivials** de ζ).

Conjectura 4.59 (Hipòtesi de Riemann)**.** *Tots els zeros no trivials de ζ són dins la recta $Re(s) = \frac{1}{2}$.*

Definició 4.60 (Dedekind)**.** Sigui K un cos de nombres (i.e., una extensió finita de $\mathbb{Q}$). Definim la funció zeta de Dedekind d'un cos de nombres K com:

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p}\subset\mathcal{O}_K \text{ ideal} \\ \text{primer no nul.}}} \frac{1}{1-N(\mathfrak{p})^{-s}} = \sum_{\substack{\mathfrak{a}\subset\mathcal{O}_K \\ \text{ideal no nul.}}} N(\mathfrak{a})^{-s},$$

on $\mathcal{O}_K$ designa la **clausura integral de $\mathbb{Z}$ a K** (i.e., les arrels a K dels polinomis mònics a coeficients a $\mathbb{Z}$, altrament anomenada l'**anell d'enters** de K), i la **norma numèrica** $N(\mathfrak{a})$ és l'ordre de l'anell $\mathcal{O}_K/\mathfrak{a}$.

[18] B_n denota l'n-èssim **nombre de Bernoulli**, on

$$B_m = 1 - \sum_{k=0}^{m-1} \binom{m}{k} \frac{B_k}{m-k+1}, \quad B_0 = 1.$$

Notem que els nombres de Bernouilli s'anul·len per $n > 1$ senar.

Observació 4.61. La segona igualtat de la definició és certa gràcies a la factorització única d'ideals per ideals primers (ja que $\mathcal{O}_K$ és un domini de Dedekind).

Per qualsevol K, la funció ζ_K admet una continuació analítica a $\mathbb{C}$, i té un pol simple a $s = 1$. A més també es conjectura que els zeros no trivials de ζ_K són tots a $\mathrm{Re}(s) = \frac{1}{2}$ (hipòtesi de Riemann generalitzada).

Si prenem $K = \mathbb{Q}$, recuperem la funció zeta de Riemann original.

Funcions zeta de corbes afins sobre cossos finits

Considerem una corba plana afí no-singular

$$C/\mathbb{F}_p : f(X, Y) = 0,$$

i denotem el seu anell de coordenades per

$$\mathbb{F}_p[x, y] := \mathbb{F}_p[C] = \mathbb{F}_p[X, Y]/(f(X, Y))$$

Definició 4.62. Paral·lelament a l'apartat anterior, definim la **funció zeta** de C com

$$\zeta(C, s) = \prod_{\substack{\mathfrak{p} \subset \mathbb{F}_p[x,y] \\ \text{ideal primer no nul.}}} \frac{1}{1 - N(\mathfrak{p})^{-s}},$$

on $N(\mathfrak{p})$ denota l'ordre de $\mathbb{F}_p[x, y]/\mathfrak{p}$.

Definició 4.63. Tenint en compte que $\mathbb{F}_p[x, y]/\mathfrak{p}$ és una extensió finita de $\mathbb{F}_p$[19], definim el **grau de** $\mathfrak{p}$, $\deg \mathfrak{p}$, com el grau d'aquesta extensió.

A partir d'això, està clar que $N(\mathfrak{p}) = p^{\deg \mathfrak{p}}$ és finit.

Definició 4.64. Definim la següent **funció zeta (majúscula)** de C com

$$Z(C, T) = \prod_{\substack{\mathfrak{p} \subset \mathbb{F}_p[x,y] \\ \text{ideal primer no nul.}}} \frac{1}{1 - T^{\deg \mathfrak{p}}}.$$

Observació 4.65. Per definició tenim $\zeta(C, s) = Z(C, p^{-s})$.

[19] No és trivial; per veure-ho s'utilitza que $\dim_{\mathrm{Krull}}(k[C]) = 1$, juntament amb el Nullstellensatz dèbil.

Proposició 4.66. *Les igualtats següents es compleixen*

$$\log Z(C,T) = \sum_{m\geq 1} N_m \frac{T^m}{m}, \qquad on\ N_m := \#C(\mathbb{F}_{p^m}),$$
$$Z(C,T) = \exp\left(\sum_{m\geq 1} N_m \frac{T^m}{m}\right).$$

Demostració. Notem que aplicant logaritmes a $Z(C,T)$ i derivant respecte T tenim

$$\begin{aligned}\frac{Z'(C,T)}{Z(C,T)} &= \sum_{\mathfrak{p}} \frac{\deg \mathfrak{p}\cdot T^{\deg \mathfrak{p}-1}}{1-T^{\deg \mathfrak{p}}} \\ &= \sum_{\mathfrak{p}}\sum_{n\geq 0} \deg \mathfrak{p}\cdot T^{(n+1)\deg \mathfrak{p}-1}.\end{aligned}$$

.

En aquesta sèrie de potències, el coeficient de T^{m-1} és $\sum \deg \mathfrak{p}$ on $\mathfrak{p}$ recorre els ideals primers (maximals, ja que es pot veure que $\mathbb{F}_p[x,y]$ té dimensió de Krull 1) no nuls de $\mathbb{F}_p[x,y] = \mathbb{F}_p[X,Y]/(f(X,Y))$ tals que $\deg \mathfrak{p}$ divideix m. Mitjançant el lema [FT] §4 22 tenim una inclusió $\mathbb{F}_p[x,y] \hookrightarrow \mathbb{F}_{p^m}$. De fet, hi haurà exactament $\deg \mathfrak{p}$ homomorfismes d'aquest tipus atès que $\mathbb{F}_p[x,y]/\mathfrak{p}$ és separable sobre $\mathbb{F}_p$. Recíprocament, tot homomorfisme $\mathbb{F}_p[x,y] \to \mathbb{F}_{p^m}$ factoritza a $\mathbb{F}_p[x,y]/\mathfrak{p}$ per algun ideal amb $\deg \mathfrak{p} \mid m$ (utilitzant, per exemple, el primer teorema d'isomorfia i [FT] §4 22 per trobar l'únic al qual factoritza amb un morfisme injectiu). Per tant, el coeficient de T^{m-1} és el nombre d'homomorfismes

$$\mathbb{F}_p[x,y] \to \mathbb{F}_{p^m}.$$

Però un tal homomorfisme vé determinat per les seves imatges a, b de x i y, i recíprocament l'homomorfisme $P(X,Y) \mapsto P(a,b) : \mathbb{F}_p[X,Y] \to \mathbb{F}_{p^m}$ factoritza a $\mathbb{F}_p[x,y]$ si i només si $f(a,b) = 0$. Per tant, hem establert una correspondència bijectiva

$$\mathrm{Hom}(\mathbb{F}_p[x,y], \mathbb{F}_{p^m}) \overset{1:1}{\leftrightarrow} C(\mathbb{F}_{p^m}).$$

D'on obtenim

$$\frac{Z'(C,T)}{Z(C,T)} = \sum_{m\geq 0} N_m T^{m-1},$$

i integrant respecte T obtenim la primera igualtat. La segona és directa aplicant l'exponencial (que es defineix dins tot anell commutatiu mitjançant el desenvolupament de Taylor). □

Funcions zeta de corbes projectives sobre cossos finits

Amb l'esperit de la darrera proposició, plantegem la següent

Definició 4.67. Donada una corba plana projectiva no-singular C, definim

$$Z(C,T) := \exp\left(\sum_{m\geq 1} N_m \frac{T^m}{m}\right), \quad \text{on } N_m := \#C(\mathbb{F}_{p^m}),$$
$$\zeta(C,s) := Z(C,p^{-s}).$$

Observació 4.68. Sigui E una corba el·líptica, i E^{aff} la seva projecció afí $E \cap \{Z \neq 0\}$. Com que $\#E(\mathbb{F}_{p^m}) = \#E^{\text{aff}}(\mathbb{F}_{p^m}) + 1$, trobem

$$Z(E,T) = \frac{1}{1-T} Z(E^{\text{aff}}, T).$$

Per simplificar l'expressió de $Z(E,T)$ utilitzem

Proposició 4.69. *A una corba el·líptica $E/\mathbb{F}_p$, hi ha exactament*

$$\#E(\mathbb{F}_p)\frac{p^m-1}{p-1}$$

divisors positius de grau m per tot $m \geq 1$.

Demostració. Consulteu [MIL] §IV 9.9 (a la prova, $\mathfrak{p}_\infty$ representa l'ideal associat al punt O de E). □

Teorema 4.70. *Sigui $E(a,b)/\mathbb{F}_p$ una corba el·líptica donada per una equació de Weierstrass* (3)*. Llavors*

$$Z(E,T) = \frac{1 + (N_1 - p - 1)T + pT^2}{(1-T)(1-pT)}, \quad \textit{amb } N_1 = \#E(\mathbb{F}_p).$$

Demostració. Observem

$$Z(E,T) = \frac{1}{1-T} Z(E^{\text{aff}}, T) = \frac{1}{1-T} \prod_{\substack{\mathfrak{p} \subset \mathbb{F}_p[x,y] ideal \\ \text{primer no nul.}}} \frac{1}{1-T^{\deg \mathfrak{p}}},$$

on $\mathbb{F}_p[x,y] := \mathbb{F}_p[C] = \mathbb{F}_p[X,Y]/(Y^2 - X^3 - aX - b)$. Tot seguit, observem que el coeficient de T^m al producte anterior és el nombre de $c_i \in \mathbb{N} \cup \{0\}$ tals que $c_0 + \sum_{i|\mathfrak{p}_i \neq \{0\}} c_i \deg \mathfrak{p}_i = m$, que és el nombre d_m de divisors positius de grau m a $E/\mathbb{F}_p$ (per la definició de divisor principal d'una corba sobre un cos perfecte no-algebraicament tancat), amb la convenció que $d_0 = 1$. Per això mateix, quan desenvolupem el productori anterior, trobem una expressió

$$Z(E,T) = \sum_{m \geq 0} d_m T^m,$$

i concluïm amb el resultat mitjançant la proposició 4.69. □

Observació 4.71. Suposem que coneixem N_1. Llavors podem trobar $\alpha, \beta \in \overline{\mathbb{Q}}$ tals que

$$1 + (N_1 - p - 1)T + pT^2 = (1 - \alpha T)(1 - \beta T)$$

i per l'expressió de l'últim teorema, tenim

$$\log Z(E,T) = \log \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-pT)} = \sum_{m>0} (1 + p^m - \alpha^m - \beta^m) \frac{T^m}{m}, \tag{16}$$

on la segona igualtat surt del desenvolupament de Taylor de $\log(1-T)$. Això dóna un mètode per computar les quantitats $N_i(E) = \#E(\mathbb{F}_{p^i})$ per tot $i \in \mathbb{N}$, ja que

$$N_m(E) = 1 + p^m - \alpha^m - \beta^m.$$

La Hipòtesi de Riemann per a $E(\mathbb{F}_p)$

D'ara en endavant, denotem (en contradicció amb els apartats anteriors)

$$N_p = \#E(\mathbb{F}_p),$$

on E és una corba el·líptica sobre $\mathbb{F}_p$.

Teorema 4.72 (Hipòtesi de Riemann per a corbes el·líptiques $E/\mathbb{F}_p$)**.** *Sigui E una corba el·líptica sobre $\mathbb{F}_p$. Llavors, tots els zeros de la funció $\zeta(E,s)$ tenen part real $\frac{1}{2}$, el que equival a*

$$|N_p - p - 1| \leq 2\sqrt{p}.^{20}$$

Demostració. Donem una prova de l'equivalència. Podeu consultar la resta de la demostració a [MIL]§IV 9.4 (exigeix una bona comprensió del mòdul de Tate).

De (16) tenim

$$\zeta(E,s) = \frac{(1-\alpha p^{-s})(1-\beta p^{-s})}{(1-p^{-s})(1-p^{1-s})}.$$

Té pols simples a $s = 0, 1$ i zeros a on $p^s = \alpha$ o $p^s = \beta$. Si escrivim $s = \sigma + it$ (amb $\sigma, t \in \mathbb{R}$), llavors $|p^s| = p^\sigma$, i els zeros de $\zeta(E,s)$ tenen part real $\frac{1}{2}$ si i només si $|\alpha|, |\beta| = p^{1/2}$.

Tal com ho hem definit anteriorment, α, β són les arrels del polinomi

$$1 + \gamma T + pT^2, \quad \text{on } \gamma := N_p - p - 1.$$

Si $\gamma^2 - 4p \leq 0$ (és a dir, si $|N_p - p - 1| \leq 2\sqrt{p}$), llavors α i β són conjugats, i com que $\alpha\beta = p$, cadascun té mòdul $p^{1/2}$. Recíprocament, si $|\alpha|, |\beta| = p^{1/2}$,

$$|N_p - p - 1| = |\alpha + \beta| \leq 2\sqrt{p}.$$

□

La funció zeta d'una varietat sobre $\mathbb{Q}$

Sigui V una varietat projectiva no-singular sobre $\mathbb{Q}$, i.e., el conjunt de zeros d'una col·lecció de polinomis homogenis $F_i(X_0, \ldots, X_n) \in \mathbb{Q}[X_0, \ldots, X_n]$, que suposem a coeficients coprimers a $\mathbb{Z}$. Siguin $\overline{F}_i(X_0, \ldots, X_n) \in \mathbb{F}_p[X_0, \ldots, X_n]$ les reduccions dels polinomis mòdul p (anàlogament al tema 3.3). Si podem triar els polinomis F_i de manera que les seves reduccions defineixin una varietat no-singular V_p sobre $\mathbb{F}_p$, llavors diem que V té **bona reducció** a p. En cas contrari, diem que V té **mala reducció** a p (això passa per un nombre finit de primers).

[20] Si $E/\mathbb{F}_q$ és una corba el·líptica, es té també $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.

D'acord amb l'apartat anterior, per cada primer on V té bona reducció definim una funció zeta

$$\zeta(V_p, s) := Z(V_p, p^{-s}), \quad \text{amb } \log Z(V_p, T) := \sum_{m\geq 1} \#V_p(\mathbb{F}_{p^m})\frac{T^m}{m}.$$

Definició 4.73. Es defineix la **funció zeta parcial (de Hasse-Weil) d'una varietat V sobre $\mathbb{Q}$** per

$$\zeta_S(V, s) := \prod_{p\notin S} \zeta(V_p, s),$$

on $S := \{\text{primers de } \mathbb{Z} \text{ on } V \text{ té reducció dolenta}\}$.

Per la hipòtesi de Riemann per V_p (que no entrem a definir), es té que $\prod_{p\notin S}\zeta(V_p, s)$ convergeix a $\mathrm{Re}(s) > d+1$, on $d = \dim V$.

Conjectura 4.74 (Hasse-Weil)**.** *Per a qualsevol varietat projectiva no-singular V sobre $\mathbb{Q}$, la funció $\zeta_S(V, s)$ admet continuació analítica al pla complex.*

Exemple 4.75. Considerem un punt $P \in \mathbb{Z}$, que és la varietat definida pel polinomi $V : X - PZ \in \mathbb{Q}[X, Z]$. Per aquesta varietat $S = \emptyset$, i per tot primer p

$$\log Z(V_p, T) = \sum_{m\geq 1} 1\frac{T^m}{m} = log\left(\frac{1}{1-T}\right).$$

En conseqüència

$$\zeta_\emptyset(V_p, s) = \prod_{p \text{ primer}} \frac{1}{1-p^{-s}},$$

que és la funció zeta de Riemann.

La funció zeta d'una corba el·líptica sobre $\mathbb{Q}$

Sigui $E/\mathbb{Q}$ una corba el·líptica, i

$$S = \{p \in \mathbb{N} \text{ primer } \mid p \text{ és de mala reducció per } E\}.$$

D'acord amb la definició 4.73 i el teorema 4.70, tenim

$$\zeta_S(E, s) = \prod_{p\notin S} \frac{1 + (N_p - p - 1)p^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})} = \frac{\zeta_S(s)\zeta_S(s-1)}{L_S(s)},$$

on $\zeta_S(s)$ denota la funció zeta de Riemann ometent els factors al producte d'Euler corresponents als primers de S, on

$$L_S(E,s) = \prod_{p \notin S} \frac{1}{1 + (N_p - p - 1)p^{-s} + p^{1-2s}}.$$

Com a la observació 4.71, tenim $\alpha_p, \beta_p \in \overline{\mathbb{Q}}$ on

$$1 + (N_p - p - 1)T + pT^2 = (1 - \alpha_p T)(1 - \beta_p T), \quad \text{amb } |\alpha_p| = |\beta_p| = p^{1/2}.$$

Per tant,

$$L_S(E,s) = \prod_{p \notin S} \frac{1}{(1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})}.$$

De l'observació 4.58, la funció zeta de Riemann convergeix per $\mathrm{Re}(s) > 1$, i tenim

$$\prod_{p \notin S} \frac{1}{1 - p^{\frac{1}{2}} p^{-s}}$$

convergeix per $\mathrm{Re}(s) > \frac{3}{2}$, d'on s'obté que $L_S(E,s) = \prod_{p \notin S} \frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}$ està definida si $\mathrm{Re}(s) > \frac{3}{2}$.

Si escrivim $L_p(T) := 1 + (N_p - p - 1)T + pT^2$ (llavors $L_S(E,s) = \prod_{p \notin S} \frac{1}{L_p(p^{-s})}$), es compleix

$$L_p(p^{-1}) = N_p/p.$$

Mitjançant la taula de la secció 3.3, s'estén la definició de $L_S(E,s)$ pels primers on E té mala reducció:

$$L_p(T) = \begin{cases} 1 + (N_p - p - 1)T + pT^2, & \text{si } p \text{ és de bona reducció per } E \\ 1 - T, & \text{si } E \text{ té reducció multiplicativa racional a } p \\ 1 + T, & \text{si } E \text{ té reducció multiplicativa irracional a } p \\ 1, & \text{si } E \text{ té reducció additiva a } p. \end{cases}$$

Definició 4.76. Amb les notacions de sobre, definim la **funció L (de Hasse-Weil)** de la corba el·líptica $E/\mathbb{Q}$ com

$$L(E,s) = \prod_{p \text{ primer}} \frac{1}{L_p(p^{-s})},$$

i la **funció zeta (de Hasse-Weil)** de la corba el·líptica $E/\mathbb{Q}$ és, llavors

$$\zeta(E,s) = \frac{\zeta(s)\zeta(s-1)}{L(E,s)}.$$

Observació 4.77. Tal com l'hem definida, la funció L de Hasse-Weil de E codifica la informació de $\#E^{\mathrm{ns}}(\mathbb{F}_{p^m})$ per tot p primer (de bona o mala reducció) i $m \geq 1$. La conjectura de Birch i Swinnerton-Dyer augura que aquest objecte analític guarda també informació aritmètica associada amb el grup $E(\mathbb{Q})$.

Teorema 4.78 (Wiles / Wiles-Taylor / Breuil, Conrand, Diamond i Taylor (1999-2001))**.** *Donada una corba el·líptica $E/\mathbb{Q}$, la funció $L(E,s)$ admet una continuació analítica a tot el pla complex.*

Demostració. És conseqüència del treball de Wiles, Breuil, Conrand, Diamond i Taylor, en demostrar que tota corba el·líptica $E/\mathbb{Q}$ és modular. □

Definició 4.79. El **conductor** de $E/\mathbb{Q}$ és el producte finit

$$N_{E/\mathbb{Q}} = \prod_{p \text{ dolent}} p^{f_p},$$

on

$$f_p = \begin{cases} 0, & \text{si } E \text{ té bona reducció a } p, \\ 1, & \text{si } E \text{ té reducció multiplicativa a } p, \\ 2, & \text{si } E \text{ té reducció additiva a } p \neq 2,3. \end{cases}$$

(la definició de f_p quan E té reducció additiva a $p = 2,3$ és més complicada, veieu [SIL] §16.1).

Observació 4.80. El conductor de $E/\mathbb{Q}$ es obtenir via la **fórmula d'Ogg-Saito**

$$f_p = \mathrm{ord}_p(\Delta) + 1 - m_p$$

(veieu [SIL] §C 15, 16.2 pels detalls sobre la quantitat m_p).

5 La conjectura de Birch i Swinnerton-Dyer

A finals dels anys cinquanta, i després del treball de Siegel sobre formes quadràtiques a *Über die analytische Theorie der quadratischen Formen*, B.J. Birch i H.P.F. Swinnerton-Dyer decideixen (com exposen al seu article *Notes on elliptic curves II*, [BSDII]) que és natural examinar el producte

$$\prod_p N_p/p.$$

Si denotem la funció de productes parcials

$$f(P) = \prod_{p \leq P} N_p/p,$$

comproven (amb la computadora EDSAC II) que el ritme de creixement de $f(P)$ manté una correlació amb el rang algebraic de E (que poden computar en molts casos gràcies als resultats del seu article anterior [BSDI]). Aquest fet els orienta a proposar la següent

Conjectura 5.1. *Si r és el rang algebraic de la corba el·líptica $E/\mathbb{Q}$, llavors existeix una constant $C \neq 0$ tal que*

$$\lim_{P \to \infty} \frac{f(P)}{(\log(P))^r} = C.$$

Aquesta conjectura prediu que podem deduïr el rang de $E(\mathbb{Q})$ a partir de la successió de valors N_p. Destaquem que és un resultat notable, ja que $E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$ no és en general ni exhaustiva ni injectiva, i a priori sembla difícil lligar les imatges de la funció de reducció amb el grup $E(\mathbb{Q})$.

A la pràctica, Birch i Swinnerton-Dyer van ser capaços de predir amb bastant d'èxit r a partir dels valors de $f(P)$. No obstant, es van topar amb que $f(P)$ oscil·la vigorosament quan P creix, i no és practicable apropar-se a C amb un error de menys del 10% en un temps raonable. Per mirar d'esquivar aquest problema, van reexpressar la seva conjectura en termes de la funció zeta.

Definició 5.2. Sota el teorema 4.78 (que al moment de la formulació era encara una conjectura), $L(E, s)$ té una expansió en sèrie de Taylor vora $s = 1$

$$L(E, s) = c_0 + c_1 \frac{(s-1)}{1!} + c_2 \frac{(s-1)^2}{2!} + \cdots .$$

Definim el **rang analític** r_{an} de E com l'ordre del zero de $L(E,s)$ a $s=1$, de manera que

$$L(E,s) = c_{r\text{an}} \frac{(s-1)^{r\text{an}}}{r_{\text{an}}!} + \text{ termes d'ordre superior.}$$

Observem que, formalment (recordem que només tenim assegurada la convergència a $\text{Re}(s) > \frac{3}{2}$), el valor de la funció L a $s=1$ és

$$L(E,1) = \prod_p p/N_p,$$

i el comportament de $f(P)$ quan $P \to \infty$ està lligat al de $L(E,s)$ a prop de $s=1$. La conjectura anterior duu a la següent

Conjectura 5.3. *Sigui $E/\mathbb{Q}$ una corba el·líptica. Llavors, el rang analític r_{an} de E i el rang algebraic r de E són iguals.*

A partir d'aquest punt, Birch i Swinnerton-Dyer es van centrar en les corbes

$$E_D/\mathbb{Q} : Y^2Z = X^3 - DXZ^2, \quad D \in \mathbb{Q}.$$

entre d'altres motius perquè podien decidir amb prou confiança si el productori $\prod_p p/N_p$ s'anul·la o no. Van obtenir prou evidències per enunciar la següent conjectura (més dèbil que l'anterior).

Conjectura 5.4. *$L(E,1) = 0$ si i només si $r > 0$.*

Uns suggeriments de Davenport i Kneser els van dur a predir que, quan $r = 0$

$$L(E_D,1) = \begin{cases} D^{-1/4} \cdot \Omega^+ \cdot \sigma(D), & \text{per } D > 0, \\ (-4D)^{-1/4} \cdot \Omega^+ \cdot \sigma(D), & \text{per } D < 0, \end{cases}$$

on Ω^+ és el període real o el seu doble (consulteu l'observació 4.35). Mitjançant aquesta fórmula, van veure que $\sigma(D)$ sol ser una potència de 2 cops un quadrat. Un resultat de Cassels indica que si el grup $Ш(E/\mathbb{Q})$ és finit, el seu ordre és un quadrat, i aquest fet concorda amb la seva intuïció que $\sigma(D)$ ha de ser essencialment l'ordre del grup de

Tate-Shafarevich. A la resta del seu article es dediquen a donar les eines necessàries per reexpressar de forma més clara $\sigma(D)$ (mitjançant el nombre de Tamagawa i el període real).

La conjectura de Birch i Swinnerton-Dyer, que compta amb nombroses evidències numèriques, és una versió refinada de la conjectura 5.3. Precisa aquestes quantitats que ens manquen, i relaciona gran part dels objectes que hem definit amb el coeficient $c_{r_{\mathrm{an}}}$.

Conjectura 5.5 (Birch i Swinnerton-Dyer, cas concret de la conjectura de Beilinson)**.** *Sigui $E/\mathbb{Q}$ una corba el·líptica amb rang algebraic r. Llavors*

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r\Omega^+}\in\mathbb{Q},$$

és no nul, i Ω^+ llegeix la part transcendent del primer coeficient no zero del desenvolupament de Taylor de $L(E,s)$ a $s=1$.

Conjectura 5.6 (Birch i Swinnerton-Dyer (cas concret de la conjectura del nombre de Tamagawa/Bloch-Kato))**.** *Considerem $E/\mathbb{Q}$ una corba el·líptica amb rang algebraic r. Llavors r és també el rang analític de E, $Ш(E/\mathbb{Q})$ és finit i*

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r}=\left(\prod_{p\ dolent}\#(E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p))\right)\cdot\frac{\Omega^+\cdot R_{E/\mathbb{Q}}\cdot\#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2},$$

on

- $\#(E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p))$ *s'anomenen nombres de Tamagawa (veieu* (8)*).*
- $\Omega^+=\int_{E(\mathbb{R})}|\omega|$*, on ω és el diferencial invariant (veieu la definició 4.34).*
- $R_{E/\mathbb{Q}}$ *és el regul·lador el·líptic* (14)*.*
- $\#Ш(E/\mathbb{Q})$ *és l'ordre del grup de Tate-Shafarevich (veieu la definició 4.4).*
- $\#E(\mathbb{Q})_{tors}$ *és el cardinal del subgrup de torsió (que podem computar gràcies a l'apartat 4.4).*

Observació 5.7. Llistem els resultats que es coneixen actualment sobre la conjectura de Birch i Swinnerton-Dyer

- El 1976, John Coates i Andrew Wiles van demostrar que si $E/\mathbb{Q}$ és dotada de multiplicació complexa[21] per un cos quadràtic imaginari K on $K = \mathbb{Q}(i)$ o $\mathbb{Q}(\sqrt{-2})$ o $\mathbb{Q}(\sqrt{-3})$ o $\mathbb{Q}(\sqrt{-7})$ o $\mathbb{Q}(\sqrt{-11})$ o $\mathbb{Q}(\sqrt{-19})$ o $\mathbb{Q}(\sqrt{-43})$ o $\mathbb{Q}(\sqrt{-67})$ o $\mathbb{Q}(\sqrt{-163})$, i $L(E,1)$ no s'anul·la, llavors $E(\mathbb{Q})$ és un grup finit (consulteu [CW]).

- El 1983, Benedict Gross i Don Zagier van mostrar que si E és una corba modular el·líptica i L té un zero d'ordre 1 a $s = 1$, llavors E té un punt racional amb ordre infinit; (a [BZ], veure Teorema de Gross-Zagier).

- El 1990, Victor Kolyvagin va mostrar que una corba el·líptica modular E per la qual $L(E,1)$ no s'anul·la, té rang $r = 0$, i que una corba el·líptica modular E tal que la funció L té un zero d'ordre 1 a $s = 1$, té rang 1.

- El 2001, Christophe Breuil, Brian Conrad, Fred Diamond i Richard Taylor, estenent el treball de Wiles, van demostrar que totes les corbes el·líptiques definides sobre els nombres racionals són modulars (teorema de Taniyama-Shimura), la qual cosa estén el segon i el tercer resultat a totes les corbes el·líptiques sobre els nombres racionals i mostra que les funcions L de totes les corbes el·líptiques sobre $\mathbb{Q}$ estan definides a $s = 1$ (veieu [BCDT]).

- El 2010, Manjul Bhargava i Arul Shankar van anunciar una prova del fet que el rang mitjà del grup de Mordell-Weil d'una corba el·líptica sobre $\mathbb{Q}$ està acotat per sobre per 7/6. Combinant això amb la prova anunciada per Chris Skinner i Éric Urban de la conjectura principal de la teoria d'Iwasawa per $GL(2)$, conclueixen que una proporció positiva de les corbes el·líptiques sobre $\mathbb{Q}$ té rang analític zero, i per tant, pel resultat de Kolyvagin, satisfà la conjectura de Birch i Swinnerton-Dyer (consulteu [BS]).

Observació 5.8. Es pot fer una formulació anàloga per a $E/F_q(T)$:

Sigui $E/\mathbb{F}_q(T)$ una corba el·líptica sobre un cos de funcions en una variable sobre un cos finit. Llavors $\mathrm{ord}_{s=1}L(E,s) = \mathrm{rang}(E(K))$ si i només si la part l-primària $Ш(E/\mathbb{F}_q(T))\{l\}$

[21] Amb multiplicació complexa per K vol dir $End(E) \otimes \mathbb{Q} \cong K$.

de $Ш(E/\mathbb{F}_q(T))$ és un grup finit per algun primer l; i en aquesta situació les conjectures de Birch i Swinnerton-Dyer són certes per a $E/\mathbb{F}_q(T)$ (consulteu [KT]).

A Corbes algebraiques i geometria algebraica

En el desenvolupament de la resta del treball utilitzem algunes definicions i resultats bàsics de geometria algebraica i de corbes algebraiques que exposem informalment en aquest apèndix.

A.1 Corbes planes afins

Durant tot aquest apartat denotem k un cos arbitrari, i $K \supseteq k$ una extensió algebraica.

El **pla afí** sobre k és[22] $\mathbb{A}^2(k) := k \times k$. Un polinomi no-constant $f \in k[X,Y]$ sense factors repetits a $\overline{k}[X,Y]$ (o, més rigorosament, la classe d'equivalència dels seus múltiples per elements de $k^\times$) defineix una **corba plana afí** C_f. Els seus punts a qualsevol extensió algebraica $K \supseteq k$ són els elements del conjunt

$$C_f(K) =: \{(x,y) \in \mathbb{A}^2(K) \mid f(x,y) = 0\}.$$

Anomenem **grau** de la corba C_f al grau màxim d'entre els graus de cada monomi de f (on el grau d'un monomi és la suma dels exponents de les indeterminades).

La corba C_f es diu **irreductible** (sobre el cos K[23]) si f és irreductible a $K[X,Y]$, i **geomètricament irreductible** si f és irreductible sobre $\overline{k}$. A més, si $f = f_1 \cdots f_r$ és una factorització de f en polinomis irreductibles i diferents dos a dos a $k[X,Y]$, tenim

$$C_f(K) = C_{f_1}(K) \cup \cdots \cup C_{f_r}(K),$$

i les corbes irreductibles C_{f_i} s'anomenen **components irreductibles** de C_f.

Usualment escrivim $C : f = 0$ enlloc de C_f, o $C : f = g$ enlloc de C_{f-g}.

Per a qualsevol $f \in k[X,Y]$, $P = (a,b) \in C_f(K)$ es diu **singular** (o **singularitat**) si $\frac{\partial f}{\partial X} = \frac{\partial f}{\partial Y} = 0$, i **no-singular** si alguna d'aquestes dues derivades no s'anul·la a P. Es defineix l'**espai tangent de Zariski** a C al punt P com

$$\left(\frac{\partial f}{\partial X}\right)_P (X-a) + \left(\frac{\partial f}{\partial Y}\right)_P (Y-b) = 0,$$

[22] Quan volem obviar el cos k, escrivim $\mathbb{A}^2$ enlloc de $\mathbb{A}^2(k)$.

[23] Quan diem que una corba és irreductible sense fixar el cos sobre el qual ho és, usualment ho és sobre el cos base k. A més, també escrivim C enlloc de C_f quan volem obviar f.

i en el cas que P no sigui singular també en diem **recta tangent** a C al punt P.

La corba C_f es diu **singular** si $C_f(\overline{k})$ conté algun punt singular, i **no-singular** si no en conté cap[24].

Per $P = (a, b) \in C_f(K)$, si

$$f(X, Y) = f_1(X - a, Y - b) + \cdots + f_n(X - a, Y - b),$$

és una descomposició de f en suma de polinomis homogenis (o formes) f_i de grau i centrats a P, anomenem **multiplicitat** de P al mínim i tal que $f_i \neq 0$, i la denotem per $m_P(f)$. Quan $i = 2$, P s'anomena **punt doble**.

Tenim que P és no-singular si i només si té multiplicitat 1, i llavors $L : f_1 = 0$ és la recta tangent a C al punt P. De la mateixa manera, quan P és singular amb multiplicitat m, podem expressar (sobre $\overline{k}$)

$$f_m(X, Y) = \prod_i L_i^{r_i},$$

on cada L_i és un polinomi homogeni de grau 1 amb coeficients a $\overline{k}$ (veieu [FUL]§2.6 5). Les rectes $L_i = 0$ s'anomenen **rectes tangents** a C_f al punt P, i r_i és la seva **multiplicitat**. A més, diem que una singularitat és **ordinària** si tota recta tangent té multiplicitat 1, i si una singularitat és ordinària i doble s'anomena **node**.

A.2 Corbes planes projectives

Sigui k un cos arbitrari. El **pla projectiu** sobre k és[25]

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

on $(x, y, z) \sim (x', y', z')$ si i només si existeix un $c \in k^\times$ tal que $(x, y, z) = (cx', cy', cz')$. Escrivim $(x : y : z)$ per la classe d'equivalència de (x, y, z) a $\mathbb{P}^2(k)$.

Un polinomi homogeni (o forma) no constant $F \in k[X, Y, Z]$ sense factors repetits a $\overline{k}$ (o, més rigorosament, la classe d'equivalència dels seus múltiples per elements de $k^\times$)

[24] Es pot veure (mitjançant el Nullstellensatz) que, si una corba és no-singular a k, llavors no conté punts singulars a cap extensió algebraica de k.

[25] Quan volem obviar el cos k, escrivim $\mathbb{P}^2$ enlloc de $\mathbb{P}^2(k)$.

defineix una **corba plana projectiva** C_F. Els seus punts a qualsevol extensió algebraica $K \supseteq k$ són els elements del conjunt

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

Observem que, atès que F és homogeni,

$$F(cx, cy, cz) = c^{\deg F} F(x, y, z) \quad \text{per tot } c \in k^\times,$$

i per tant no té massa sentit parlar del valor de F a un punt no-nul de $\mathbb{P}^2$, però si dels seus zeros a $\mathbb{P}^2(K)$. Anomenem **grau** de la corba C_F al grau de F.

Per $i = 0, 1, 2$, sigui $U_i := \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(k) \mid x_i \neq 0\}$. Veiem que U_2 (i de la mateixa manera U_0 i U_1) és, de forma natural, un pla afí via la bijecció

$$U_2 \to \mathbb{A}^2(k) : (x_0 : x_1 : x_2) \mapsto \left(\frac{x_0}{x_2}, \frac{x_1}{x_2}\right).$$

D'aquesta manera, una corba projectiva plana $C = C_F$ és la unió de tres corbes afins planes

$$C = C_0 \cup C_1 \cup C_2, \quad C_i = C \cap U_i,$$

anomenades **projeccions (o cartes) afins** de C (respecte la variable x_i), i definides pels polinomis $F(1, x_1, x_2)$, $F(x_0, 1, x_2)$ i $F(x_0, x_1, 1)$.

La corba C_F es diu **irreductible** sobre el cos $K \supseteq k$[26] (resp. **geomètricament irreductible**) si cada projecció afí és irreductible sobre K (resp. sobre $\overline{k}$).

Exemple A.1. Considerem la corba plana projectiva sobre k amb $\mathrm{char}(k) \neq 2, 3$

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

Com que l'únic punt amb $Z = 0$ és $(0 : 1 : 0)$, tenim que

$$C = C_2 \cup \{(0 : 1 : 0)\},$$

i a la resta del treball diem que C_2 és la projecció afí de C, i que $(0 : 1 : 0)$ és el **punt a l'infinit**. A més notem que, per aquesta mateixa raó, $C = C_1 \cup C_2$.

[26] Quan diem que una corba és irreductible sense fixar el cos sobre el qual ho és, usualment ho és sobre el cos base k. A més, també escrivim C enlloc de C_f quan volem obviar f.

Les notacions i les nocions d'espai de Zariski, recta tangent, multiplicitat, etc. es poden estendre a les corbes projectives tenint en compte que qualsevol punt d'una corba projectiva és dins d'una projecció afí.

A.3 Resultants

En aquest apartat donem els resultats de teoria de resultants que utilitzem al treball.

Sigui $f(X) = s_0X^m + s_1X^{m-1} + \cdots + s_m$ i $g(X) = t_0X^n + t_1X^{n-1} + \cdots + t_n$ polinomis a coeficients sobre un cos k arbitrari. Definim el **resultant** $\mathrm{Res}(f,g)$ de f i g pel determinant

$$Res(f,g) := \begin{vmatrix} s_0 & s_1 & \cdots & s_m & & \\ & s_0 & \cdots & s_{m-1} & s_m & \\ & & \cdots & & & \cdots \\ t_0 & t_1 & \cdots & t_m & & \\ & t_0 & \cdots & t_{m-1} & t_m & \\ & & \cdots & & & \cdots \end{vmatrix} \begin{matrix} \\ n \text{ files} \\ \\ \\ m \text{ files} \\ \end{matrix}$$

A més, definim el **discriminant** del polinomi f per

$$\Delta(f) = (-1)^{\frac{1}{2}n(n-1)}\frac{1}{s_0}\mathrm{Res}(f,f').$$

Utilitzem ben sovint els quatre resultats següents (sobretot el segon), la demostració dels quals podeu consultar a [MIL] §I 24-26.

Proposició A.2. *El resultant* $\mathrm{Res}(f,g) = 0$ *si i només si*

(*a*) $s_0 = t_0 = 0$, *o*

(*b*) *els dos polinomis tenen una arrel en comú a* $\overline{k}$ *(o, equivalentment, un factor en comú a* $k[X]$*).*

Proposició A.3. *Siguin* $l(X,Y), h(X,Y) \in k[X,Y]$. *Posem* $r(X) \in k[X]$ *el resultant de* l *i de* h *calculat mirant* l *i* h *com a polinomis en* Y *a coeficients a* $k[X]$. *Llavors,*

- *Existeixen* $a(X,Y), b(X,Y) \in k[X,Y]$ *tals que*

$$al + bh = r(X) \in k[X],$$

  i $\deg_Y(a) < \deg_Y(h)$, $\deg_Y(b) < \deg_Y(l)$.

- *El polinomi* $r = 0$ *si i només si* l *i* h *tenen un factor en comú a* $k[X,Y]$.

Observació A.4. Donats $l(X) = s_0X^m + s_1X^{m-1} + \cdots + s_m$ i $h(X) = t_0X^n + t_1X^{n-1} + \cdots + t_n$, descrivim un algorisme per trobar els polinomis $a(X,Y)$ i $b(X,Y)$ de la darrera proposició.

Anomenem $c_1, \ldots, c_{m+n}$ a les columnes de la matriu

$$\begin{pmatrix} s_0 & s_1 & \cdots & s_m & & \\ & s_0 & \cdots & s_{m-1} & s_m & \\ & & \cdots & & & \cdots \\ t_0 & t_1 & \cdots & t_m & & \\ & t_0 & \cdots & t_{m-1} & t_m & \\ & & \cdots & & & \cdots \end{pmatrix}.$$

Tenim la següent identitat

$$\begin{pmatrix} X^{n-1}l(X) \\ X^{n-2}l(X) \\ \vdots \\ l(X) \\ X^{m-1}h(X) \\ \vdots \\ h(X) \end{pmatrix} = X^{m+n-1}c_1 + \cdots + 1c_{m+n},$$

i gràcies a aquesta, denotant per c la part esquerra de la igualtat i per les propietats del determinant, obtenim

$$\mathrm{Res}(l,h) := \det(c_1, \ldots, c_{m+n}) = \det(c_1, \ldots, c_{m+n-1}, c).$$

L'expansió de Laplace d'aquest últim determinant per la columna c ens dóna l'expressió desitjada.

Corol·lari A.5. *Si $l, g \in k[X,Y]$ no tenen cap factor en comú a $k[X,Y]$, llavors tampoc no en tenen cap a $K[X,Y]$ per cap extensió algebraica de cossos $K \supseteq k$.*

Proposició A.6. *Siguin $F, G \in k[X,Y]$ polinomis homogenis, i reescrivim* $\mathrm{Res}(F,G) := \mathrm{Res}(F(x,1), G(x,1))$. *Llavors el resultant* $\mathrm{Res}(F,G) = 0$ *si i només si F i G tenen un zero no trivial*[27] *a $\mathbb{P}^1(\overline{k})$.*

A.4 Nombres d'intersecció

Definició A.7. Sigui k un cos arbitrari. Considerem $P = (a,b) \in \mathbb{A}^2(k)$, dos polinomis $F, G \in k[X,Y]$ no necessàriament homogenis, i f i g les homogeneïtzacions de F i G a $k[X,Y,Z]$. Definim el **nombre d'intersecció** $I(P, F \cap G)$ de les cartes afins (respecte Z) de les corbes C_f i C_g al punt P com l'únic (gràcies a [FUL] §3.3 3) objecte que compleix les propietats

(a) $I(P, F \cap G) \in \mathbb{N} \cup \{0\}$ si F i G intersecten pròpiament[28] a P. En cas contrari, $I(P, F \cap G) = \infty$.

(b) $I(P, F \cap G) = 0$ si i només si F i G no s'anul·len simultàniament a P (i.e., si $P \notin C_F \cap C_G$).

(c) Si T és un canvi de coordenades afí a $\mathbb{A}^2$, i $T(Q) = P$, llavors $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

(d) $I(P, F \cap G) = I(P, G \cap F)$.

(e) $I(P, F \cap G) \geq m_P(F) m_P(G)$, amb igualtat si i només si C_F i C_G no tenen rectes tangents en comú a P.

(f) Si $F = \prod_i F_i^{r_i}$ i $G = \prod_j G_j^{s_j}$ són productes de polinomis sobre $k[X,Y]$, llavors $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$.

[27] És a dir, diferent del zero trivial $(0:1)$ (si s_0 o $t_0 \neq 0$).

[28] Dos polinomis **intersecten pròpiament** a un punt P si i només si s'anul·len a P i no tenen cap factor en comú que tingui P per arrel.

(g) $I(P, F \cap G) = I(P, F \cap (G + AF))$ per qualsevol $A \in k[X, Y]$.

Usualment denotem $I(P, C_F \cap C_G)$ per $I(P, F \cap G)$, i $I(F, G)$ com el nombre d'intersecció de les corbes C_f i C_g a l'origen (amb aquesta notació, $I(X, Y) = 1$ gràcies al punt (e)).

Notem que, amb la darrera definició,

$$I(P, F \cap G) = I(f(X + a, Y + b), g(X + a, Y + b)).$$

Observació A.8. Aquestes propietats ens proporcionen un algorisme per calcular el nombre d'intersecció $I(F, G)$ per $F, G \in k[X, Y]$.

En primer lloc, gràcies a la teoria de resultants, trobem $a, b \in k[X, Y]$ i $r \in k[X]$ tals que $aF + bG = r$ i $\deg_Y(b) < \deg_Y(F)$, $\deg_Y(a) < \deg_Y(G)$. Si $\deg_Y(F) \leq \deg_Y(G)$, escrivim

$$I(F, G) \overset{(f)}{=} I(F, bG) - I(F, b) \overset{(g)}{=} I(F, r) - I(F, b),$$

i en cas contrari, escrivim

$$I(F, G) = I(r, G) - I(a, G).$$

Procedint així amb cada un dels sumands, reduïm el grau respecte Y fins arribar a expressar $I(F, G)$ en sumands de nombres d'intersecció de l'estil $I(f, g)$ on $g \in k[X]$. Si escrivim $g(X) = X^m g_0(X)$ amb $g_0(0) \neq 0$, tenim

$$I(f, g) \overset{(b),(f)}{=} mI(f, X),$$

i en virtut de (g) podem extreure múltiples de X a f fins a obtenir $f \in k[Y]$. Posant $f(Y) = Y^n f_0(Y)$ amb $f_0(0) \neq 0$, veiem que

$$I(f, X) \overset{(b)}{=} I(Y^n, X) \overset{(f)}{=} nI(Y, X) \overset{(e)}{=} n,$$

I per tant $I(f, g) = mn$.

Cal tenir ben present el següent teorema, que juntament amb els nombres d'intersecció és una eina d'una utilitat inqüestionable en la construcció del grup de Mordell-Weil d'una corba el·líptica.

Teorema A.9 (Teorema de Bézout)**.** *Siguin C i D corbes planes projectives sobre k de graus m i n respectivament, sense components irreductibles en comú.*

Llavors C i D intersecten sobre $\overline{k}$ a exactament mn punts comptant multiplicitats, i.e.,

$$\sum_{P \in C(\overline{k}) \cup D(\overline{k})} I(P, C \cap D) = mn.$$

Demostració. Consulteu [FUL] §5.3 . □

A.5 Nullstellensatz

En aquest apartat introduïm un dels teoremes més destacats en geometria algebraica, el teorema dels zeros de Hilbert o Nullstellensatz. Ens cal la notació següent.

Definició A.10. Sigui k un cos, i $F \in k[X_1 \ldots, X_n]$. El conjunt de zeros de F a $\mathbb{A}^n(k)$ s'anomena **hipersuperfície (o conjunt algebraic) definida per** F, i la denotem per $V(F)$.

A més, per qualsevol subconjunt $X \in \mathbb{A}^n(k)$, el conjunt de polinomis a $\bar{k}[X_1, \ldots, X_n]$ que s'anul·len a X formen un ideal, que anomenem **ideal de** X i que denotem per $I(X)$. Amb aquesta notació, diem que X és **definida** sobre k si el seu ideal pot ser generat per polinomis a $k[X_1 \ldots, X_n]$. A més, X s'anomena **varietat** si $I(X)$ és un ideal primer a $\bar{k}[X_1, \ldots, X_n]$.

Tot seguit enunciem quatre formulacions del Nullstellensatz sense demostrar-les (podeu trobar-ne les demostracions a [FUL] §1.7, a [WiTZH], o a qualsevol tractat bàsic de geometria algebraica).

Teorema A.11 (Existència dels zeros)**.** *Sigui $\overline{k}$ un cos algebraicament tancat, i I un ideal propi de $\overline{k}[X_1, \ldots, X_n]$. Llavors $V(I) \neq \emptyset$.*

Teorema A.12 (Nullstellensatz dèbil)**.** *Sigui k un cos, i L una k-àlgebra*[29] *finitament*

[29] Sigui k un cos, i A un espai vectorial sobre k equipat amb una operació $(x, y) \mapsto x \cdot y : A \times A \to A$. Llavors A és una k-àlgebra si i només si la operació $\cdot$ és bilineal; o el que és equivalent, si i només si $\cdot$ és distributiva per la dreta i per l'esquerra respecte $+_A$, i a més és compatible per escalars (i.e., $(ax) \cdot (by) = (ab)(x \cdot y)$ per $x, y \in A$, $a, b \in k$.)

generada (com a k-àlgebra). Si L és un cos, llavors L és una extensió algebraica de k.

Teorema A.13 (Nullstellensatz)**.** *Sigui $\overline{k}$ un cos algebraicament tancat, i I un ideal de $\overline{k}[X_1, \ldots, X_n]$. Llavors, $I(V(I)) = Rad(I)$, on $Rad(I)$ és el radical de l'ideal I (el conjunt d'arrels n-èssimes dels elements de I a $\overline{k}[X_1, \ldots, X_n]$).*

Teorema A.14 (Nullstellensatz)**.** *Sigui $\overline{k}$ un cos algebraicament tancat, i M un ideal maximal de $\overline{k}[X_1, \ldots, X_n]$. Llavors existeix $(a_1, \ldots, a_n) \in \overline{k}^n$ tal que $M = (X_1 - a_1, \ldots, X_n - a_n)$.*

Aquesta darrera versió del Nullstellensatz guarda una relació amb el fet següent.

Lema A.15. *Si K és un cos, i $(a_1, \ldots, a_n) \in K^n$, llavors l'ideal $I = (X_1 - a_1, \ldots, X_n - a_n)$ és un ideal maximal de $K[X_1, \ldots, X_n]$.*

A.6 El conjunt de punts racionals d'una corba plana

Sigui $C := C_F$ una corba plana projectiva sobre $\mathbb{Q}$ i geomètricament irreductible. En aquest apartat discutim informalment dues qüestions fonamentals en l'estudi de les corbes algebraiques:

(a) C té cap punt amb coordenades a $\mathbb{Q}$?

(b) Si la resposta és que sí, podem descriure el conjunt de punts racionals?

En acabar l'apartat haurem vist com les corbes de grau 3, i més concretament les corbes el·líptiques, són pràcticament els casos més particulars i intrigants que podem considerar.

Corbes planes projectives de grau 1

Tots els casos es redueixen a la recta

$$C : aX + bY + cZ = 0, \quad a, b, c \in \mathbb{Q}, \text{no tots zero.}$$

El conjunt de punts de C a $\mathbb{P}^2(\mathbb{Q})$ mai és buit, i és essencialment la recta projectiva $\mathbb{P}^1(\mathbb{Q})$ gràcies a la bijecció

$$(s:t) \mapsto \left(s:t:-\frac{a}{c}s-\frac{b}{c}t) : \mathbb{P}^1 \to C(\mathbb{Q}\right).$$

Corbes planes projectives de grau 2

Notem que $C/\mathbb{Q}$ no pot ser singular, ja que si P té multiplicitat $m \geq 2$, una recta que passi per P i per un altre punt Q compleix

$$I(P, L \cap C) + I(Q, L \cap C) \overset{A.7(e)}{\geq} m + 1 \geq 3,$$

que entra en contradicció amb el teorema de Bézout.

Per respondre la primera pregunta, Legendre mostra que tota corba projectiva de grau 2 compleix el principi local-global (o de Hasse). En altres paraules, veu que mitjançant un canvi elemental de variables podem escriure F en la forma

$$F = aX^2 + bY^2 + cZ^2 \quad a, b, c \in \mathbb{Z} \text{ lliures de quadrats},$$

i demostra que si a, b, c no tenen tots el mateix signe (i.e., si F té solucions sobre $\mathbb{R}$) i $abc \neq 0$ (cas en el qual no és directe trobar solucions a $\mathbb{R}$), llavors existeix una solució no trivial de $F = 0$ a $\mathbb{Q}$ si i només si $-bc, -ca, -ab$ són residus quadràtics mòdul a, b, c respectivament. Per la llei de reciprocitat quadràtica es pot veure que això implica que, per un cert m depenent de a, b, c, $C(\mathbb{Q}) \neq \emptyset$ si i només si $F(X, Y, Z)$ mod m té una solució en enters coprimers amb m (que és comprovable en un nombre finit de passos).

També es pot veure que, si C conté un punt racional P, i L és una recta projectiva a coeficients racionals que passa per P, llavors L talla a C a un punt de $C(\mathbb{Q})$.

Corbes planes projectives de grau 3

Si $C/\mathbb{Q}$ és no-singular, encara no es coneix cap mètode general per esbrinar si té cap punt a $\mathbb{Q}$. I si el té, la descripció de $C(\mathbb{Q})$ és l'objectiu de tot aquest treball.

En canvi, si C és singular, es pot veure que la seva singularitat P pertany a $C(\mathbb{Q})$ (atès que, si suposem que pertany a un cos de nombres K, $\mathrm{Gal}(K/\mathbb{Q})$ fixa P, i per tant

$P \in C(\mathbb{Q})$). Qualsevol recta projectiva racional L que passi per P i talli C a un altre punt, ho fa a $P_0 \in C(\mathbb{Q})$, i obtenim una parametrització de $E(\mathbb{Q})$. De fet, es pot veure ([MIL] §II.3) que en aquest cas $C(\mathbb{Q})$ és isomorf a $(\mathbb{Q}, +)$ o a $(\mathbb{Q}^\times, \times)$ (que no són finitament generats).

Corbes planes projectives de gènere ≥ 2

El 1983, Faltings demostrà que, per tota corba projectiva $C = C_F$ definida sobre $\mathbb{Q}$ amb gènere > 1, i.e., tal que

$$\frac{(\deg C - 1)(\deg C - 2)}{2} - \sum_{P \in C(\overline{\mathbb{Q}})} \frac{m_P(F)(m_P(F) - 1)}{2} > 1,$$

el conjunt $C(\mathbb{Q})$ és finit.

A.7 La llei de grup d'una corba cúbica

Sigui k un cos, i C_F/k una corba plana projectiva no singular de grau 3, amb $C(k) \neq \emptyset$ (suposem $O \in C(k)$).

Teorema A.16. *Amb la operació i les notacions donades al principi de l'apartat 3.2, $C(k)$ és un grup commutatiu.*

Demostració. Per definició, és directe veure que $P+Q = Q+P$ i que $O+P = O(OP) = P$.

A més, per a qualsevol $P \in C(k)$, sigui $P' = P(OO)$. Llavors, $PP' = OO$, i $O(PP') = O(OO) = O$, i.e., $P + P' = O$.

Per veure l'associativitat, escrivim $l(P, Q)$ per la recta a $\mathbb{P}^2(k)$ que passa per P i Q. Per qualssevol $P, Q, R \in C(k)$, denotem

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

Llavors, $(P + Q) + R = OS$ i $P + (Q + R) = OT$, i per demostrar l'associativitat n'hi ha prou amb veure que $S = T$.

Considerem les corbes cúbiques

$$F = 0,$$
$$l(P,Q) \cdot l(R, P+Q) \cdot l(QR, O) = 0,$$
$$l(P,QR) \cdot l(Q,R) \cdot l(P,O) = 0.$$

Totes tres passen pels vuit punts

$$O, P, Q, R, PQ, QR, P+Q, Q+R,$$

I les dues últimes passen per

$$U = l(P, Q+R) \cap l(P+Q, R).$$

En el cas que les sis rectes que defineixen les dues últimes cúbiques siguin diferents, la següent proposició afirma $S = U = T$. Per la resta de casos, consulteu [MIL] §I 3.1. □

Proposició A.17. *Sigui $\overline{k}$ un cos algebraicament tancat i considerem dues corbes planes projectives de grau 3. Si aquestes intersecten en exactament nou punts, qualsevol corba cúbica que passi per vuit d'aquests punts passarà també pel novè.*

Demostració. Consulteu [MIL] §I 3.2.

A.8 Funcions regulars i racionals

Funcions regulars i racionals sobre corbes afins

Ho dividim en dos casos.

- $\overline{k}$ algebraicament tancat

  Sigui C_f una corba plana afí definida per $f \in \overline{k}[X,Y]$ i irreductible sobre $\overline{k}$. Anomenem **funció regular** a C a qualsevol funció definida per

  $$(a,b) \mapsto g(a,b) : C(\overline{k}) \to \overline{k}, \quad \text{per algun } g(X,Y) \in \overline{k}[X,Y].$$

Clarament, qualsevol múltiple de $f(X,Y) \in \overline{k}[X,Y]$ defineix una funció regular nul·la, i el contrari també és cert (gràcies al Nullstellensatz A.13). Atès aquest fet, denotem l'**anell de funcions regulars** per

$$\overline{k}[C_f] := \overline{k}[X,Y]/(f(X,Y)) = \overline{k}[x,y],$$

on x i y són les funcions coordenada $P \mapsto x(P)$, $P \mapsto y(P)$ a $C(\overline{k})$. Els elements de $\overline{k}[C]$ són polinomis amb indeterminades x i y.

Com que l'ideal (f) és primer, l'anell $\overline{k}[C]$ és un domini d'integritat. Denotem $\overline{k}(C)$ el cos de fraccions de $\overline{k}[C]$, i l'anomenem **cos de fraccions racionals** a C. Els seus elements, les **funcions racionals** a C, són funcions de l'estil

$$(a,b) \mapsto \frac{g(a,b)}{h(a,b)} : C(\overline{k}) \backslash \{P \in \mathbb{A}^2(\overline{k}) \mid h(P) = 0\} \to \overline{k}.$$

- k perfecte

  L'**anell de funcions regulars** sobre C_f és

  $$k[C_f] := k[X,Y]/(f(X,Y)),$$

  on $f(X,Y)$ és irreductible sobre $k[X,Y]$.

  Observació A.18. Cal notar, però, que les funcions regulars ja no han de ser necessàriament definides sobre $C(k)$ (ja que, per exemple, $C(k)$ pot ser buit). No obstant, podem salvar aquesta dificultat dient que les **funcions racionals** a C són les famílies de funcions $g \in k[C]$ on, per qualsevol cos $K \supset k$, $g : C(K) \to K$, i són compatibles per les inclusions de cossos $K \subseteq L$.

  Una **funció racional** a C_f és un element del **cos de fraccions** $k(C_f) = k(x,y)$ de $k[C_f]$.

  A certs punts del treball tenen especial rellevància els ideals primers no nuls de $k[C_f]$. Els anomenem **divisors primers** a C_f, i anomenem **grup de divisors** de C_f al grup abelià lliure $\mathrm{Div}(C_f)$ generat pel conjunt de divisors primers a C_f.

Observació A.19. Observem que, pel Nullstellensatz, els divisors primers a $k[C]$ són tots de la forma $(x-a, y-b)$ per $(a,b) \in C(k)$. Això es manté coherent amb la subsecció posterior.

Funcions regulars i racionals sobre corbes projectives

Ho dividim en dos casos.

- $\overline{k}$ algebraicament tancat

  Sigui $C_F/\overline{k}$ una corba plana projectiva definida per un polinomi homogeni irreductible $F(X,Y,Z)$. Pels mateixos motius que al principi de l'apartat anterior, anomenem **funció regular** C a qualsevol funció $C(\overline{k}) \to \overline{k}$ de l'**anell de funcions regulars** a C

  $$\overline{k}[C_F] := \overline{k}[X,Y,Z]/(F(X,Y,Z)) = \overline{k}[x,y,z].$$

  Ara, diem $\overline{k}[x,y,z]_d$ als elements de $\overline{k}[x,y,z]$ que admeten un representant homogeni de grau d. Amb això, denotem $\overline{k}(x,y,z)$ el cos de fraccions de $\overline{k}[x,y,z]$, i definim el **cos de funcions racionals** a C per

  $$\overline{k}(C) := \{g/h \mid g,h \in \overline{k}[x,y,z]_d \text{ per algun } d\} = \overline{k}(x,y,z)_0.$$

  Una **funció racional** a C és un element $f = g/h : C(\overline{k})\backslash\{\text{zeros de } h\} \to k$ de $k(C_F)$.

- k perfecte

  Tant l'**anell de funcions racionals** com el **cos de funcions racionals** es defineixen com al cas de k algebraicament tancat.

  No obstant, $C_F(k)$ pot ser buit, i per salvar aquest fet i definir les funcions regulars i les funcions racionals a C_F hem de fer l'observació anàloga a A.18.

  Observem que hi ha una identificació natural entre $k(C_F)$ i $k(C_i)$ per a qualsevol projecció afí C_i de C_F (homogeneïtzant). Amb aquesta, qualsevol divisor primer a

un dels C_i defineix un anell de valuació discreta[30] $k[C_i]_{(\mathfrak{p})} \subseteq k(C_F)$ (que és l'anell de funcions regulars de C a $\mathfrak{p}$, i no depèn de la carta C_i), que anomenem **divisor primer** a C_F. Anomenem **grup de divisors** a C al grup lliure abelià generat pels divisors primers a C_F.

A més, per qualsevol divisor primer $\mathfrak{p}$ de $k(C_F)$, definim $\deg(\mathfrak{p})$ com la dimensió del cos residual $k[C_i]_{(p)}/\mathfrak{p}$ com a k-e.v., i $\deg(\sum n_\mathfrak{p}\mathfrak{p}) = \sum n_\mathfrak{p} \deg(\mathfrak{p})$. Notem que qualsevol $h \in k(C)^\times$ defineix un divisor principal

$$\operatorname{div}(h) = \sum_{\mathfrak{p}} \operatorname{ord}_\mathfrak{p}(h)\mathfrak{p},$$

on $\operatorname{ord}_\mathfrak{p}(h)$ és l'ordre natural de l'anell de valuació discreta $\mathfrak{p}$ de l'anell $k[C_i]_{(\mathfrak{p})}/(\mathfrak{p})$ (la potència d'un uniformitzant de $\mathfrak{p}$ a l'expressió de h com a producte d'una unitat per aquest uniformitzant, i no depèn de la carta).

A.9 Divisors

En aquesta secció $\overline{k}$ denota sempre un cos algebraicament tancat (pel cas on k és només perfecte, veieu l'apartat anterior o [MIL] §I.4), i C_F una corba projectiva no singular definida sobre k.

El **grup de divisors** a C_F, denotat per $\operatorname{Div}(C)$, és el grup abelià lliure generat pels punts del conjunt $C_F(\overline{k})$. Per tant, un element de $\operatorname{Div}(C)$ és una suma finita

$$D = \sum_{P \in C(\overline{k})} n_P[P], \quad n_P \in \mathbb{Z}, \quad P \in C(\overline{k}).$$

Definim el **grau** de D per $\deg(D) = \sum_P n_P$, i diem $\operatorname{Div}^n(C)$ al **grup de divisors de grau** n. A més, associem a $\operatorname{Div}(C)$ l'ordre parcial

$$\sum n_P[P] \geq \sum m_P[P] \Leftrightarrow n_P \geq m_P \text{ per tot } P.$$

En particular, diem que $D \neq 0$ és **positiu** si $n_P \geq 0$ per tot P.

[30] Un **anell de valuació discreta** (AVD) és un domini d'ideals principals amb un únic ideal maximal no nul.

Sigui $\varphi(X,Y,Z) = \frac{G(X,Y,Z)}{H(X,Y,Z)}$ una funció racional no nul·la a C (on $\deg(G) = \deg(H)$), i suposem que F no divideix H. Com que $\varphi \neq 0$, F tampoc divideix G. El teorema de Bézout aplicat a φ i a φ^{-1} afirma

$$(\deg F) \cdot m = \sum_{\{P|F(P)=G(P)=0\}} I(P, F \cap G)$$
$$(\deg F) \cdot m = \sum_{\{P|F(P)=H(P)=0\}} I(P, F \cap H).$$

Definim el **divisor** d'una funció racional φ com
$\operatorname{div}(\varphi) = \sum_{\{P|F(P)=G(P)=0\}} I(P, F \cap G)[P] - \sum_{\{P|F(P)=H(P)=0\}} I(P, F \cap H)[P]$.
Tenim doncs $\deg(\operatorname{div}(\varphi)) = 0$.

Anomenem **divisor principal** a C a qualsevol divisor associat a una funció racional sobre C, i denotem per $P(C)$ el **grup de divisors principals** a C, que és un subgrup de $\operatorname{Div}^0(C)$.

Definició A.20. Definim els **grups de Picard** per

$$\operatorname{Pic}(C) = \operatorname{Div}(C)/P(C), \quad \operatorname{Pic}^0(C) = \operatorname{Div}^0(C)/P(C).$$

Com comprovarem, la següent proposició ens dóna un morfisme molt interessant.

Proposició A.21. *Sigui $C/\overline{k}$ una corba projectiva no singular de gènere 1 tal que $C(\overline{k}) \neq 0$, i considerem $O \in C(\overline{k})$. L'aplicació*

$$P \mapsto [P] - [O] : C(\overline{k}) \to Pic^0(C)$$

és bijectiva.

Demostració. Consulteu [MIL] §I 4.10. □

Observació A.22. El fet interessant d'aquesta bijecció és que defineix una estructura de grup a $C(\overline{k})$ amb la condició natural que la converteix en un homomorfisme:

$$P + Q = S \text{ a } C(\overline{k}) \Leftrightarrow [P] + [Q] = [S] + [O] \text{ a } \operatorname{Pic}^0(C).$$

A més a més, sorprenentment, aquesta estructura de grup és la mateixa que hem definit a l'apartat 3.2 per $\overline{k}$ algebraicament tancat. Per veure-ho, suposem que $P+Q=S$. Considerem l_f la recta (definida per $f=0$) que passa per P i Q, i r_g la recta que passa per O i S. Per la definició de la llei de grup a l'apartat 3.2, sabem que l_f i r_g tallen $C(\overline{k})$ un punt en comú R. Prenent la funció racional $\varphi = \frac{f}{g}$, i calculant-ne el divisor (principal)

$$\operatorname{div}(\varphi) = [P]+[Q]+[R]-[O]-[S]-[R] = [P]+[Q]-[S]-[O].$$

Per tant, $[P]+[Q]=[S]+[O]$ a $\operatorname{Pic}^0(C)$.

Teorema de Riemann-Roch i gènere

Donat un divisor D a la corba plana projectiva no-singular C_F sobre un cos $\overline{k}$ algebraicament tancat, definim

$$L(D) = \{\varphi \in \overline{k}(C) \mid \operatorname{div}(\varphi) + D \geq 0\} \cup \{0\},$$

i posem $\ell(D)$ la seva dimensió com a $\overline{k}$-espai vectorial (que, de fet, és sempre finita). Els següents teoremes (que no demostrem) ens acoten $\ell(D)$ a partir de D i d'una altra quantitat molt important en l'estudi de les corbes algebraiques.

Teorema A.23 (Roch)**.** *Existeix un enter g tal que, per a qualsevol divisor D a C,*

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

amb igualtat quan $\deg(D) > 2g-2$ *suficientment positiu.*

Definició A.24. L'enter g determinat pel teorema s'anomena el **gènere** de C.

Observació A.25. Com notem al primer capítol d'aquest treball, per una corba plana projectiva no-singular C, el gènere de C es pot expressar com

$$g(C) = \frac{(\deg C - 1)(\deg C - 2)}{2}.$$

De fet, el teorema de Riemann-Roch és la següent millora del teorema de Roch.

Teorema A.26 (Riemann-Roch)**.** *Existeix un enter g tal que, per a qualsevol divisor D a C,*

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

on W és un divisor canònic (i.e., un divisor associat a alguna forma diferencial a C).

B Cohomologia de grups (H^0 i H^1)

La definició de dos dels objectes més rellevants de la part racional de la conjectura de Birch i Swinnerton-Dyer són els grups de Selmer i de Tate-Shafarevich. En aquest treball presentem aquests objectes via cohomologia Galoisiana, que és la formulació més utilitzada actualment.

B.1 Cohomologia de grups finits

Definició B.1. Sigui G un grup finit, i M un grup abelià. Una **acció** de G a M és una aplicació $(\sigma, m) \mapsto \sigma m : G \times M \to M$ tal que

(a) $\sigma(m + m') = \sigma m + \sigma m' \quad \forall \sigma \in G, m, m' \in M,$

(b) $(\sigma\tau)(m) = \sigma(\tau(m)) \quad \forall \sigma, \tau \in G, m \in M,$

(c) $1_G m = m \quad \forall m \in M.$

En cas que existeixi una tal acció diem que G **actua** sobre M, i anomenem G**-mòdul** a M.

A més, donats dos G-mòduls M i N, diem que una aplicació $f : M \to N$ és un **homomorfisme** de G-mòduls (o que és G**-lineal**) si

$$f(x + y) = f(x) + f(y) \quad \forall x, y \in M,$$
$$f(ax) = af(x) \quad \forall a \in G, x \in M.$$

Exemple B.2. Sigui L una extensió finita de Galois d'un cos k amb grup de Galois $G := \mathrm{Gal}(L/k)$, i sigui E una corba el·líptica sobre k. Llavors $E(L) \subseteq \mathbb{P}^2(L)$ (fixada una equació (3)) esdevé fàcilment un G-mòdul amb l'acció component a component.

Definició B.3. El 0**-èssim grup de cohomologia** d'un G-mòdul M, que denotem per $H^0(G, M)$, és el conjunt d'elements G-invariants de M, i.e.,

$$H^0(G, M) := M^G = \{m \in M \mid \sigma m = m \text{ per tot } \sigma \in G\},$$

que és G-mòdul.

Exemple B.4. Amb les hipòtesis del darrer exemple, gràcies al teorema fonamental de la Teoria de Galois,

$$H^0(\mathrm{Gal}(L/k), L) = K, \quad H^0(\mathrm{Gal}(L/k), L^\times) = K^\times, \quad H^0(\mathrm{Gal}(L/k), E(L)) = E(K).$$

Definició B.5. Sigui M un G-mòdul. Definim el grup d'1-**cocadenes** de G a M com

$$C^1(G, M) = \{\text{aplicacions } f : G \to M\}.$$

El grup d'1-**cocicles**, o d'**homomorfismes creuats**, (de G a M) són les 1-cocadenes que compleixen la **condició de cocicle**

$$Z^1(G, M) = \left\{ f \in C^1(G, M) \;\mid\; f(\sigma\tau) = f(\sigma) + \sigma f(\tau) \quad \forall \sigma, \tau \in G \right\}.$$

Definim el grup d'1-**cofronteres**, o d'**homomorfismes creuats principals** (de G a M) pel conjunt de 1-cocadenes que compleixen la **condició de covora**

$$B^1(G, M) = \left\{ f \in C^1(G, M) \;\mid\; \exists m \in M \text{ tal que } f(\sigma) = \sigma m - m \; \forall \sigma \in G \right\}.$$

Amb aquestes definicions, tenim que $B^1(G, M) \subset Z^1(G, M)$. El **primer grup de cohomologia** d'un G-mòdul M és el grup abelià quocient (amb la operació de M)

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

que també és un G-mòdul.

Donat un 1-cocicle $f \in Z^1(G, M)$, denotem la seva classe dins de $H^1(G, M)$ per $\{f\}$.

Exemple B.6. Si G actua trivialment sobre M (i.e., $\sigma m = m \quad \forall (\sigma, m) \in G \times M$), tenim que $H^0(G, M) = M$ i $H^1(G, M) = \mathrm{Hom}(G, M)$.

Definició B.7. Una successió de G-mòduls (i G-homomorfismes)

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

es diu **exacta a** M_i si $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$. La successió es diu **exacta** si és exacta a cada M_i.

Proposició B.8. *Considerem una successió curta de G-mòduls*

$$0 \longrightarrow M \xrightarrow{\phi} N \xrightarrow{\psi} P \longrightarrow 0.$$

Llavors obtenim una successió llarga exacta de G-mòduls

$$\begin{array}{ccccccc} 0 \longrightarrow & H^0(G,M) & \xrightarrow{\phi_0} & H^0(G,N) & \xrightarrow{\psi_0} & H^0(G,P) & , \\ & & & & & \downarrow{\scriptstyle \delta_0} & \\ & H^1(G,P) & \xleftarrow{\psi_1} & H^1(G,N) & \xleftarrow{\phi_1} & H^1(G,M) & \end{array}$$

on l'homomorfisme δ, que s'anomena connecting*, es defineix de la manera següent:*

Sigui $p \in H^0(G,P)$. Triem un element $n \in N$ tal que $\psi(n) = p$. Definim $\delta(p)$ com la classe $\{\sigma \mapsto \sigma n - n : G \mapsto M\} \in H^1(G,M)$ (pensant M dins de N via la injecció ϕ)[31].

Demostració. Veiem que $\delta_0(p)$ està ben definit. Si prenem un $n' \in N$ diferent de n tal que $\psi_0(n') = p$, n'obtenim un altre pretendent a $\delta(p)$ llur diferència amb l'anterior és $\{\sigma \mapsto \sigma(n'-n) - (n'-n)\}$, que és classe d'una covora perquè $n' - n \in \mathrm{Ker}(\psi_0) = Im(\phi_0) = M$.

La successió és exacta a $H^0(G,P)$, ja que $\mathrm{Ker}(\delta_0) = \{p \in H^0(G,P) \mid \sigma n = n \text{ per tot } \sigma \in G, n \in N \text{ tal que } \psi(n) = p\} = \mathrm{Im}(\psi_0)$. També és exacta a $H^1(G,M)$, atès que $\mathrm{Im}(\delta_0) = \{\{\sigma \mapsto \sigma n - n : G \to M\} \mid \psi_0(n) \in H^0(G,P)\} = Ker(\phi_1)$.

Veiem l'exactitud a $H^1(G,N)$. D'una banda, si $\{f\} \in \mathrm{Im}(\phi_1)$, està clar que $\{f \circ \psi_1\} = 0$ (atès que $\phi_1 \circ \psi_1 = 0$), i $\{f\} \in \mathrm{Ker}(\psi_1)$. D'altra banda, si prenem $\{f\} \in \mathrm{Ker}(\psi_1)$, notem que la imatge de f està continguda dins de $\mathrm{Ker}(\psi) = \mathrm{Im}(\phi) \subset N$ (de la successió curta), i que $\phi : M \to Im(\phi)$ és invertible i la seva inversa és G-lineal. Prenent la classe $\{\phi^{-1} \circ f\} \in H^1(G,M)$ obtenim un element de la preimatge de $\{f\}$, i $\{f\} \in \mathrm{Im}(\phi_1)$.

Finalment, és senzill veure que la presa d'invariants preserva l'exactitud de la successió curta, llevat que ψ no ha de ser necessàriament exhaustiva. □

Definició B.9. Sigui H un subgrup de G, i M un G-mòdul. Llavors, és clar que M és també un H-mòdul, i que qualsevol 1-cocadena (resp. cocicle, resp. covora) de G a M

[31] Els subíndexs dels morfismes hi són perquè, donat $\varphi : M \to N$, tenim $\varphi_i : H^i(G,M) \to H^i(G,N)$ i un morfisme connecting $\delta_i : H^i(G,M) \to H^{i+1}(G,N)$.

esdevé, mitjançant la restricció a H, una 1-cocadena (resp. cocicle, resp. covora) de H a M. D'aquesta manera definim l'**homomorfisme restricció**

$$\mathrm{Res} : H^1(G, M) \to H^1(H, M).$$

Definició B.10. Sigui H un subgrup normal de G, i M un G-mòdul. Llavors M^H és un G/H-mòdul, i una covora $f : G/H \to M^H$ defineix una covora de G a M amb la composició

$$\begin{array}{ccc} G & \overset{\mathrm{Inf}(f)}{\dashrightarrow} & M \\ \downarrow & & \uparrow \\ G/H & \xrightarrow{f} & M^H \end{array}$$

i d'aquesta manera obtenim l'**homomorfisme inflació**

$$\mathrm{Inf} : H^1(G/H, M^H) \to H^1(G, M).$$

Proposició B.11. *Sigui M un G-mòdul i H un subgrup normal de G. La següent successió, que anomenada* **inflació-restricció**

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{Inf} H^1(G, M) \xrightarrow{Res} H^1(H, M)$$

és exacta.

Demostració. Seguint les definicions s'obté que $\mathrm{Res} \circ \mathrm{Inf} = 0$,; aleshores falta veure $\mathrm{Ker}(\mathrm{Res}) \subseteq \mathrm{Im}(\mathrm{Inf})$. Sigui g un 1-cocicle amb $\mathrm{Res}(\{g\}) = 0$. Per tant dóna un $m \in M$ tal que

$$g(\tau) = \tau m - m \quad \text{per tot } \tau \in H,$$

i restant a g la 1-covora (de G a M) $\sigma \mapsto \sigma m - m$ n'obtenim un 1-cocicle $f \in Z^1(G, M)$ de la mateixa classe complint $f(\tau) = 0$ per tot $\tau \in H$. De la condició de cocicle aplicada a $\sigma \in G$ i $\tau \in H$ s'obté

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau) = f(\sigma),$$

i per tant $f(\sigma)$ depèn només de la classe de σ a G/H. A més, com que $H \lhd G$, existeix un $\tau' \in H$ de manera que $\tau\sigma = \sigma\tau'$. Aplicant que f factoritza a G/H i la condició de cocicle,

obtenim

$$f(\sigma) = f(\sigma\tau') = f(\tau\sigma) = f(\tau) + \tau f(\sigma) = \tau f(\sigma).$$

d'on $f(\sigma) \in M^H$, provant $\{f\} \in \mathrm{Im}(\mathrm{Inf})$.

Per veure que Inf és injectiva, prenem un 1-cocicle f amb $\mathrm{Inf}(\{f\}) = 0$. Existeix un $m \in M$ tal que $f(\sigma) = \sigma m - m$ per tot $\sigma \in G$. Però f depèn només de $\sigma(\mathrm{mod}\ H)$, així que

$$\sigma m - m = \sigma\tau m - m \quad \text{per tot } \tau \in H.$$

Prenent $\sigma = 1_G$ observem que $\tau m - m = 0$, és a dir $m \in M^H$, i per tant $\{f\} = 0 \in H^1(G/H, M^H)$. □

Proposició B.12. *Si G té ordre m, llavors $mH^1(G, M) = 0$.*

Demostració. Consulteu [MIL] §IV 1.6. □

B.2 Cohomologia de grups de Galois infinits

Definició B.13. Sigui $(I, \leq)$ un conjunt parcialment ordenat i dirigit[32]. Sigui $(G_i)_{i\in I}$ una família de grups, i suposem que tenim una família d'homomorfismes $f_{ij} : G_j \to G_i$ per tot $i \leq j$ amb les propietats

(a) $f_{ii} = \mathrm{id}_{G_i}$,

(b) $f_{ik} = f_{ij} \circ f_{jk}$ per tot $i \leq j \leq k$.

Llavors, el conjunt $((G_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ s'anomena **sistema invers** de grups i morfismes sobre I, i anomenem **morfismes de transició** als morfismes f_{ij}.

Definim el **límit invers** del sistema invers $((G_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ com el següent subgrup del producte directe dels G_i

$$\varprojlim_{i\in I} G_i = \left\{ a \in \prod_{i\in I} G_i \mid a_i = f_{ij}(a_j) \text{ per tot } i \leq j \in I \right\}.$$

[32]És a dir, un conjunt dotat d'una relació binària reflexiva, antisimètrica i transitiva, amb la hipòtesi addicional que qualsevol parella d'elements té una cota superior en comú.

A l'hora de treballar amb el límit invers, sovint s'obvien els morfismes de transició i el conjunt I.

Si un grup és límit invers d'un sistema invers de grups finits, diem que és un grup **profinit**.

Sigui k un cos perfecte, i $\overline{k}$ una clausura algebraica de k (per tant, $\overline{k}/k$ és Galois). Durant tot aquest apartat, denotem per G el grup $\mathrm{Gal}(\overline{k}/k)$. Es pot veure que

$$G \cong \varprojlim_{L/k \text{ finita Galois, } L\subset\overline{k}} \mathrm{Gal}(L/k),$$

i per tant el grup G és profinit. Com a tal, vé dotat d'una topologia natural, anomenada **topologia de Krull**, on una base d'entorns del zero són els subgrups de G de la forma $\mathrm{Gal}(\overline{k}/F)$ on F/k és una extensió finita de Galois.

Definició B.14. Un G-mòdul M es diu **discret** quan l'acció $G \times M \to M$ és contínua per la topologia de Krull a G i la topologia discreta a M. Això equival per definició a

$$M = \bigcup_{H\subset G \text{ obert}} M^H.$$

A més, donats dos G-mòduls M i N, diem que una aplicació $f : M \to N$ és un **homomorfisme** de G-mòduls (o que és **G-lineal**) si

$$f(x+y) = f(x) + f(y) \quad \forall x, y \in M,$$
$$f(ax) = af(x) \quad \forall a \in G, x \in M.$$

Exemple B.15. Considerem E una corba el·líptica sobre un cos k. Llavors $E(\overline{k})$ esdevé fàcilment un G-mòdul amb l'acció component a component. És discret ja que $E(\overline{k}) = \cup_{L/k \text{ finita}, L\subset\overline{k}} E(L)$.

Definició B.16. El **0-èssim grup de cohomologia** d'un G-mòdul discret M, que denotem per $H^0(G, M)$, és el conjunt d'elements G-invariants de M, i.e.,

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

Podríem definir el primer grup de cohomologia com ho hem fet a l'apartat anterior. Ens serà, però, d'utilitat en el cas de G-mòduls discrets, afegir certes condicions de continuitat.

Definició B.17. Suposem G equipat amb la topologia de Krull, i sigui M un G-mòdul discret amb la topologia discreta. Definim el grup d'1-**cocadenes contínues** de G a M com el conjunt

$$C^1_{\text{cont}}(G,M) = \{\text{aplicacions contínues} f : G \to M\}.$$

El grup d'1-**cocicles continus**, o d'**homomorfismes creuats continus**, (de G a M) són les 1-cocadenes contínues que compleixen la **condició de cocicle**

$$Z^1_{\text{cont}}(G,M) = \left\{ f \in C^1_{\text{cont}}(G,M) \;\mid\; f(\sigma\tau) = f(\sigma) + \sigma f(\tau) \quad \forall \sigma,\tau \in G \right\}.$$

Definim el grup d'1-**covores contínues**, o d'**homomorfismes creuats principals continus** (de G a M) pel conjunt de 1-cocadenes contínues que compleixen la **condició de covora**

$$B^1_{\text{cont}}(G,M) = \left\{ f \in C^1_{\text{cont}}(G,M) \;\mid\; \exists m \in M \text{ tal que } f(\sigma) = \sigma m - m \;\forall \sigma \in G \right\}.$$

Amb aquestes definicions, està clar que tenim la cadena de subgrups $B^1_{\text{cont}}(G,M) \subset Z^1_{\text{cont}}(G,M) \subset Z^1(G,M)$.

Observació B.18. Cal notar que per qualsevol $m \in M$ fix, l'aplicació $G \mapsto M : \sigma \mapsto m^\sigma - m$ és contínua, ja que és suma de dues aplicacions contínues (M vé equipada amb la topologia discreta i l'acció de G a M és contínua), i $C^1_{\text{cont}}(G,M)$ és un grup. Per tant, denotem el grup d'1-**covores** de G a M per

$$B^1(G,M) := \left\{ f \in C^1(G,M) \;\mid\; \exists m \in M \text{ tal que } f(\sigma) = \sigma m - m \;\forall \sigma \in G \right\},$$

i $B^1_{\text{cont}}(G,M) = B^1(G,M)$.

Definició B.19. El **primer grup de cohomologia** d'un G-mòdul discret M és el grup abelià quocient (amb la operació de M)

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

Donat un 1-cocicle $f \in Z^1_{\text{cont}}(G,M)$, denotem la seva classe dins de $H^1(G,M)$ per $\{f\}$

Exemple B.20. Si G actua trivialment sobre M (i.e., $\sigma m = m \quad \forall(\sigma, m) \in G \times M$), tenim que $H^0(G, M) = M$ i que $H^1(G, M)$ és el grup $\mathrm{Hom}_{\mathrm{cont}}(G, M)$ d'homomorfismes continus de G a M.

Proposició B.21. *Considerem la successió curta de G-mòduls*

$$0 \longrightarrow M \xrightarrow{\phi} N \xrightarrow{\psi} P \longrightarrow 0.$$

Aquesta indueix una successió llarga exacta de G-mòduls

$$\begin{array}{ccccccc} 0 \longrightarrow & H^0(G,M) & \xrightarrow{\phi_0} & H^0(G,N) & \xrightarrow{\psi_0} & H^0(G,P) & , \\ & & & & & \downarrow{\scriptstyle \delta_1} & \\ & H^1(G,P) & \xleftarrow{\psi_1} & H^1(G,N) & \xleftarrow{\phi_1} & H^1(G,M) & \end{array}$$

on l'homomorfisme δ[33] *es defineix com a la proposició B.21.*

Demostració. Similar a la de la proposició B.8. □

Definició B.22. Sigui M un G-mòdul discret, i considerem L/k una extensió finita de Galois. Llavors, $\mathrm{Gal}(\overline{k}/L)$ és un subgrup obert de G, i M és naturalment un $\mathrm{Gal}(\overline{k}/L)$-mòdul discret. D'aquesta manera definim l'**homomorfisme restricció**

$$\mathrm{Res} : H^1(G, M) \to H^1(\mathrm{Gal}(\overline{k}/L), M).$$

Definició B.23. Sigui M un G-mòdul i $\mathrm{Gal}(\overline{(k)}/L)$ un subgrup normal de G. Observem que $G/\mathrm{Gal}(\overline{k}/L) \equiv G(L/k)$, i que el submòdul $M^{\mathrm{Gal}(\overline{k}/L)}$ té una estructura de $\mathrm{Gal}(L/k)$-mòdul. Qualsevol 1-cocicle $f : \mathrm{Gal}(L/k) \to M^{\mathrm{Gal}(\overline{k}/L)}$ defineix un 1-cococicle de G a M amb la composició

$$\begin{array}{ccc} G & \xrightarrow{\mathrm{Inf}(f)} & M \\ \downarrow{\scriptstyle \mathrm{proj}} & & \uparrow{\scriptstyle \mathrm{incl}} \\ \mathrm{Gal}(L/k) & \xrightarrow{f} & M^{\mathrm{Gal}(\overline{k}/L)}, \end{array}$$

i d'aquesta manera obtenim l'**homomorfisme inflació**

$$\mathrm{Inf} : H^1(\mathrm{Gal}(L/k), M^{\mathrm{Gal}(\overline{k}/L)}) \to H^1(G, M).$$

[33] Anomenat homomorfisme *connecting* a la literatura.

Proposició B.24. *Sigui M un G-mòdul i $Gal(\overline{(}k)/L)$ un subgrup normal de G. La següent successió, que anomenem d'***inflació-restricció**

$$0 \to H^1(\mathrm{Gal}(L/k), M^{\mathrm{Gal}(\overline{k}/L)}) \stackrel{Inf}{\to} H^1(G, M) \stackrel{Res}{\to} H^1(\mathrm{Gal}(\overline{k}/L), M)$$

és exacta.

Demostració. Similar a la de la proposició B.24. □

Proposició B.25 (Teorema 90 de Hilbert)**.** *Sigui L una extensió finita de Galois d'un cos k. Llavors, $H^1(Gal(L/k), L^\times) = 0$. A més, $H^1(G, \overline{k}^\times) = 0$..*

Demostració. Veieu [MIL] §IV 1.3, 1.8(a). □

Corol·lari B.26. *Prenem un $m \geq 1$ enter, i suposem que $char(k) = 0$ o que $char(k)$ no divideix m. Denotem per*

$$\mu_m(k) = \{\zeta \in k^\times \mid \zeta^n = 1\}.$$

Llavors

$$H^1(G, \mu_m) \cong k^\times/(k^\times)^m.$$

Demostració. Considerem la successió exacta

$$1 \longrightarrow \mu_m(\overline{k}) \stackrel{incl}{\longrightarrow} \overline{k}^\times \stackrel{z\mapsto z^m}{\longrightarrow} \overline{k}^\times \longrightarrow 1\ .$$

Aplicant la proposició B.21 i el teorema 90 de Hilbert tenim la successió exacta

$$1 \longrightarrow k^\times \stackrel{z\mapsto z^m}{\longrightarrow} k^\times \stackrel{\delta}{\longrightarrow} H^1(G, \mu_m(\overline{k})) \longrightarrow 1\ ,$$

d'on deduïm el resultat. □

C Corbes el·líptiques sobre $\mathbb{C}$

En aquesta secció donem una breu descripció de les corbes el·líptiques sobre el cos $\mathbb{C}$. Com veurem, hi intervenen majoritàriament tècniques analítiques.

C.1 Xarxes, bases i funcions doblement periòdiques

Definició C.1. Una **xarxa** a $\mathbb{C}$ és un subgrup additiu, que denotem per Λ, generat additivament per dos nombres complexos ω_1, ω_2 (anomenats **base** de Λ) linealment independents com a vectors sobre $\mathbb{R}$, i.e.,

$$\Lambda := \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \qquad \text{amb } \omega_1, \omega_2 \neq 0 \text{ i } \operatorname{Im}\left(\frac{\omega_2}{\omega_1}\right) \neq 0.$$

Definició C.2. Anomenem **paral·lelogram fonamental** (o, a vegades, **domini fonamental**) per Λ a qualsevol conjunt de la forma

$$D := \{a + \alpha\omega_1 + \beta\omega_2 \mid 0 \leq \alpha, \beta < 1\}$$

on $a \in \mathbb{C}$ és fix i ω_1, ω_2 és una base per Λ.

Definició C.3. Una **funció doblement periòdica** f respecte la xarxa Λ és una funció f a $\mathbb{C}$ tal que

$$f(z + \omega) = f(z), \quad \forall z \in \mathbb{C}, \forall \omega \in \Lambda.$$

Si ω_1, ω_2 és una base per Λ, aquesta condició equival a

$$\begin{cases} f(z + \omega_1) = f(z) \\ f(z + \omega_1) = f(z) \end{cases}, \quad \forall z \in \mathbb{C}, \forall \omega \in \Lambda.$$

D'una funció doblement periòdica i meromorfa en diem **funció el·líptica**.

Veiem que donar una funció doblement periòdica equival a donar una funció ben definida sobre $\mathbb{C}/\Lambda$[34]. El conjunt de funcions el·líptiques per Λ, que denotem $\mathbb{C}(\Lambda)$, és clarament un cos amb les operacions usuals de suma i producte.

[34] A la literatura també es sol anomenar funció doblement periòdica a una funció d'aquest tipus, sense diferenciar-les. En aquest cas, es sol parlar de $\mathbb{C}/\Lambda$ enlloc del paral·lelogram fonamental respecte Λ.

Proposició C.4. *Sigui $f \in \mathbb{C}(\Lambda)$ una funció el·líptica, i D un paral·lelogram fonamental per Λ tal que f no té zeros ni pols a la frontera de D (que existeix, ja que sinó obtindríem una quantitat no-numerable de pols, i f no podria ser meromorfa). Llavors, tenim*

(a) $\sum_{P \in D} \operatorname{Res}_P(f) = 0,$

(b) $\sum_{P \in D} \operatorname{ord}_P(f) = 0,$

(c) $\sum_{P \in D} \operatorname{ord}_P(f) \cdot P \equiv 0 \mod \Lambda = 0,$

on $\operatorname{ord}_P(f)$ és l'ordre[35] *de P com a zero (en positiu) o pol (en negatiu) de f, i $\operatorname{Res}_P(f)$ és el residu de f a P.*

Demostració. Els punts (a) i (b) són directes aplicant el teorema dels residus a f i a f'/f (tenint en compte que $\operatorname{Res}_P(f'/f) = \operatorname{ord}_P(f)$) respectivament. El punt (c) s'obté aplicant el mateix teorema a $\mathrm{id} \cdot f'/f$ (veure [SIL] §VI.2 2.2). □

Definició C.5. Sigui f una funció el·líptica (per Λ) i D un paral·lelogram fonamental de Λ. Definim l'**ordre** de f com la suma dels ordres dels pols de f a D.

Corol·lari C.6. *Tota funció el·líptica no constant té almenys ordre dos. Similarment, tota funció el·líptica no constant té almenys un zero.*

Demostració. Prenem una funció el·líptica no constant f. Com que tota funció holomorfa acotada a tot $\mathbb{C}$ és constant (gràcies al teorema de Liouville), f no pot ser holomorfa i ha de tenir algun pol. Si f té només un pol simple P, el primer punt de la proposició ens dóna $\operatorname{Res}_P(f) = 0$, que contradiu el fet que P sigui un pol simple.

Finalment, si f és una funció el·líptica sense zeros, $1/f$ és una funció el·líptica sense pols, i per tant és constant. □

[35] S'anomena **ordre** d'un zero o un pol z_0 de f al mínim enter n tal que l'n-èssim coeficient de la sèrie de Laurent centrada a z_0 sigui no nul.

C.2 La funció $\wp$ de Weierstrass

De l'últim corol·lari n'obtenim que, en algun sentit, les funcions el·líptiques (respecte Λ) no constants més simples són aquelles que tenen un pol doble a cada punt de Λ. Un exemple molt important d'una tal funció és la **funció $\wp$ de Weierstrass**

$$\wp(z) := \frac{1}{z} + \sum_{\omega\in\Lambda,\omega\neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \tag{17}$$

$$\wp'(z) := \sum_{\omega\in\Lambda} \frac{-2}{(z-\omega)^3}.$$

Proposició C.7. *Aquestes dues sèries convergeixen normalment*[36] *sobre qualsevol conjunt compacte de $\mathbb{C}$. A més, llurs sumes $\wp$ i $\wp'$ són funcions meromorfes doblement periòdiques.*

Demostració. Veieu [MIL] §III 2.4. □

Observació C.8. De la convergència normal de $\wp$ n'extreiem la convergència uniforme (i també l'absoluta), i en conseqüència podem calcular-ne la derivada tot derivant sumand a sumand. Així $\wp'$ és efectivament la derivada de $\wp$.

De fet, la següent proposició ens mostra com $\wp$ vé únicament determinada per la condició sobre els pols.

Proposició C.9. *Sigui Λ una xarxa a $\mathbb{C}$. La funció $\wp$ de Weierstrass determinada per aquesta xarxa és, llevat de suma i producte per constants no nul·les, la única funció el·líptica d'ordre dos amb pols d'ordre dos a Λ.*

Demostració. Sigui f una funció el·líptica amb només pols d'ordre dos als punts de Λ. Llavors, $z \mapsto f(z) - f(-z)$ és una funció doblement periòdica d'ordre com a molt u, i a més és senar, per tant és constant i nul·la. N'obtenim que f és una funció parella d'ordre dos i, després de sumar i multiplicar per constants adequades, la seva sèrie de Laurent centrada a zero pren la forma

$$f(z) = z^{-2} + 0 + z^2 g(z) \quad \text{amb } g \text{ holomorfa a prop de } z = 0.$$

[36] Una sèrie $\sum_n f_n$ de funcions holomorfes **convergeix normalment** a un subconjunt $A \subseteq \mathbb{C}$ quan $\sum_n \sup_{z\in A} |f_n(z)|$ convergeix. Una sèrie de funcions meromorfes **convergeix normalment** si, quan elidim un nombre finit de termes f_i, obtenim una sèrie normalment convergent de funcions holomorfes.

Així, f i $\wp$ ([SIL] §VI 3.1(b)) són holomorfes sobre $\mathbb{C}\backslash\Lambda$, i $\lim_{z\to 0}(f(z)-\wp(z))=0$. Per tant, la funció doblement periòdica $g: z\mapsto f(z)-\wp(z)$, holomorfa sobre $\mathbb{C}\backslash\Lambda$, estén a una funció doblement periòdica i holomorfa sobre $\mathbb{C}$. Per l'últim corol·lari, g és constant, i com que $g(0)=0$ (per evitar la singularitat), obtenim $f=\wp$. □

El cos de funcions el·líptiques

Definició C.10. Sigui Λ una xarxa a $\mathbb{C}$. Definim la **sèrie d'Eisenstein** de pes $2k$ (per Λ) com

$$G_{2k}(\Lambda)=\sum_{\omega\in\Lambda,\omega\neq 0}\omega^{-2k}.$$

Proposició C.11. *Per tot enter $k\geq 2$, $G_{2k}(\Lambda)$ és absolutament convergent*

Demostració. Veieu [SIL] §VI 3.1(a). □

Proposició C.12. *Tenim la següent relació algebraica entre $\wp$ i $\wp'$*

$$\wp'(z)^2=4\wp(z)^3-60G_4(\Lambda)\wp(z)-140G_6(\Lambda).$$

Demostració. Per tot z amb $|z|<|\omega|$,

$$\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}=\frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2}-1\right)=\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}.$$

Substituïnt-ho a (17), commutant els sumatoris (gràcies a la convergència normal de (17)) i observant que $\sum_{\omega\in\Lambda,\omega\neq 0}\omega^{2k+1}=0$ per tot $k\in\mathbb{Z}$, obtenim la següent sèrie de Laurent de $\wp$ centrada a $z=0$,

$$\wp(z)=\frac{1}{z^2}+\sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}.$$

A partir d'aquí, només cal expressar adequadament $\wp'(z)^2$ i $\wp(z)^3$ i tenir en compte que són doblement periòdiques per veure que la igualtat es compleix per tot $z\in\mathbb{C}\backslash\Lambda$ (veieu [SIL] §VI 3.5 per més detalls). □

Proposició C.13. *Tota funció el·líptica es pot expressar com a funció racional de $\wp$ i $\wp'$, i.e., $\mathbb{C}(\Lambda)=\mathbb{C}(\wp,\wp')$.*

Demostració. Veieu [MIL] §III 2.7. □

Corbes el·líptiques com a superfícies de Riemann

Recordem que una **superfície de Riemann** és un espai topològic connex de Hausdorff X que admet una base numerable pel seu conjunt d'oberts, juntament amb una **estructura complexa** [37].

Observació C.14. El conjunt $\mathbb{C}/\Lambda$, anomenat **tor complex**, és una superfície de Riemann amb la topologia quocient.

Per donar-li una estructura complexa, partim de la projecció $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$. Per a cada obert $U_i \in \mathbb{C}/\Lambda$ escollim un obert $V_i \in \mathbb{C}$ sense punts equivalents mòdul Λ i tal que $\pi(V_i) = U_i$. Prenem llavors la carta local $\psi_i := \pi^{-1} : U_i \to V_i$.

Està clar que les cartes són compatibles dos a dos, ja que si $z \in \psi_i(U_i \cap U_j)$, veiem que $\pi(z) = \pi(\phi_j(\psi_i^{-1}(z)))$, i la funció $z \mapsto z - \phi_j(\psi_i^{-1}(z)) \in \Lambda$ és contínua, i per tant constant. A partir d'aquí obtenim la biholomorfia de $\phi_2 \circ \phi_1^{-1}$.

En aquest apartat veiem que tota superfície de Riemann $\mathbb{C}/\Lambda$ és isomorfa a una corba el·líptica sobre $\mathbb{C}$ i viceversa. El primer resultat ens el dóna la següent

Proposició C.15. (*a*) *La corba*

$$E(\Lambda)/\mathbb{C} : Y^2Z = 4X^3 - 60G_4(\Lambda)XZ^2 - 140G_6(\Lambda)Z^3$$

és una corba el·líptica.

(*b*) *A més, l'aplicació*

$$\phi : \mathbb{C}/\Lambda \to E(\Lambda)(\mathbb{C}), \quad \begin{cases} z \mapsto (\wp(z) : \wp'(z) : 1), & z \neq 0 \\ 0 \mapsto (0 : 1 : 0) \end{cases}$$

és un isomorfisme de grups.

[37] Vagament, per qualsevol obert U_i d'un recobriment per oberts de $X = \cup_i U_i$, tenim un homeomorfisme (anomenat **carta**) z_i de U_i a un obert qualsevol de $\mathbb{C}$. A més, aquests homeomorfismes han de ser compatibles dos a dos, i.e., $z_i \circ z_j^{-1} : z_j(U_i \cap U_j) \to z_i(U_i \cap U_j)$ i la seva inversa han de ser holomorfs (es diu que són biholomorfs). Veure [MIL] §III.3 per més detalls.

Demostració. (a) Sigui $\{\omega_1, \omega_2\}$ una base per la xarxa Λ, i escrivim $\omega_3 = \omega_1 + \omega_2$. Atès que $\wp'$ és una funció el·líptica senar, observem que, per cada $i = 1, 2, 3$

$$\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(\frac{-\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right),$$

així que $\wp'(\omega_i/2) = 0$. De la proposició C.12 tenim que $\wp(\omega_i/2)$ són arrels del polinomi $f(X) = 4X^3 - 60G_4(\Lambda)X - 140G_6(\Lambda)$. Per veure la no-singularitat de $E(\Lambda)$ n'hi ha prou amb comprovar que les tres arrels $\wp(\omega_i/2)$ són diferents.

La funció $z \mapsto \wp(z) - \wp(\omega_i/2)$ és parella, així que té com a mínim un zero doble a $z = \omega_i/2$. No obstant, és una funció el·líptica d'ordre 2, i per la proposició C.4(b) només té un zero al paral·lelogram $D_0 := \{\alpha\omega_1 + \beta\omega_2 \mid \alpha, \beta \in [0, 1)\}$. Això ens diu que, dins de D_0, $\wp(z)$ només pren el valor $\wp(\omega_i/2)$ a $z = \omega_i/2$, així que $\omega_i/2 \neq \omega_j/2$ per $i \neq j$.

(b) La imatge de ϕ està continguda a $E(\Lambda)(\mathbb{C})$ gràcies a la proposició C.12 i al punt anterior, i està ben definida per la doble periodicitat de $\wp$ i $\wp'$ respecte Λ.

Per veure que ϕ és exhaustiva, sigui $(x : y : 1) \in E(\Lambda)(\mathbb{C})$. Llavors $z \mapsto \wp(z) - x$ és una funció el·líptica no constant, així que per la proposició C.6 té un zero $z = a$. Se segueix de la proposició C.12 que $\wp'(a)^2 = y^2$. Com que $\wp'$ és senar i $\wp$ parella, intercanviant a per $-a$ si cal obtenim $\wp'(a) = y$. Llavors, $\phi(a) = (x, y)$, i ϕ és exhaustiva.

Per veure la injectivitat, suposem que $\phi(z_1) = \phi(z_2)$. Aleshores $z \mapsto \wp(z) - \wp(z_1)$ és una funció el·líptica d'ordre dos que s'anul·la a z_1, $-z_1$ i z_2. Si assumim que $2z_1 \notin \Lambda$, és clar que $z_2 \equiv \pm z_1 \pmod{\Lambda}$ per alguna elecció del signe de z_1. Per aquest fet i per la hipòtesi inicial,

$$\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z_1),$$

i això implica $z_1 \equiv z_2 \pmod{\Lambda}$ atès que $\wp'(z_1) \neq 0$ (ja que, pel punt anterior, si $\wp'(z_1) = 0$, tenim $f(\wp(z_1)) = 0$, i llavors z_1 hauria de ser alguna de les tres arrels $\omega_i/2$ de f, però no pot ser perquè $2z_1 \notin \Lambda$). Pel cas $2z_1 \in \Lambda$, la funció el·líptica

parella d'ordre dos $z \mapsto \wp(z) - \wp(z_1)$ té un zero doble a z_1 i s'anul·la a z_2. Concluïm, gràcies a la proposició C.4(b), que $z_1 \equiv z_2 \pmod{\Lambda}$, i per tant ϕ és injectiva.

Per comprovar que ϕ és homomorfisme, observem primer que $\mathbb{C}/\Lambda$ és un grup amb la suma. Considerem ara $z_1, z_2 \in \mathbb{C}$. La proposició a [SIL] §VI 3.4 ens indica que podem trobar una funció el·líptica $f \in \mathbb{C}(\Lambda)$ amb divisor

$$\operatorname{div}(f) = [z_1 + z_2] - [z_1] - [z_2] + [0].$$

Llavors, la proposició C.13 ens permet expressar f com una funció racional de $\wp, \wp'$, i.e., $f(z) = \tilde{F}(\wp(z), \wp'(z))$ amb $\tilde{F} \in \mathbb{C}(X, Y)$. Si F és la projecció de $\tilde{F}$ al cos $\mathbb{C}(E(\Lambda))$ de funcions racionals sobre $E(\Lambda)$, podem escriure

$$\operatorname{div}(F) = [\phi(z_1 + z_2)] - [\phi(z_1)] - [\phi(z_2)] + [\phi(0)],$$

i de [SIL] §III 3.5 n'obtenim $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$.

□

Observació C.16. De fet, ϕ també és un morfisme analític entre superfícies de Riemann. Consulteu [SIL] §VI 3.6 o [MIL] §III 3.7.

Amb això hem verificat que els grups $\mathbb{C}/\Lambda$ i $E(\Lambda)(\mathbb{C})$ són estructuralment el mateix, el que indica que tot tor complex és una corba el·líptica. La següent proposició ens assegura l'oposat.

Proposició C.17. *El grup de Mordell-Weil d'una corba el·líptica $E/\mathbb{C}$ és isomorf sobre $\mathbb{C}$ a $E(\Lambda)(\mathbb{C})$ per alguna xarxa Λ.*

Demostració. Com que $\mathbb{C}$ és algebraicament tancat, la proposició 3.4(c) classifica (llevat d'isomorfisme) les corbes el·líptiques mitjançant els respectius j-invariants. Donat una xarxa Λ, la corba

$$E(\Lambda)/\mathbb{C} : Y^2Z = 4X^3 - 60G_4(\Lambda)XZ^2 - 140G_6$$

té discriminant $\Delta(\Lambda) = (60G_4)^3 - 27(140G_6)^2$ i j-invariant

$$j(\Lambda) = \frac{1728(60G_4(\Lambda))^3}{(60G_4(\Lambda))^3 - 27(140G_6(\Lambda))^2}.$$

Per $c \in \mathbb{C}^\times$, tenim $G_4(c\Lambda) = c^{-4}G_4(\Lambda)$ i $G_6(c\Lambda) = c^{-6}G_6(\Lambda)$, i llavors $j(c\Lambda) = j(\Lambda)$. Això ens permet definir

$$j : \mathbb{C}^\times \to \mathbb{C}, \quad j(\tau) = j(\mathbb{Z}\tau + \mathbb{Z}).$$

De fet, com que $j(\tau) = j(\tau^{-1})$, podem considerar $j \in \mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.

Es pot veure que $j : \mathbb{H} \to \mathbb{C}$ és exhaustiva ([MIL] §V 2.2). Per tant, donada $E/\mathbb{C}$, existeix $\tau \in \mathbb{C}$ tal que $j(E) = j(\tau)$, i $E(\mathbb{C})$ és isomorf a $E(\mathbb{Z}\tau + \mathbb{Z})(\mathbb{C})$. □

Referències

[ATI] M.F.Atiyah, I.G. Macdonald, *Introducción al Álgebra Conmutativa*. Barcelona. Editorial Reverté. 1973.

[AV] J.S.Milne, *Abelian Varieties*. Disponible a `www.jmilne.org/math/`. 2008.

[BCDT] Christophe Breuil, Brian Conrad, Fred Diamond, Richard Taylor, *On the Modularity of Elliptic Curves over $\mathbb{Q}$: Wild 3-adic Exercises*. Journal of the American Mathematical Society 14 (4): pàg 843 a 939. doi:10.1090/S0894-0347-01-00370-8. 2001.

[BS] Manjul Bhargava, Arul Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*. arXiv:1007.0052. 2010.

[BSDI] B.J. Birch i H.P.F. Swinnerton-Dyer, *Notes on elliptic curves. I.*. Journal für die reine und angewandte Mathematik (Crelles Journal). Número 212, Pàgines 7 a 25. 1963.

[BSDII] B.J. Birch i H.P.F. Swinnerton-Dyer, *Notes on elliptic curves. II.*. Journal für die reine und angewandte Mathematik (Crelles Journal). Número 218, Pàgines 79 a 108. 1965.

[BZ] Benedict H. Gross i Don B. Zagier, *Heegner points and derivatives of L-series*. Inventiones Mathematicae 84 (2): pàg 225 a 320. doi:10.1007/BF01388809. MR0833192. 1986.

[CAS] J. W. S. Cassels, *Lectures On Elliptic Curves*. London Mathematical Society Student Texts. Cambridge University Press. Cambridge. 1991.

[COM] Salvador Comalada, *Elliptic curves with trivial conductor over quadratic fields.*. Pacific J. Math. Volume 144, Number 2 (1990), 237-258. Número 2, Pàgines 237 a 258. 1990.

[CW] J. Coates i A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*. Inventiones Mathematicae 39 (3): pàg 223 a 251. doi:10.1007/BF01402975. 1977.

[FT] J.S.Milne, *Fields and Galois Theory*. Disponible a `www.jmilne.org/math/`. 2011.

[FUL] William Fulton, *Algebraic Curves*. Reading, Massachusetts. The Benjamin/Cummings Publishing Company, INC. 1969.

[HAR] Hartshorne, R., *Algebraic Geometry*. New York. Springer-Verlag: 1977.

[HUS] Dale Husemöller, *Elliptic Curves*. New York. Springer-Verlag. 1986.

[JKS] D. Jeon, C. H. Kim i A. Schweizer, *Acta Arith. 113* no. 3, pàg 291 a 301, 2004.

[KT] Kazuya Kato i Fabien Trihan, *On the conjectures of Birch and Swinnerton-Dyer in characteristic* $p > 0$. Invent. Math. 153. 2003.

[MAZ] B. Mazur, *Modular curves and the Eisenstein ideal*. Inst. Hautes Études. Sci. Publ. Math. No. 47. Pàg. 33 a 186. 1978.

[MER] L. Merel, *Invent. Math. 124*, no. 1-3. pàg 437 a 449. 1996.

[MIL] J.S.Milne, *Elliptic Curves*. Charleston, South Carolina. BookSurge Publishers. 2006.

[SIL] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. New York. Springer-Verlag. 1994.

[SIL-TATE] Joseph H. Silverman i John Tate, *Rational Points on Elliptic Curves*. New York. BookSurge Publishers. 1992.

[STN] William A. Stein, *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach*. Disponible a `http://modular.math.washington.edu`. 2007.

[SU] Chris Skinner i Éric Urban, *The Iwasawa main conjectures for GL2*. En preparació. 2010.

[WIL] Andrew Wiles, *The Birch and Swinnerton-Dyer Conjecture*. Disponible a `http://www.claymath.org/millennium/`.

[WiTZH] *Teorema dels zeros de Hilbert.* Disponible a http://ca.wikipedia.org/wiki/Teorema_dels_zeros_de_Hilbert.