16

Notes del Seminari de Teoria de Nombres
(UB - UAB - UPC)

L'ALGORITME DE LIU PER A CORBES DE GÈNERE DOS

Edició a cura de

V. Rotger

Amb contribucions de

F. Creixell L. E. García X. Guitart
F. Bars V. Rotger S. Molina
S. Arias de Reyna X. Xarles

V. Rotger
Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Av. Victor Balaguer s/n 08800
Vilanova i la Geltrú (Barcelona)

Classificació AMS
Primària: 11F12, 11G18, 11G20, 11R52, 11S45
Secundària: 11G25, 11T71

Barcelona, 2007
ISBN: 84-934244-5-5.

Introducció

L'aritmètica de corbes de gènere més gran o igual que 2 és ben desconeguda, sobretot si ho comparem amb el vast coneixement que tenim actualment de les corbes el·líptiques i els espectaculars resultats que s'han obtingut en els darrers anys. De l'ampli ventall de teoremes i eines computacionals que disposem sobre l'aritmètica de corbes el·líptiques, molts d'ells són encara una incògnita en gènere superior.

Un exemple ben clar (entre d'altres que podriem triar) el trobem en l'estudi dels models d'aquestes corbes sobre l'anell d'enters d'un cos local o global.

Sigui K un cos de nombres i sigui $K_\wp$ la completació de K respecte el valor absolut no-arquimedià associat a un ideal primer $\wp$ de K. Sigui $\mathcal{O}_\wp$ l'anell d'enters de $K_\wp$ i $k_\wp$ el cos residual.

Si E és una corba el·líptica sobre $K_\wp$, existeixen tres models distingits de E sobre $\mathcal{O}_\wp$: el model minimal de Weierstrass $\mathcal{W}$, el model minimal regular $\mathcal{E}_{min}$ i el model de Néron $\mathcal{E}$. Tots tres són esquemes sobre l'espectre d'$\mathcal{O}_\wp$.

Tenen dimensió 2 i són la unió disjunta de dues corbes: la fibra tancada $\mathcal{W}_\wp$ (respectivament $\mathcal{E}_{min,\wp}$ i $\mathcal{E}_\wp$) sobre el cos finit $k_\wp$ i la fibra genèrica sobre $K_\wp$, que en tots tres casos no és altra que la corba el·líptica E.

Així doncs, tots tres models són birregularment equivalents perquè les respectives fibres genèriques (que són un obert dens de l'esquema) son totes tres isomorfes. Tot i així, en general els esquemes $\mathcal{W}$, $\mathcal{E}_{min}$ i $\mathcal{E}$ no són pas isomorfs: això succeeix quan $\wp$ és un primer de mala reducció d'E.

En aquest cas, $\mathcal{W}_\wp$ és una corba racional amb una singularitat nodal o cuspidal en un punt p. Si p és un punt regular en l'esquema sencer $\mathcal{W}$ (que ben potser malgrat p no ho sigui pas en la fibra tancada), aleshores $\mathcal{E}_{min} = \mathcal{W}$. En cas contrari, $\mathcal{E}_{min}$ es construeix a partir de $\mathcal{W}$ fent explotar tantes vegades com sigui necessari el punt p fins a obtenir un model regular.

En qualsevol cas, el model de Néron $\mathcal{E}$ es construeix a partir d'$\mathcal{E}_{min}$ senzillament substraient les singularitats de la fibra tancada $\mathcal{E}_{min,\wp}$.

Ja fa algunes dècades, Tate va descriure un algoritme per a calcular explícitament tots aquests models a partir d'una equació de Weierstrass qualsevol per a E.

Sigui ara C una corba de gènere més gran o igual que 2 sobre el mateix cos $K_\wp$. De nou existeixen dos models de C distingits sobre l'anell d'enters $\mathcal{O}_\wp$: el model estable $\mathcal{C}_{st}$ i el model minimal regular $\mathcal{C}_{min}$. Els dos poden considerar-se una generalització del model minimal de Weierstrass i el model minimal regular per a corbes el·líptiques, respectivament. El model de Néron troba la seva generalització natural en el context de les varietats abelianes; així, podem consideral el model de Néron $\mathcal{J}$ de la varietat Jacobiana J de C.

Una primera dificultat que ens trobem en considerar

aquests models enters de C és que el model estable $\mathcal{C}_{st}$ sobre l'espectre d'$\mathcal{O}_\wp$ no existeix pas sempre. Un teorema de Deligne-Mumford ens assegura però que existeix una extensió finita $L/K_\wp$ sobre la qual $C \times L$ admet un model estable. El càlcul i les propietats d'aquesta extensió (o extensions, ja que en general no n'existeix una de minimal) és una qüestió que no està resolta completament. En aquestes notes descrivim els treballs de Liu que resolen aquest problema en gènere dos.

En qualsevol cas, les possibles configuracions de la fibra tancada del model estable de $C \times L$ són prou conegudes. Si el gènere és 2, per exemple, tan sols n'hi ha *set* de possibles. Cal comparar aquest resultat amb el fet que hi ha tres possibles reduccions del model minimal de Weierstrass d'una corba el·líptica: una corba llisa de gènere 1 o una corba racional amb una singularitat nodal o cuspidal, com ja hem comentat anteriorment.

El model minimal regular $\mathcal{C}_{min}$ de C sobre $K_\wp$ sempre existeix. Però una altra dificultat que apareix en gènere superior és la de determinar quines són les possibles configuracions de la fibra tancada de $\mathcal{C}_{min}$ i com es pot calcular a partir d'una eqüació per a C.

En efecte, fins i tot per a gèneres petits, es sap que el nombre de possibles configuracions de $\mathcal{C}_{min,\wp}$ és aparatosament gran. Veurem en aquestes notes de quina manera es poden organitzar i descriurem l'algoritme de Liu per al seu càlcul explícit en gènere dos, sobre primers que no divideixen a 2. De passada, veurem com aquest algoritme també es pot utilitzar per a descriure el grup de components connexes del model de Néron de les jacobianes d'aquestes corbes.

Finalment, un invariant important de C és el conductor, que dóna una mesura de la reducció dolenta de la corba en relació a les representacions de Galois associades als mòduls de Tate de la seva varietat Jacobiana. Al darrer capítol, definim i estudiem aquest invariant, comparant-lo amb la noció de discriminant minimal. A més, mostrem algunes de les seves aplicacions al càlcul de les imatges de les representacions de Galois que hem fet esment.

Tot plegat configura el material bàsic per a entendre part dels treballs de Liu sobre models enters de corbes algebraiques de gènere dos sobre cossos locals de característica residual senar.

En un apèndix, afegim l'exposició de Xavier Xarles sobre aplicacions més avançades dels continguts d'aquestes notes: el treball de Lorenzini i Tucker sobre les eqüacions de Thue.

Victor Rotger

Barcelona, 8 de Maig de 2007.

Índex

Capítol 1

Superfícies aritmètiques

Francesc Creixell[1]

1.1 Introducció

En aquest capítol inicial s'estableixen les definicions i resultats bàsics que seran necessaris en la resta de capítols per estudiar la reducció de corbes algebraiques i els seus diferents models.

La primera part del capítol està dedicada al llenguatge d'esquemes. Es repassen breument les propietats d'esquemes i morfisme més importants i aquelles que seran necessaries per a la definició de superfície aritmètica. En la segona part s'introdueix la definició de superfície aritmètica, se'n donen les propietats més bàsiques i s'estudia un cas particular per exemplificar el contingut teòric del que s'ha exposat fins aleshores. Finalment, la darrera secció està dedicada a la teoria de la intersecció per a superfícies aritmètiques donant-ne els resultats més rellevants.

[1]Dep. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya. E-mail: francesc.creixell@upc.edu

El que s'ha volgut en la preparació d'aquest text és fer una exposició clara i concisa dels aspectes i conceptes bàsics de la teoria de superfícies aritmètiques, donant major importància a les idees intuïtives que justifiquen les definicions que no pas al feixuc formalisme que impregna el llenguatge d'esquemes. En aquest sentit, no s'ha inclós la demostració de cap dels resultats exposats, si bé, se'n donen les referències.

1.2 Propietats d'esquemes i morfismes

Repassem en aquesta secció les definicions i conceptes bàsics del llenguatge d'esquemes que més endavant, quan treballem en superfícies aritmètiques, haurem de tenir ben consolidats. Les referències bàsiques per aquesta secció són [10] i [17].

Recordem que un esquema $(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ és un espai topològic $\mathfrak{X}$ dotat d'un feix d'anells $\mathcal{O}_{\mathfrak{X}}$ tal que localment és isomorf a l'espectre d'un anell. En particular, les fibres $\mathcal{O}_{\mathfrak{X},p}$ són anells locals per a tot $p \in \mathfrak{X}$. D'ara en endavant notarem els esquemes sense fer referència al seu feix estructural $\mathcal{O}_{\mathfrak{X}}$.

Definició 1.2.1. *Un esquema $\mathfrak{X}$ és noetherià si és quasi-compacte i per a tot obert afí $U \subset \mathfrak{X}$ l'anell $\mathcal{O}_{\mathfrak{X}}(U)$ és noetherià.*

Com que no volem desenvolupar aquí una teoria general d'esquemes sinó centrar-nos només en les parts del llenguatge que ens seran profitoses més endavant, suposarem a partir d'ara que tots els esquemes són noetherians [2]. Ens

[2] Cal no oblidar aquesta hipòtesi, ja que algun dels resultats exposats en aquest capítol pot deixar de ser cert si no es satisfà aquesta propietat.

estalviem d'aquesta forma haver de tractar amb una generalitat que no necessitem.

Definició 1.2.2. Un esquema $\mathfrak{X}$ és reduït si per a tot obert $U \subset \mathfrak{X}$ l'anell $\mathcal{O}_{\mathfrak{X}}(U)$ és reduït, és a dir, sense elements nilpotents.

Definició 1.2.3. Un esquema $\mathfrak{X}$ és íntegre si per a tot obert $U \subset \mathfrak{X}$ l'anell $\mathcal{O}_{\mathfrak{X}}(U)$ és domini d'integritat.

Es té la següent caracterització:

Proposició 1.2.4. *Un esquema $\mathfrak{X}$ és íntegre si, i només si, és irreductible i reduit.*

Demostració: [10, II, 3.1]. □

En els esquemes íntegres té sentit la noció de cos de funcions racionals. Si $\mathfrak{X}$ és un esquema íntegre aleshores la seva irreductiblitat implica l'existència d'un punt $\xi \in \mathfrak{X}$ únic tal que la seva clausura $\overline{\{\xi\}}$ és tot l'espai $\mathfrak{X}$. Anomenem aquest punt, punt genèric de $\mathfrak{X}$. Es comprova que per a tot obert afi $\mathrm{Spec}(A) \subset \mathfrak{X}$ és té $\mathrm{Frac}(A) = \mathcal{O}_{\mathfrak{X},\xi}$ i per a tot $p \in \mathfrak{X}$ una injecció natural $\mathcal{O}_{p,\mathfrak{X}} \hookrightarrow \mathcal{O}_{\mathfrak{X},\xi}$. Al cos de $\mathcal{O}_{\mathfrak{X},\xi}$ se'l demonina cos de funcions racionals de $\mathfrak{X}$ i se'l denota per $\mathcal{K}(\mathfrak{X})$.

Un element $f \in \mathcal{K}(\mathfrak{X})$ és regular en un punt $p \in \mathfrak{X}$ si $f \in \mathcal{O}_{\mathfrak{X},p}$. El conjunt de punts regulars de f és un obert que denotarem per U_f.

Els elements de $\mathcal{K}(\mathfrak{X})$ tenen una interpretació com a funcions de la següent forma:

$$\begin{array}{rccc} f: & U_f & \longrightarrow & \bigsqcup_{p\in U_f} k(p) \\ & p & \longrightarrow & f_p \end{array}$$

on f_p és la classe de f en el cos residual $k(p) = \mathcal{O}_{\mathfrak{X},p}/\mathcal{M}_p$ en p.

Exemple 1.2.5. Sigui A un domini de integritat i $\mathfrak{X} = \mathrm{Spec}(A)$ aleshores $\mathcal{K}(\mathfrak{X}) \cong \mathrm{Frac}(A)$.

Exemple 1.2.6. Si V és una varietat algebraica definida sobre un cos k i $\mathcal{V}$ és el k-esquema associat, aleshores $\mathcal{K}(\mathcal{V}) \cong k(V)$ i la intepretació dels elements de $\mathcal{K}(\mathcal{V})$ com a funcions coincideix amb la dels elements de $k(V)$ quan restringim U_f als punts tancats, ja que en aquest cas els cossos residuals $k(p)$ són tots k.

Un morfisme d'esquemes és un parell $(f, f^\sharp)$ on $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ és una aplicació contínua entre els corresponents espais topològics i $f^\sharp : \mathcal{O}_\mathcal{Y} \longrightarrow f_*\mathcal{O}_\mathfrak{X}$ és un morfisme de feixos tal que el morfisme d'anells locals $f^\sharp : \mathcal{O}_{\mathcal{Y},f(p)} \longrightarrow \mathcal{O}_{\mathfrak{X},p}$ induït en les fibres és un morfisme local.

Donat un esquema $\mathcal{S}$, que anomenem esquema base, un $\mathcal{S}$-esquema és un esquema $\mathfrak{X}$ conjutament amb un morfisme $\pi : \mathfrak{X} \longrightarrow \mathcal{S}$ que anomenem morfisme estructural. Donats dos $\mathcal{S}$-esquemes $\pi_\mathfrak{X} : \mathfrak{X} \longrightarrow \mathcal{S}$ i $\pi_\mathcal{Y} : \mathcal{Y} \longrightarrow \mathcal{S}$, un morfisme de $\mathcal{S}$-esquemes és un morfisme $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ tal que $\pi_\mathfrak{X} = \pi_\mathcal{Y} \circ f$. Quan l'esquema base és un esquema afí, $\mathcal{S} = \mathrm{Spec}(A)$, parlarem aleshores de A-esquemes.

Definició 1.2.7. Un morfisme d'esquemes $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ és de tipus finit si per a tot obert afí $V = \mathrm{Spec}(B) \subset \mathcal{Y}$ es té que $f^{-1}(V)$ és quasi-compacte i per a qualsevol obert afí $U = \mathrm{Spec}(A) \subset f^{-1}(V)$ l'anell A és una B-àlgebra finit generada.

Exemple 1.2.8. Sigui K un cos i $\phi : V \longrightarrow W$ un morfisme de varietats algebraiques K-definides. El corresponent

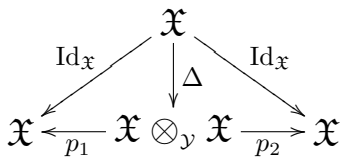
morfisme de K-esquemes $\widetilde{\phi} : \mathcal{V} \longrightarrow \mathcal{W}$ és de tipus finit ja que localment ve induït per morfisme de K-àlgebra finit generades i els espais són quasi-compactes.

Forma part de l'esperit del llenguatge d'esquemes definir conceptes referits a morfismes i no pas als propis esquemes. En són exemples les nocions de morfisme separat, propi o projectiu que tot seguit definirem.

Quan una propietat d'un morfisme és referida al morfisme estructural $\pi : \mathfrak{X} \longrightarrow \mathcal{S}$ d'un $\mathcal{S}$-esquema $\mathfrak{X}$, diem que és el $\mathcal{S}$-esquema $\mathfrak{X}$ qui satisfà la propietat, o fins i tot, simplement diem que és $\mathfrak{X}$ qui compleix la propietat quan l'esquema base $\mathcal{S}$ és evident pel context. D'aquesta forma parlem d'esquemes projectius, separats o propis, si bé, aquestes propietats són referides a morfismes.

Dins la categoria d'espais topològics, un espai topològic T és hausdorff si, i només si, la diagonal $\{(t,t) \in T \times T \,|\, t \in T\}$ és un tancat dins el producte $T \times T$. L'anàleg a aquesta propietat dins la categoria d'esquemes és la noció de morfisme separat.

Donat un morfisme $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ aleshores existeix un únic morfisme $\Delta : \mathfrak{X} \longrightarrow \mathfrak{X} \otimes_{\mathcal{Y}} \mathfrak{X}$ tal que el diagrama:

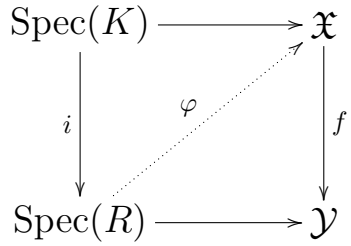


commuta. Anomenem a Δ el morfisme diagonal.

Definició 1.2.9. Un morfisme $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ és separat si $\Delta : \mathfrak{X} \longrightarrow \mathfrak{X} \times_{\mathcal{Y}} \mathfrak{X}$ és una immersió tancada.

El que es vol amb aquesta definició és que un morfisme $g : \mathcal{C} - p \longrightarrow \mathfrak{X}$ d'un esquema $\mathcal{C}$ menys un punt p a un esquema separable $\mathfrak{X}$ només pugui estendre's, en cas que sigui possible, a tot l'esquema $\mathcal{C}$ d'una única forma. Aquesta idea però cal expressar-la localment. El següent teorema n'és la formalització resultant.

Teorema 1.2.10. (Criteri valoratiu per a la separabilitat) *Un morfisme $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ és separable si, i només si, per a qualsevol anell de valoració R amb cos de fraccions K i tot diagrama commutatiu:*



existeix com a molt un únic φ fent el diagrama sencer commutatiu.

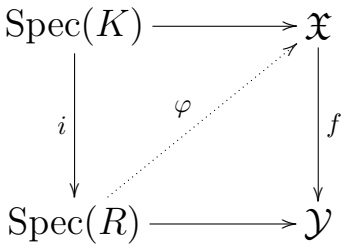
Demostració: [10, II, 4.3]. □

Definició 1.2.11. Un morfisme d'esquemes $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ és propi si és separable, de tipus finit i universalment tancat.

Recordem que un morfisme $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ és universalment tancat si com a aplicació continua és tancada i per a tot $\mathcal{Y}$-esquema $\mathcal{Y}' \longrightarrow \mathcal{Y}$, el morfisme induït $f' : \mathfrak{X} \otimes_{\mathcal{Y}} \mathcal{Y}' \longrightarrow \mathcal{Y}'$ també ho és.

Així com en el cas de morfisme separable el que es vol és aconseguir que un mateix morfisme no pugui tenir més d'una extensió en un punt, amb la propietat el que es pretén és que sempre existeixi aquesta extensió.

Teorema 1.2.12. (Criteri valoratiu per a la propietat) *Sigui $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ de tipus finit. Aleshores f és propi si, i només si, per a qualsevol anell de valoració R amb cos de fraccions K i tot diagrama commutatiu:*



existeix un morfisme φ fent el diagrama sencer commutatiu. Aquest morfisme haurà d'ésser únic.

Demostració: [10, II, 4.7]. □

Comunment, els morfisme propis amb els que es treballa són el projectius.

Definició 1.2.13. Un morfisme $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ és projectiu si factoritza com:

$$\mathfrak{X} \xrightarrow{i} \mathbb{P}^n_{\mathcal{Y}} \longrightarrow \mathcal{Y}$$

on $i : \mathfrak{X} \longrightarrow \mathcal{Y}$ és una immersió tancada.

Efectivament, es verifica que els morfisme projectius són propis.

Teorema 1.2.14. *Tot morfisme projectiu és propi*

Demostració: [10, II, 4.9]. □

Exemple 1.2.15. Sigui V/K una varietat algebraica definida sobre un cos K i $\mathcal{V}$ el K-esquema associat:

- $\mathcal{V}$ és separat.

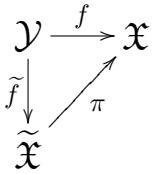
- Si V és projectiva $\Rightarrow \mathcal{V}$ és projectiu i en particular propi.

- Si V és afí $\Rightarrow \mathcal{V}$ no és propi i en particular no és projectiu.

Un anell A és normal si és íntegrament tancat sobre el seu cos de fraccions $\mathrm{Frac}(A)$.

Definició 1.2.16. Un esquema $\mathfrak{X}$ és normal en $p \in \mathfrak{X}$ si l'anell local $\mathcal{O}_{\mathfrak{X},p}$ és normal. $\mathfrak{X}$ és normal si ho és en tot punt.

Definició 1.2.17. Donat un esquema íntegre $\mathfrak{X}$, una normalització de $\mathfrak{X}$ és un esquema $\widetilde{\mathfrak{X}}$ i un morfisme $\pi : \widetilde{\mathfrak{X}} \longrightarrow \mathfrak{X}$ tal que $\widetilde{\mathfrak{X}}$ és normal i per a tot $f : \mathcal{Y} \longrightarrow \mathfrak{X}$ dominant amb $\mathcal{Y}$ normal existeix un únic $\widetilde{f}$ fent commutatiu el diagrama:



Hi ha una forma sencilla de construir la normalització d'un esquema íntegre $\mathfrak{X}$ donat. Quan l'esquema $\mathfrak{X} = \mathrm{Spec}(A)$ és l'espectre d'un domini de integritat A, aleshores l'esquema $\widetilde{\mathfrak{X}} = \mathrm{Spec}(\widetilde{A})$, on $\widetilde{A}$ és la clausura entera de A dins $\mathrm{Frac}(A)$, és una normalització de $\mathfrak{X}$.

En general si $\mathfrak{X} = \bigcup_{i\in I} \mathrm{Spec}(A_i)$ aleshores la normalització $\widetilde{\mathfrak{X}}$ s'obté enganxant les normalitzacions $\{\mathrm{Spec}(\widetilde{A_i}) \longrightarrow \mathrm{Spec}(A_i)\}_{i\in I}$.

Un anell local noetherià $(A, \mathfrak{m})$ amb cos residual $k = A/\mathfrak{m}$ és regular si:

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim_{\mathrm{Krull}}(A).$$

Equivalentment, si l'ideal maximal $\mathfrak{m}$ està generat per $\dim_{\text{Krull}}(A)$ elements.

Definició 1.2.18. Un esquema $\mathfrak{X}$ és regular en un punt $p \in \mathfrak{X}$ si $\mathcal{O}_{\mathfrak{X},p}$ és regular. L'esquema és regular si ho és en cada punt.

La noció de regularitat d'un esquema és la traducció de la no-singularitat d'una varietat algebraica al llenguatge d'esquemes.

Es deriva dels resultats en àlgebra commutativa que la regularitat d'un esquema implica la seva normalitat.

Proposició 1.2.19. *Sigui A un domini de integritat, local i noetherià. Si A és regular aleshores és normal. Si a més, A té dimensió* 1*, el recíproc també és cert.*

Demostració: [2]. □

Exemple 1.2.20. La normalització d'una corba és la seva desingularització.

El concepte anàleg al de punt K-racional d'una varietat algebraica dins el llenguatge d'esquemes és el de secció.

Definició 1.2.21. Siguin $\mathfrak{X} \longrightarrow \mathcal{S}$ i $\mathcal{T} \longrightarrow \mathcal{S}$ $\mathcal{S}$-esquemes, una $\mathcal{T}$-secció de $\mathfrak{X}$ és un morfisme de $\mathcal{S}$-esquemes $\sigma : \mathcal{T} \longrightarrow \mathfrak{X}$.

Utilitzem la notació:

$$\mathfrak{X}(\mathcal{T}) = \{\mathcal{T}\text{-seccions de } \mathfrak{X}\}.$$

En el cas que l'esquema base sigui afí, $\mathcal{S} = \text{Spec}(A)$, denotem el conjunt de $\mathcal{S}$-seccions per $\mathfrak{X}(A)$ i anomenem els seus elements punts A-racionals.

Els següents exemples posen de manifest l'equivalència entre el concepte clàssic de punt racional i el de secció en llenguatge d'esquemes.

Exemple 1.2.22. Sigui K un cos, $I \subset K[X_1, \ldots, X_n]$ un ideal, $V = V(I)$ la corresponent varietat afí i

$$\mathcal{V} = \mathrm{Spec}(K[X_1, \ldots, X_n]/I)$$

el K-esquema associat. Donat un punt $p = (p_1, \ldots, p_n) \in V(K)$, aquest permet definir el morfime de K-àlgebras:

$$\begin{array}{rccc} \widetilde{\sigma}_p : & K[X_1, \ldots, X_n]/I & \longrightarrow & K \\ & X_i & \longrightarrow & p_i \end{array}$$

que a la seva vegada indueix una secció $\sigma_p \in \mathcal{V}(K)$. Reciprocament, donada una secció $\sigma \in \mathcal{V}(K)$ aquesta indueix un morfisme de K-àlgebras $\widetilde{\sigma} : K[X_1, \ldots, X_n]/I \longrightarrow K$, aleshores el punt $(\widetilde{\sigma}(X_1), \ldots, \widetilde{\sigma}(X_n))$ pertany a $V(K)$. Aquesta correspondència és clarament bijectiva.

Exemple 1.2.23. Més en general, donat un cos K i un K-esquema $\mathfrak{X}$, es té una bijecció entre els elements de $\mathfrak{X}(K)$ i el conjunt $\{p \in \mathfrak{X} |\, \mathcal{O}_{\mathfrak{X},p} = K\}$ que envia un element $\sigma \in \mathfrak{X}(K)$ a $\sigma((0))$.

Donat un anell A i un A-mòdul M, es diu que M és mòdul pla si el functor $M \otimes_A \cdot$ és exacte. Recordem que en general aquest functor conserva únicament l'exactitut per la dreta.

Sobre un domini d'ideals principals A, un A-mòdul M és pla si, i només si, M és lliure de torsió. En particular, donat un cos K, tota K-àlgebra és un K-mòdul pla.

Definició 1.2.24. Un morfisme d'esquemes $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ és pla en $p \in \mathfrak{X}$ si:

$$\mathcal{O}_{\mathfrak{X},p} \text{ és un } \mathcal{O}_{\mathcal{Y},f(p)}\text{-mòdul pla}$$

via el morfisme induït $f_p^\sharp : \mathcal{O}_{\mathcal{Y},f(p)} \longrightarrow \mathcal{O}_{\mathfrak{X},p}$. Diem que f és pla si ho és en tot punt de $\mathfrak{X}$.

Exemple 1.2.25. Donat que tota àlgebra sobre un cos és plana, tot esquema sobre un cos és pla.

Pel que respecte a esquemes sobre anells de Dedekind es té la següent caracterització.

Proposició 1.2.26. *Sigui $\mathcal{D}$ un anell de Dedekind i $\mathfrak{X}$ un esquema reduït. Un morfisme $f : \mathfrak{X} \longrightarrow \mathrm{Spec}(\mathcal{D})$ és pla $\Leftrightarrow$ cada component irreductible de $\mathfrak{X}$ domina* $\mathrm{Spec}(\mathcal{D})$.

Demostració: [17, 4.3.9]. □

Més en general, la planor d'un morfisme $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ implica que la família de fibres del morfisme $\{\mathfrak{X}_p\}_{p\in\mathcal{Y}}$ constitueix una família *contínua* d'esquemes. Aquesta noció poc clara de continuïtat queda precisada en el següent teorema.

Teorema 1.2.27. *Sigui $\mathcal{S}$ un esquema íntegre i $\mathfrak{X} \subset \mathbb{P}^n_{\mathcal{S}}$ un subesquema tancat. Aleshores $\mathfrak{X}$ és pla sobre $\mathcal{S}$ si, i només si, per a tot $p \in \mathcal{S}$ el polinomi de Hilbert de la fibra $\mathfrak{X}_p \subset \mathbb{P}^n_{k(p)}$ és independent de p. En particular la dimensió, el grau i el gènere aritmètic de $\mathfrak{X}_p$ no depèn de p.*

Demostració: [10, III, 9.9]. □

Acabem aquesta secció amb la definició de morfisme llis.

Definició 1.2.28. Sigui $f : \mathfrak{X} \longrightarrow \mathcal{Y}$ un morfisme de tipus finit. Diem que f és llis en $x \in \mathfrak{X}$ si:

- f és pla en x i

- $\mathfrak{X}_y \otimes_{k(y)} \overline{k(y)}$ és regular x, on $y = f(x)$.

Diem que f és llis si ho és en tot punt.

Observem que aquesta definició imposa la regularitat de totes les fibres del morfisme $\mathfrak{X} \longrightarrow \mathcal{Y}$.

Es comprova que la llisor d'un morfisme $\mathfrak{X} \longrightarrow \mathcal{Y}$ implica la regularitat de l'esquema $\mathfrak{X}$. El recíproc no és cert en general, si bé pot ser-ho sota certes hipòtesis addicionals.

Exemple 1.2.29. Sigui K un cos i $\mathfrak{X}$ un K-esquema. Si $\mathfrak{X}$ és llis aleshores és un esquema regular.

Exemple 1.2.30. Sigui K un cos perfecte i $\mathfrak{X}$ un K-esquema. $\mathfrak{X}$ és llis si, i només si, $\mathfrak{X}$ és un esquema regular.

Exemple 1.2.31. Veurem a la següent secció exemples d'esquemes regulars no llisos. Més concretament, estudiarem el cas particular d'una superfície aritmètica que serà regular pero no llisa.

1.3 Superfícies Aritmètiques

Per a tota aquesta secció establim les següents notacions.

$\mathcal{D}$, anell de Dedekind.
K, cos de fraccions de $\mathcal{D}$.
$\mathcal{S} = \mathrm{Spec}(\mathcal{D})$.

1.3.1 Definició i primeres propietats

Definició 1.3.1. Una superfície aritmètica $\mathcal{C}$ sobre $\mathcal{D}$ és un esquema sobre $\mathcal{S}$:

$$\pi : \mathcal{C} \longrightarrow \mathcal{S}$$

íntegre, normal, de tipus finit i pla sobre $\mathcal{S}$ de dimensió 2.

Dins la literatura especialitzada es poden trobar diferents definicions de superfície aritmètica. Així per exemple, a [17] un esquema $\mathcal{C}$ és una superfície aritmètica si a més de les propietats imposades en la nostra definició l'esquema $\mathcal{C}$ és projectiu i regular. A [34] s'afegeix a la nostra de definició que l'esquema $\mathcal{C}$ sigui excelent. Aquesta divergència en les definicions ens ha obligat als que hem preparat el seminari a establir una definició compatible amb les diferents definicions trobades. Aquest problema s'ha resolt prenent la definició més restrictiva possible que no entres en contradicció amb les utilitzades per altres autors.

Exemple 1.3.2. Sigui K un cos de nombres amb anell d'enters algebraics $\mathcal{O}_K$ i E/K una corba el·líptica definida sobre K. L'$\mathcal{O}_K$-esquema $\mathcal{C}_E$ determinat per una equació de Weierstrass de E amb coeficients a $\mathcal{O}_K$ és una superfície aritmètica sobre $\mathcal{O}_K$ si $\mathcal{C}_E$ és normal. En general, aquesta normalitat és difícil de comprovar. Ara bé, si prenem (en cas que existeixi) un model minimal de Weirstrass global W/K i el tipus de reducció en els primers de mala reducció és o bé multiplicatiu I1 o bé additiu II, aleshores el $\mathcal{O}_K$-esquema $\mathcal{C}_W$ determinat per W és una superfície aritmètica ja que $\mathcal{C}_W$ és el model regular minimal de W (Cap. 2 §[4.1], Cap. 3 §2).

Abans d'estudiar amb deteniment un exemple concret de superfície aritmètica, és important aclarir certs fets i propietats que es deriven de la mateixa definició que poden no resultar evidents.

- Per la definició que hem adoptat, és possible que una superfície aritmètica $\mathcal{C}$ no sigui ni regular, ni projectiva, ni pròpia.

- Tota superfície aritmètica $\mathcal{C}$ és íntegre. Per tant, és irreductible i reduïda i té cos de funcions $\mathcal{K}(\mathcal{C})$.

- Si η és el punt genèric de $\mathcal{S}$, aleshores la fibra genèrica $\mathcal{C}_\eta$ és una corba llisa sobre el cos K.

- Les fibres especials $\mathcal{C}_\mathfrak{p}$ són corbes definides els corssos residuals $k(\mathfrak{p}) = \mathcal{D}/\mathfrak{p}$.

- Si $\mathcal{C}$ és pròpia o projectiva aleshores les fibres especials $\mathcal{C}_\mathfrak{p}$ són pròpies o projectives respectivament.

- Per a cada corba irreductible $\mathfrak{X} \subset \mathcal{C}$ l'anell local $\mathcal{O}_{\mathcal{C},\mathfrak{X}}$ és un anell de valoració discreta amb cos de fraccions $\mathcal{K}(\mathcal{C})$ i valoració $\mathrm{ord}_\mathfrak{X} : K(\mathcal{C})^* \longrightarrow \mathbb{Z}$.

- Si u és un uniformitzant per a $\mathfrak{p} \in \mathcal{S}$, es verifica:

$$\mathcal{C}_\mathfrak{p} = \sum_{\mathfrak{X} \subset \pi^{-1}(\mathfrak{p})} n_i \mathfrak{X}_i, \quad \text{on} \quad n_i = \mathrm{ord}_{\mathfrak{X}_i}(\pi^* u).$$

- Donat que $\mathcal{C}$ és plana sobre $\mathcal{C}$ el gènere aritmètic de les fibres es conseva. Així doncs:

$$p_a(\mathcal{C}_\mathfrak{p}) = p_a(C_\eta) = g(C_\eta).$$

- Encara que $\mathcal{C}$ sigui regular, $\mathcal{C}_\mathfrak{p}$ pot tenir punts no-regulars, és a dir, pot no ser llisa.

1.3.2 Un exemple particular

Estudiem en aquesta secció un exemple particular de superfície aritmètica. Prenem l'anell:

$$\mathcal{A} = \frac{\mathbb{Z}[x, y]}{(y^2 - x^3 + x^2 - 6)}.$$

i l'esquema $\mathcal{C} = \mathrm{Spec}(\mathcal{A})$. Veurem que aquest esquema és una superfície aritmètica.

Observem primerament que la inclusió $i : \mathbb{Z} \longrightarrow \mathcal{A}$ indueix una estructura $\pi : \mathcal{C} \longrightarrow \mathrm{Spec}(\mathbb{Z})$ de $\mathrm{Spec}(\mathbb{Z})$-esquema en $\mathcal{C}$.

Donat que l'anell $\mathcal{A}$ és una $\mathbb{Z}$-algebra finit generada i lliure de torsió, aleshores el morfisme estructural $\pi : \mathcal{C} \longrightarrow \mathrm{Spec}(\mathbb{Z})$ és de tipus finit i pla. A més, l'esquema $\mathcal{C}$ és íntegre i de dimensió 2 per ser-ho l'anell $\mathcal{A}$.

Ens resta veure que l'esquema $\mathcal{C}$ és normal per porder assegurar que $\mathcal{C}$ és una superfície aritmètica.

Notem que donat que la superficie $\mathcal{C}$ és afí aleshores no és pròpia.

Per provar que $\mathcal{C}$ és normal veurem que la superfície és regular. Això ho farem estudiant les diferents fibres.

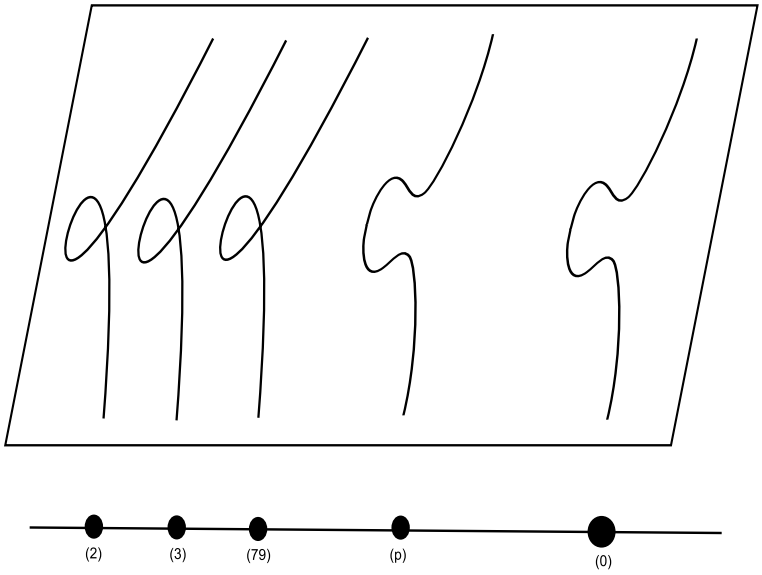
La fibra genèrica és la corba el·líptica definida sobre $\mathbb{Q}$ donada per l'equació:

$$\mathcal{C}_\eta : Y^2 = X^3 - X^2 + 6.$$

El discriminant de $\mathcal{C}_\eta$ és $\Delta_{\mathcal{C}_\eta} = -2^6 \cdot 3 \cdot 79$. Per tant, $\mathcal{C}_\eta$ és regular i les úniques fibres especials no regulars amb els respectius punts singulars són:

$$\begin{aligned}
\mathcal{C}_2 : &\quad Y^2 = X^3 - X^2, \quad P_2 = (0,0), \\
\mathcal{C}_3 : &\quad Y^2 = X^3 - X^2, \quad P_3 = (0,0), \\
\mathcal{C}_{79} : &\quad Y^2 = X^3 - X^2 + 6, \quad P_{79} = (27,0).
\end{aligned}$$

Una representació gràfica de la superfície $\mathcal{C}$ és:



Donat que $\mathcal{C}$ té fibres singulars, és evident que no pot ser un esquema llis. Ara bé, si estudiem els punts singulars de les fibres veurem que aquests són punts regulars de l'esquema:

- $\mathcal{C}_2$: l'ideal maximal corresponent al punt singular és $M_2 = (X, Y, 2)$. Es té la igualtat:

$$2 = -\frac{1}{3}(Y^2 - X^3 + X^2) \in M_2$$

Per tant, $\dim_{\mathbb{F}_2}(M_2/M_2^2) = 2$ i el punt M_2 és regular dins $\mathcal{C}$.

- $\mathcal{C}_3$: l'ideal maximal corresponent al punt singular és $M_3 = (X, Y, 3)$. Es té la igualtat:

$$3 = -\frac{1}{2}(Y^2 - X^3 + X^2) \in M_3$$

Per tant, $\dim_{\mathbb{F}_3}(M_3/M_3^2) = 2$ i el punt M_3 és regular dins $\mathcal{C}$.

- $\mathcal{C}_{79}$: l'ideal maximal corresponent al punt singular és $M_{79} = (X - 27, Y, 79)$. Es té la igualtat:

$$79 = -\frac{1}{27X - 489}(Y^2 - (X - 27)^2(X + 53)) \in M_{79}$$

Per tant, $\dim_{\mathbb{F}_{79}}(M_{79}/M_{79}^2) = 2$ i el punt M_{79} és regular dins $\mathcal{C}$.

Així doncs, la superfície $\mathcal{C}$ és regular i conseqüentment normal. Per tant, $\mathcal{C}$ és una superfície aritmètica.

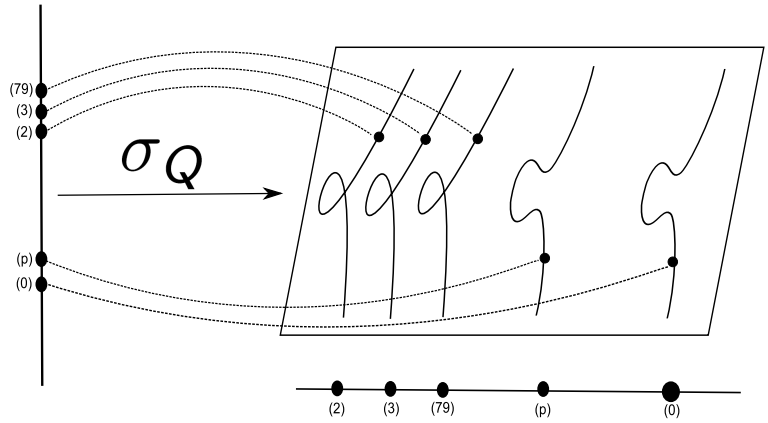
Observem que la fibra genèrica $\mathcal{C}_\eta$ conté el punt $\mathbb{Q}$-racional $Q = (-1, 2) \in \mathcal{C}_\eta(\mathbb{Q})$. Donat que aquest punts té coordenades enteres, podem definir a partir d'ell una $\mathbb{Z}$-secció $\sigma_Q \in \mathcal{C}(\mathbb{Z})$ mitjançant el morfisme:

$$\begin{array}{rccc} \phi: & \frac{\mathbb{Z}[x,y]}{(y^2-x^3+x^2-6)} & \longrightarrow & \mathbb{Z} \\ & x & \longrightarrow & -1 \\ & y & \longrightarrow & 2 \end{array}$$

Aquesta secció opera de la següent forma:

$$\sigma_Q((p)) = \phi^{-1}((p)) = (x+1, y-2, p).$$

Per tant, envia cada primer (p) enter a la reducció del punt Q a $\mathcal{C}_p$. La següent figura il·lustra aquesta idea:



Notem que aquesta construcció ha estat possible perquè el punt Q té coordenades enteres. Si les coordenades haguessin estat racionals aleshores no hauriem pogut definir la secció. Per exemple, si haguessim pres el punt $[2]Q = (73/16, -574/64)$. Això succeeix perquè la superfície $\mathcal{C}$ és afí.

Treballant amb l'esquema projectiu associat, és a dir,

$$\text{Proj}\left(\frac{\mathbb{Z}[x,y,z]}{y^2z - x^3 + x^2z - 6z^3}\right)$$

aquest problema desapareix, ja que aleshores l'esquema és propi. Dit d'una manera més sencilla, en coordenades projectives hauriem pogut eliminar denominadors.

1.3.3 Punts de superficies aritmètiques

En l'exemple de l'apartat anterior hem pogut comprovar com els punts imatge d'una secció en les diferents fibres d'una superfície, són punts regulars. Aquest, és un fet general:

Proposició 1.3.3. *Sigui $\pi : \mathcal{C} \longrightarrow \mathcal{S}$ una superfície aritmètica sobre $\mathcal{D}$ i $\sigma \in \mathcal{C}(\mathcal{D})$ una $\mathcal{D}$-secció. Aleshores $\sigma(\mathfrak{p}) \in \mathcal{C}_{\mathfrak{p}}$ és un punt regular per a tot $\mathfrak{p} \in \mathcal{S}$.*

Demostració: [34, IV, 4.3]. □

També ens ha servit l'exemple anterior per entendre que en general no tot punt de la fibra genèrica indueix un secció sobre tota la superficíe aritmètica, i que aquest problema sembla desaparéixer quan treballem amb esquemes propis. El següent corol·lari de la proposició anterior formalitza aquesta idea entre d'altres fets.

Corol·lari 1.3.4. *Sigui $\mathcal{C} \longrightarrow \mathcal{S}$ una superfície aritmètica i $\mathcal{C}_\eta/K$ la fibra genèrica.*

i) Si $\mathcal{C}$ és pròpia sobre $\mathcal{D}$ aleshores $\mathcal{C}_\eta(K) = \mathcal{C}(\mathcal{D})$.

ii) Si $\mathcal{C}$ és regular, sigui $\mathcal{C}^0 = \mathcal{C} - \mathrm{Sing}(\mathcal{C}_{\mathfrak{p}})$ el major esquema llis dins de $\mathcal{C}$. Aleshores:

$$\mathcal{C}(\mathcal{D}) = \mathcal{C}^0(\mathcal{D}).$$

iii) En particular, si $\mathcal{C}$ és pròpia i regular, aleshores:

$$\mathcal{C}_\eta(K) = \mathcal{C}(\mathcal{D}) = \mathcal{C}^0(\mathcal{D}).$$

Demostració: [34, IV, 4.4]. □

1.3.4 Gènere aritmètic de les fibres

Acabem aquesta secció donant una fòrmula que estableix la relació entre el gènere aritmètic d'una corba i el de les seves components irreductibles. Aquest resultat ens serà útil en els propers capítols.

Sigui C una corba sobre un cos k. Per a cada punt $p \in C$ definim:

$$S_p := \widetilde{\mathcal{O}}_{C,p}/\mathcal{O}_{C,p},$$

on $\widetilde{\mathcal{O}}_{C,p}$ és la clausura entera de l'anell local $\mathcal{O}_{C,p}$ dins el seu cos de fraccions.

Proposició 1.3.5. *Sigui C una corba reduïda definida sobre un cos k i $C_1, \ldots, C_n$ les seves components irreductibles. Aleshores:*

$$p_a(C) + n - 1 = \sum_{1 \leq i \leq n} p_a(\widetilde{C}_i) + \sum_{P \in C} \dim_k(S_P),$$

on $\widetilde{C}_i$ és la normalització de C_i.

Demostració: [17, 7.5.4]. □

Observem que el terme de la dreta de la igualtat té sentit ja que per a un punt $P \in C$ regular es satisfà $S_P = 0$. Notem també que la fòrnula mostra que el gènere aritmètic d'una corba irreductible és sempre major o igual que el gènere geòmetric de la seva desingularització, i que hi ha igualtat únicament quan la corba és regular. En particular, tota corba irreductible de gènere aritmètic 0 és regular.

1.4 Teoria de la intersecció en superfícies aritmètiques

Volem desenvolupar en aquesta darrera secció una teoria de la intersecció per a superfícies aritmètiques similar a la que es té per a superfícies definides sobre cossos algebraicament tancats.

1.4.1 Intersecció sobre un cos algebraicament tancat

Sigui S una superfície no-singular projectiva definida sobre un cos K algebraicament tancat.

Recordem que per a qualsevol corba $\Gamma \subset S$ irreductible l'anell $\mathcal{O}_{S,\Gamma}$ és un anell de valoració discreta. Notem per $\mathrm{ord}_\Gamma : K(S)^* \longrightarrow \mathbb{Z}$ la valoració d'aquest anell estesa al cos de fraccions de $\mathcal{O}_{S,\Gamma}$, el cos de funcions racionals $K(S)$ de S.

Donada una funció racional $f \in K(S)$ poden associar-li el divisor:

$$\mathrm{div}(f) = \sum_{\Gamma \in S} \mathrm{ord}_\Gamma(f)\Gamma.$$

Aquest divisor està ben definit ja que $\mathrm{ord}_\Gamma(f) = 0$ per a tota $\Gamma \in S$ llevat d'un nombre finit.

Definició 1.4.1. Donat un divisor $D \in \mathrm{Div}(S)$ i un punt $P \in S$, una equació local per a D en P és una funció racional $f \in K(S)$ tal que

$$P \notin D - \mathrm{div}(f)$$

En el cas particular que $D = \Gamma$ és una corba irreductible i $P \in \Gamma$, estem demanant que $\mathrm{ord}_\Gamma(f) = 1$ i que $\mathrm{ord}_{\Gamma'}(f) = 0$ per a qualsevol altra corba Γ' tal que $P \in \Gamma'$.

L'objectiu és construir un aparellament bilineal simètric

$$\mathrm{Div}(S) \times \mathrm{Div}(S) \longrightarrow \mathbb{Z} \qquad (D_1, D_2) \longrightarrow D_1 \cdot D_2$$

de tal manera que aporti informació sobre l'intersecció de divisors. La construcció d'aquest aparellament s'assoleix en dos estadis.

Primerament cal definir la multiplicitat d'intersecció de dos divisors en un punt.

Definició 1.4.2. Sigui un punt $P \in S$ i $D_1, D_2 \in \mathrm{Div}(S)$ divisors sense components en comú. Es defineix la multiplicitat d'intersecció de D_1 i D_2 en P com:

$$(D_1 \cdot D_2)_P = \dim_K \mathcal{O}_{S,P}/(f_1, f_2)$$

on f_i és una equació local per a D_i en P.

Aquesta definició permet establir el que serà la multiplicitat de intersecció de dos divisors sense components en comú. Si C i D són divisors sense components en comú, aleshores es pren:

$$C \cdot D = \sum_{P \in C \cap D} (C \cdot D)_P$$

Aquesta expressió no resol el cas general. No és útil quan els divisors considerats tenen components en comú. Ara bé, es demostra que aquesta definició és independent de dependència lineal i que donats dos divisors amb components en comú sempre és possible trobar-ne un nou parell sense components en comú i linealment dependents del parell donat. En definitiva, es té el següent teorema.

Teorema 1.4.3. *Sigui S una superfície projectiva definida sobre un cos K algebraicament tancat. Existeix un únic aparellament bilineal simètric:*

$$\begin{array}{rcl} \mathrm{Div}(S) \times \mathrm{Div}(S) & \longrightarrow & \mathbb{Z} \\ (C, D) & \longrightarrow & C \cdot D \end{array}$$

tal que:

i) Si C i D no tenen components en comú, aleshores:

$$C \cdot D = \sum_{P \in C \cap D} (C \cdot D)_P$$

ii) Si $D_1 \sim D_2$ aleshores: $D_1 \cdot D = D_2 \cdot D$

L'aparellament del teorema és evidentment l'aparellament que s'estava buscant. Anomenem multiplicitat o índex de intersecció dels divisors D_1 i D_2 al valor $D_1 \cdot D_2$.

1.4.2 Intersecció en superfícies aritmètiques

En aquesta secció en restringirem al cas de superfícies definides sobre anells de valoració discreta. Fixem les següents notacions:

$\mathcal{R}$, anell de valoració discreta.

$\mathfrak{p}$, anell maximal de $\mathcal{R}$.

$\kappa = \mathcal{R}/\mathfrak{p}$, cos residual de $\mathcal{R}$.

$\mathcal{S} = \mathrm{Spec}(\mathcal{R})$.

Volem desenvolupar una teoria similar a la que acabem de veure però pel cas de superfícies aritmètiques.

La principal dificultat amb la que hom es topa en l'intent d'estendre el resultats del cas algebraicament tancat al cas de superfícies aritmètiques, és que en aquestes sempre

hi ha divisors irreductibles no propis. Més concretament, si bé una superfície aritmètica $\mathcal{C} \longrightarrow \mathcal{S}$ pot ser pròpia i conseqüentment també les components irreductibles de les fibres especials, la no propietat de l'esquema base $\mathcal{S}$ comporta l'existència de divisors irreductbles no propis. Així per exemple, la imatge d'una $\mathcal{R}$-secció $\sigma(\mathcal{S}) \subset \mathcal{C}$ serà sempre un divisor no propi.

Observem que per definició, una superfície aritmètica $\mathcal{C} \longrightarrow \mathcal{S}$ és normal i que per tant tenim sobre ella un bona teoria de divisors de Weil ([10]). Notem també, que la definició d'equació local d'un punt en un divisor, i la de multiplicitat de intersecció de dos divisors en un punt donades pel cas algebraicament tancat segueixen sent vàlides per a superfícies aritmètiques. Conseqüenment, no les repetim.

La idea per superar l'entrebanc que suposen els divisors no propis és restringir una de les coordenades de l'aparellament bilineal a una classe de divisors propis que haurem d'establir. Necessitem les següents definicions.

Definició 1.4.4. Un divisor irreductible $D \in \mathrm{Div}(\mathcal{C})$ és horitzontal si la restricció $\pi : D \longrightarrow \mathcal{S}$ és exahustiva.

És un exemple de divisor horitzontal la imatge d'una $\mathcal{R}$-secció $\sigma \in \mathcal{C}(\mathcal{R})$.

És l'existència d'aquesta classe de divisors la que entorpeix la construcció d'una bona teoria de l'intersecció. Es poden trobar exemples de divisor hortizontals C, D_1, D_2 amb D_1 i D_2 linealment dependents i tals que $C \cap D_1 \neq \emptyset$ i $C \cap D_2 = \emptyset$. Això impedeix la definició d'un aparellament independent de la dependència lineal pel conjunt total de divisors $\mathrm{Div}(\mathcal{C})$.

Definició 1.4.5. Un divisor irreductible $D \in \mathrm{Div}(\mathcal{C})$ és fibral si és una component de la fibra especial $\mathcal{C}_\mathfrak{p}$. Un divisor $D \in \mathrm{Div}(\mathcal{C})$ és fibral si ho són les seves components irreductibles.

Notem el subgrup generat pels divisors fibrals per

$$\mathrm{Div}_\mathfrak{p}(\mathcal{C}) = \{D \in \mathrm{Div}(\mathcal{C}) |\, D \text{ fibral}\}.$$

Observem que quan la superfície és pròpia aleshores els divisors fibrals irreductibles són propis.

Fetes aquestes definicions ja podem presentar el resultat principal.

Teorema 1.4.6. *Sigui $\mathcal{C}$ una superfície aritmètica regular i pròpia sobre $\mathcal{R}$. Aleshores existeix un únic aparellament bilineal:*

$$\begin{array}{ccc} \mathrm{Div}(\mathcal{C}) \times \mathrm{Div}_\mathfrak{p}(\mathcal{C}) & \longrightarrow & \mathbb{Z} \\ (D, F) & \longrightarrow & D \cdot F \end{array}$$

tal que:

i) Si D i C no tenen components en comú, aleshores:

$$D \cdot C = \sum_{x \in D \cap C} (D \cdot C)_x.$$

ii) Si $D_1 \sim D_2$ aleshores $D_1 \cdot C = D_2 \cdot C$ per a tot $C \in \mathrm{Div}_\mathfrak{p}(\mathcal{C})$

iii) Si $F_1, F_2 \in \mathrm{Div}_\mathfrak{p}(\mathcal{C})$ aleshores $F_1 \cdot F_2 = F_2 \cdot F_1$.

Observem que l'aparellament aconseguit no és simètric.

El resultat següent dóna informació sobre l'índex d'autointersecció de divisors fibrals i caracteritza els multiples del divisor constituït per la fibra especial $\mathcal{C}_\mathfrak{p}$.

Proposició 1.4.7. *Sigui $\mathcal{C}$ una superfície aritmètica regular i pròpia sobre $\mathcal{R}$, i $F \in \mathrm{Div}_{\mathfrak{p}}(\mathcal{C})$ un divisor fibral. Aleshores:*

$$F^2 \leq 0,$$

i les següents condicions són equivalents:

i) $F^2 = 0$.

ii) $F \cdot F' = 0$ *per a tot* $F' \in \mathrm{Div}_{\mathfrak{p}}(\mathcal{C})$.

iii) $F = a\mathcal{C}_{\mathfrak{p}}$ *amb* $a \in \mathbb{Q}$.

Acabem l'exposició amb l'anomenada fòrmula d'adjunció que posa en relació el gènere aritmètic d'un divisor i el seu índex de intersecció amb el divisor canònic.

Teorema 1.4.8. (Fòrmula d'adjunció) *Sigui $\mathcal{C}$ una superfície aritmètica regular i pròpia sobre $\mathcal{R}$. Existeix un divisor $\mathcal{K}_{\mathcal{C}} \in \mathrm{Div}(\mathcal{C})$, anomenat divisor canònic, tal que:*

$$F^2 + \mathcal{K}_{\mathcal{C}} \cdot F = 2p_a(F) - 2$$

per a qualsevol $F \in \mathrm{Div}_{\mathfrak{p}}(\mathcal{C})$.

Aquest resultat podria prendre's com a definició alternativa a la definició clàssica del divisor canònic.

Capítol 2

Models minimals, canònics i estables

Luis E. García[1]

2.1 Notacions

En tot aquest capítol A denotarà un anell de Dedekind, K el seu cos de fraccions i $S = \mathrm{Spec}(A)$. Una superfície aritmètica $X \to S$ és un esquema de dimensió 2, integre, normal, de tipus finit i pla sobre S (cf. Cap. 1, §3.1). Donada una superfície aritmètica $X \to S$, denotarem per $X_\eta =_{df} X \times_S \mathrm{Spec}(K)$ la seva fibra genèrica. Donada una corba projectiva C sobre un cos k, denotarem per $p_a(C)$ el seu gènere aritmètic. Si a més C és llisa, denotarem per $g(C)$ o simplement g el seu gènere geomètric.

[1]Dep. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya. E-mail: luigarm2@aaa.upv.es

2.2 Introducció

Sigui $X \to S$ una superfície aritmètica. Si $Y \to S$ és una altra superfície aritmètica i existeix un morfisme birracional $Y \dashrightarrow X$, diem que X és un *model* de Y. A diferència del cas de corbes pròpies sobre un cos k, donada una superfície aritmètica regular $X \to S$, poden existir infinits models regulars de X, la majoria dels quals no són gaire interessants. En aquest capítol descriurem alguns models canònicament associats a X amb propietats addicionals que els fan útils, com veurem als capítols posteriors.

A la tercera secció d'aquest capítol introduïm els conceptes de model regular minimal i model regular relativament minimal d'una superfície aritmètica regular $X \to S$. El fet que una superfície aritmètica Y sigui un model minimal per a X està relacionat amb l'existència de certs divisors primers en Y, anomenats *divisors excepcionals*.

Definirem aquest concepte i discutirem el criteri de Castelnuovo, que ens dóna una caracterització dels divisors excepcionals. Usant aquest resultat, veurem que tota superfície aritmètica admet un model regular relativament minimal i deduïrem una condició suficient per a l'existència d'un (únic) model minimal, que denotarem per X_{min}. Aquesta condició es compleix en tots els casos que ens interessen.

A més, considerarem corbes algebraiques C sobre un cos K i introduïrem el concepte de *model de C sobre S*. Usant els resultats anteriors, deduïrem l'existència d'un únic model minimal de C sobre S per a corbes de gènere $g(C) \geq 1$.

A la secció 4 definirem el concepte de model canònic X_{can} d'una superfície aritmètica $X \to S$. Aquest model

s'obté a partir de contraccions successives del model minimal regular. La construcció és lleugerament diferent per a $p_a(X_\eta) \geq 2$ i $p_a(X_\eta) = 1$. En general, el model canònic no és regular. Altrament, té altres avantatges: mentre que en el model minimal regular l'estructura de la fibra sobre un punt tancat de S pot ser molt complexa, en el model canònic el nombre de components irreductibles d'aquesta fibra està uniformement fitat en funció del gènere aritmètic de la fibra genèrica (en el cas $p_a(X_\eta) \geq 2$). Discutirem aquests aspectes del model canònic i, en el cas $p_a(X_\eta) = 1$ analitzarem la seva relació amb el model minimal de Weierstrass de X_η.

A la darrera secció definirem les nocions de bona i mala reducció sobre $s \in S$, que seran utilitzades en els següents capítols. Veurem que per a estudiar corbes llises i projectives sobre un cos k necessitem considerar models no necessàriament regulars, i això ens portarà a la definició de models *estables i semiestables*. Aquests models no són regulars en general, però les seves singularitats són conegudes. Seràn molt utilitzats en els següents capítols (cf. Cap. 3, Cap. 5). Explicarem quina relació tenen amb el model minimal regular i el model canònic introduits a les seccions anteriors; en particular veurem que existeix un model semiestable si i només si el model minimal regular és semiestable i a més veurem que si $g(C) > 1$ i existeix un model estable, aleshores és únic i isomorf a C_{can}.

Finalment, enunciarem el teorema de Deligne-Mumford: donat un anell de valoració discreta R amb cos de fraccions K i una corba C sobre K amb $g(C) \geq 2$, existeix una extensió finita de Galois L/K i un model estable de $C \times_K L$

sobre R', on R' denota la clausura integral de R en L. Aplicacions d'aquest teorema es poden trobar en el Cap. 5.

2.3 Model regular minimal

2.3.1 Models regulars de superfícies aritmètiques

Començem per introduir la noció de model regular d'una superfície aritmètica.

Definició 2.3.1. Sigui $X \to S$ una superfície aritmètica. Un *model regular* de X és un parell $(Y \to S, f)$, on $Y \to S$ és una superfície aritmètica regular i $f : Y \dashrightarrow X$ es una aplicació birracional. Un morfisme de dos models regulars Y, Z de X és un morfisme de S-esquemes $Y \to Z$ que és compatible amb les aplicacions birracionals $Y \dashrightarrow X$, $Z \dashrightarrow X$.

Com ja hem assenyalat a la introducció, una superfície aritmètica $X \to S$ admet, en general, infinits models regulars. La següent definició introdueix un model regular amb una certa propietat de minimalitat que serà molt important als capítols posteriors.

Definició 2.3.2. Sigui $Y \to S$ una superfície aritmètica regular. Es diu que $Y \to S$ és *minimal* si tota aplicació birracional de S-superfícies aritmètiques regulars $Z \dashrightarrow Y$ és un morfisme birracional (és a dir, que tot morfisme $U \to Y$ de S-esquemes, on U és obert en Z, s'estén a un morfisme $Z \to Y$).

És evident que dos models regulars minimals d'una mateixa superfície aritmètica $X \to S$ són isomorfs. Per tant, podem parlar del *model minimal de* $X \to S$. La següent proposició ens dóna una propietat senzilla dels models minimals.

Proposició 2.3.3. *Sigui $X \to S$ una superfície aritmètica minimal. Aleshores la aplicació canònica $Aut_S(X) \to Aut(X_\eta)$ és bijectiva. En altres paraules, tot automorfisme de X_η s'estén de manera única a un automorfisme de X.*

Demostració. Un automorfisme $\sigma_\eta \in Aut(X_\eta)$ defineix una aplicació birracional $\sigma : X \dashrightarrow X$. Com X és minimal, σ s'estén a un morfisme. Considerant σ_η^{-1}, veiem que σ es un automorfisme de X. □

Per a determinar l'existència del model minimal necessitem el concepte de divisor excepcional, que definim a continuació.

Definició 2.3.4. Sigui $X \to S$ una superfície aritmètica regular. Un divisor primer E sobre X es diu *divisor excepcional* (també -1-*corba*) si existeix una superfície aritmètica regular $Y \to S$ i un morfisme $f : X \to Y$ de S-esquemes tal que $f(E)$ és un punt i $f : X \backslash E \to Y \backslash f(E)$ és un isomorfisme.

Com $f(E)$ és un punt, es dedueix que la imatge de E en S també es un punt i, per tant, que E és un divisor vertical.

És a dir, els divisors excepcionals són els que apareixen com a blow-ups de punts (cf. [17, p. 412]). És clar que l'existència de divisors excepcionals en un model implica que no és minimal: si Y es un model de $X \to S$ i E és

un divisor excepcional de Y, aleshores existeix $Y' \to S$ i un S-morfisme $f : Y \to Y'$ tal que E és el blow-up de $f(E)$. Deduïm que Y' és un model de X y que el morfisme $f^{-1}_{f(E)} : Y' \backslash f(E) \to Y \backslash E$ no s'estén a Y', per tant Y no és model minimal.

Les definicions següents semblen, doncs, naturals.

Definició 2.3.5. Donada una superfície aritmètica regular $X \to S$, es diu que és *relativament minimal* si no conté cap divisor excepcional.

Definició 2.3.6. Sigui $X \to S$ una superfície aritmètica. Un model regular Y de $X \to S$ es diu *model regular relativament minimal de* X si és relativament minimal com a superfície aritmètica regular sobre S.

Exemple 2.3.7. Una superfície aritmètica projectiva llisa $X \to S$ és relativament minimal. De fet, donat un divisor vertical V de X, es compleix $V^2 = 0$ (cf. [17, p. 418]) i es dedueix que V no és excepcional. Si a més $g(X_\eta) \geq 1$, aleshores $X \to S$ és minimal, com veurem al teorema 2.3.11.

Al contrari que el model regular minimal, el model regular relativament minimal no és únic en general, encara que sí que ho és en els casos que ens interessen (cf. 2.3.11). Per a determinar la relació entre el model regular minimal i el model regular relativament minimal, necessitem una caracterització intrínseca dels divisors excepcionals que és interessant per si mateixa.

Teorema 2.3.8 (Criteri de Castelnuovo). *Sigui $X \to S$ una superfície aritmètica projectiva i regular i $E \subseteq X_s$ un divisor primer vertical. Sigui $k' = H^0(E, \mathcal{O}_E)$. Aleshores*

E és un divisor excepcional si i solament si $E \simeq \mathbb{P}^1_{k'}$ i $E^2 = -[k' : k(s)]$.

A partir d'aquest criteri, es pot donar una altra caracterització dels divisors excepcionals.

Proposició 2.3.9. *Sigui $X \to S$ una superfície aritmètica projectiva i regular. Sigui $K_{X/S}$ un divisor canònic i $E \subseteq X_s$ un divisor primer vertical de X. Aleshores E és excepcional si i solament si $K_{X/S} \cdot E < 0$ i $E^2 < 0$. En aquest cas, es compleix $K_{X/S} \cdot E = E^2$.*

Les demostracions es poden trobar a [17, p. 416-417]. Mitjançant aquestes caracteritzacions, es pot demostrar que tota superfície aritmètica $X \to S$ té un model relativament minimal.

Teorema 2.3.10. *Sigui $X \to S$ una superfície aritmètica projectiva. Aleshores existeix un morfisme birracional $Y \to X$ de S-superfícies aritmètiques amb Y relativament minimal.*

Què podem dir sobre l'existència d'un model minimal? El raonament fet abans de la definició 2.3.5 prova que els models minimals són relativament minimals, i de fet que existeix un model minimal si i solament si tots els models minimals són isomorfs. El següent teorema ens assegura l'existéncia del model minimal pels cassos que ens interessen. La demostració es pot trobar a [17, p. 422].

Teorema 2.3.11. *Sigui $X \to S$ una superfície aritmètica projectiva amb $p_a(X_\eta) \geq 1$. Aleshores X admet un (únic) model minimal sobre S, i qualsevol model relativament minimal de X és minimal.*

Remarca 2.3.12. El teorema és fals sense la hipòtesi $p_a(X_\eta) \geq 1$. De fet, $X = \mathbb{P}^1_S$ ens dóna un contraexemple (cf. [17, p. 422]).

Donem ara un criteri per a determinar si una superfície aritmética és minimal. Aquest criteri és una conseqüència directa de la proposició 2.3.9 i el teorema 2.3.11.

Definició 2.3.13. Un divisor sobre una superfície aritmètica regular $X \to S$ es diu *numericament efectiu* si $D \cdot C \geq 0$ per a tot divisor primer vertical C.

Corol·lari 2.3.14. *Sigui $X \to S$ una superfície aritmètica projectiva amb $p_a(X_\eta) \geq 1$. Sigui $K_{X/S}$ un divisor canònic. Aleshores $X \to S$ és minimal si i solament si $K_{X/S}$ és numericament efectiu.*

Finalment, la següent proposició ens diu que la noció de model minimal és estable per certs canvis de base.

Proposició 2.3.15. *Sigui $X \to S$ una superfície aritmètica projectiva tal que $p_a(X_\eta) \geq 1$. Sigui $S' \to S$ un morfisme. Suposem que $S' \to S$ és étale i exhaustiu o que $S = Spec(R)$, amb R un anell de valoració discreta i $S' = Spec(\hat{R})$. Aleshores $X \to S$ és minimal si i solament si $X \times_S S' \to S'$ és minimal.*

2.3.2 Models de corbes

A continuació definim el concepte de model sobre S d'una corba definida sobre K.

Definició 2.3.16. Sigui C una corba normal, connexa i projectiva sobre K. Un *model de C sobre S* és una superfície aritmètica $\mathfrak{C} \to S$ amb un isomorfisme $f : \mathfrak{C}_\eta \to C$.

Es diu que $(\mathfrak{C}, f)$ verifica la propietat (P) si el morfisme $\mathfrak{C} \to S$ verifica (P). Un *morfisme* $\mathfrak{C} \to \mathfrak{C}'$ és un S-morfisme compatible amb els morfismes $f : \mathfrak{C}_\eta \to C$ i $f' : \mathfrak{C}'_\eta \to C$.

Normalment no mencionarem explícitament l'isomorfisme $f : \mathfrak{C}_\eta \to C$ i parlarem simplement del model $\mathfrak{C} \to S$.

Exemple 2.3.17. Sigui $S = \mathrm{Spec}(A)$ i suposem que C està definida per polinomis homogenis $f_1, \ldots, f_k \in K[X_0, \ldots, X_n]$. Multiplicant els polinomis per elements de A podem suposar que $f_1, \ldots, f_k \in A[X_0, \ldots, X_n]$. Aleshores, si $X = \mathrm{Proj}(A[X_0, \ldots, X_n]/(f_1, \ldots, f_k))$ és normal, es dedueix que X és un model de C.

Proposició 2.3.18. *Sigui C una corba llisa i projectiva sobre K de gènere (geomètric) g. Aleshores C admet un model projectiu regular relativament minimal sobre S. Si $g \geq 1$, aleshores C admet un únic model regular minimal $\mathfrak{C}_{min}$.*

Demostració. Construïm $\mathfrak{C}$ com al exemple 2.3.17. Es defineix $\mathfrak{C}_0$ com la clausura de Zariski de C en $\mathfrak{C}$. Aleshores $\mathfrak{C}_0$ admet una desingularització estricta (cf. [17, Cor. 8.3.51]), és a dir, existeix un esquema regular $\mathfrak{C}_{reg}$ i un morfisme birracional $\pi : \mathfrak{C}_{reg} \to \mathfrak{C}_0$ tal que π és un isomorfisme sobre tot punt regular de X. La proposició es dedueix ara del teorema 2.3.10. □

2.4 Model canònic

Donada una superfície aritmètica $X \to S$, el divisor canònic $K_{X/S}$ no és, en general, ample. Si volem obtindre un divisor canònic ample, cal fer una contracció de tots els divisors

primers verticals C que satisfan $K_{X/S} \cdot C = 0$. L'existència d'aquesta contracció està garantida pel criteri de contractibilitat d'Artin. Obtenim així el model canònic de X.

Definició 2.4.1. Sigui $X \to S$ una superfície minimal amb $p_a(X_\eta) \geq 2$. Sigui $f : X \to Y$ la contracció dels divisors primers verticals Γ tals que $K_{X/S} \cdot \Gamma = 0$. La superfície $Y \to S$ es diu el *model canònic* de X. Aquest model és singular sempre que existeix una component contreta.

La següent proposició ens dóna una propietat interessant del model canònic de $X \to S$.

Proposició 2.4.2. *Sigui $Y \to S$ un model canònic d'una superfície aritmètica minimal. Sigui $s \in S$ un punt tancat i n el nombre de components irreductibles de Y_s. Aleshores $n \leq 2p_a(X_\eta) - 2$.*

Per un tractament detallat del model canònic i les seves propietats, cf. [17, Cap. 9.4].

Introduïm a continuació el concepte de model canònic d'una corba projectiva llisa C sobre K.

Definició 2.4.3. Sigui C una corba projectiva llisa sobre K de gènere $g \geq 2$ i $\mathfrak{C}_{min}$ el seu model regular minimal sobre S (cf. 2.3.18). El model canònic $\mathfrak{C}_{can}$ associat a la superfície regular minimal $\mathfrak{C}_{min}$ es diu *model canònic de C*.

El següent diagrama l'hem extret de [17] i mostra el procés per a obtenir els diferents models de C sobre K, si $g(C) > 1$. Si C és una corba el·líptica amb un punt $o \in C(K)$, aleshores cal sustituïr $\mathfrak{C}_{can}$ pel model minimal de Weierstrass (cf. 2.4.6) i el morfisme $\mathfrak{C}_{min} \to \mathfrak{C}_{can}$ per la contracció de les -2-corbes Γ amb $\Gamma \cap \overline{\{o\}} = \emptyset$.

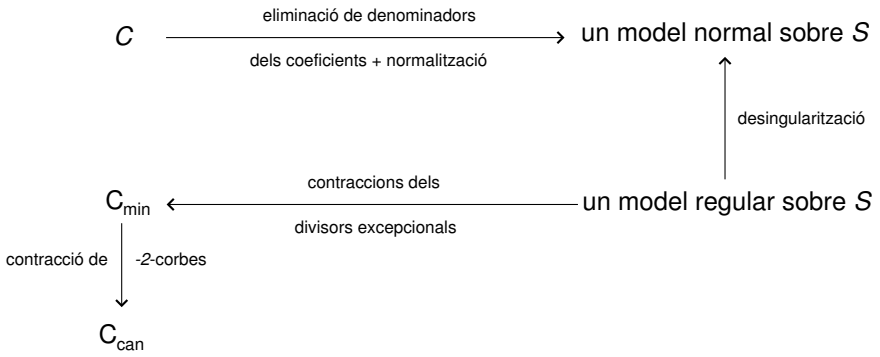


Figura 2.1: Obtenció dels models regular minimal i canònic.

Exemple 2.4.4. Sigui $S = \mathrm{Spec}(\mathbb{Z})$ i C la corba de Fermat

$$C: \quad x^4 + y^4 + z^4 = 0$$

definida sobre $\mathbb{Q}$. Anem a determinar explćitament el model regular minimal $\mathfrak{C}_{min}$ i el model canònic $\mathfrak{C}_{can}$ de C sobre S. Ho farem seguint el procés descrit a la figura 2.1. Començem per definir un model de C sobre S:

$$\mathfrak{C}: \quad \mathrm{Proj}(\mathbb{Z}[x,y,z]/(x^4 + y^4 + z^4))$$

És evident que $\mathfrak{C}$ és un esquema integre, projectiu i de dimensió 2 sobre $\mathbb{Z}$. A més, $f : \mathfrak{C} \to S$ és pla, ja que és no constant (cf. [17, p. 137]). Es pot probar també que $\mathfrak{C}$ és normal (cf. [17, p. 339]). Per tant, $\mathfrak{C}$ és un model de C sobre S.

El següent pas és trobar els punts singulars de $\mathfrak{C}$. En general, donada una superfície aritmètica de la forma $X = \mathrm{Spec}(\mathbb{Z}[x,y]/(f(x,y)))$ i un primer $p \in \mathbb{Z}$, un punt de X_p

és singular si i només si:

$$\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial p} = 0$$

Aplicant el criteri del jacobià (cf. [17, p. 130]) és fàcil veure que $\mathfrak{C}_p$ és llisa excepte quan $p = 2$, per tant, els punts singulars de $\mathfrak{C}$ es troben dins de la fibra $\mathfrak{C}_2$. Per a trobarlos, considerem en primer lloc l'obert afí $U = D_+(z) \subseteq \mathfrak{C}$. Fent el canvi de variable $y = v - 1$, $x = u + v$, l'equació $x^4 + y^4 + 1 = 0$ s'escriu:

$$u^4 + 2G = 0,\ G = (v^2 - v + 1)^2 + 3v^2u^2 + 2v^3u + 2vu^3\ (*)$$

Pel que s'ha dit abans, els punts singulars dins de U_2 corresponen als zeros de G mòdul 2 i, per tant, l'únic punt singular $q \in U_2$ correspon al ideal $\mathfrak{m} = (2, u, v^2 - v + 1)$. A més, la fibra $U_2 = \operatorname{Spec} \mathbb{F}_2[u, v]/(u^4)$ és una recta afí de multiplicitat 4. Per la simetria de l'equació inicial, és clar que q és l'únic punt singular de $\mathfrak{C}_2$.

Com que ja hem vist que l'únic punt singular de $\mathfrak{C}$ és q, per trobar un model regular fem un blowing-up $\tilde{\mathfrak{C}}$ de $\mathfrak{C}$ en el punt q. L'esquema $\mathfrak{C}$ és la unió de tres peces afins $\operatorname{Spec}(A_1)$, $\operatorname{Spec}(A_2)$ i $\operatorname{Spec}(A_3)$ i anem a trobar la fibra sobre 2 de $\tilde{\mathfrak{C}}$ pegant les fibres d'aquests esquemes.

Sigui $A = \mathbb{Z}[u, v]/(u^4 + 2G)$. La primera peça afí és $\operatorname{Spec}(A_1)$, amb $A_1 = A[u_1, v_1]$, $u_1 = u/2$, $v_1 = (v^2 - v + 1)/2$. Substituint aquestes relacions a l'equació $(*)$ obtenim:

$$A_1 = \mathbb{Z}[u, v, u_1, v_1]/I$$

amb

$$I = (2u_1 - u, 2v_1 - (v^2 - v + 1), 2u_1^4 + v_2^2 + 3v^2u_1^2 + v^3u_1 + 4vu_1^3)$$

i la fibra sobre 2 corresponent a aquesta peça afí és:

$$\mathrm{Spec}(\mathbb{F}_2[v,u_1,v_1]/(v^2-v+1,v_1^2+v^2u_1^2+v^3u_1))$$

que és una cònica afí llisa sobre $\mathbb{F}_2[v]/(v^2-v+1)=\mathbb{F}_4$. Similarment (cf. [17, p. 458]) es calculen les fibres sobre 2 corresponents a $\mathrm{Spec}(A_1)$ i $\mathrm{Spec}(A_2)$: obtenim una recta afí Γ_2 amb multiplicitat 2 i una altra cònica afí llisa sobre $\mathbb{F}_4$ que es pega amb la que hem trobat anteriorment per a donar una cònica llisa i projectiva Γ_1. Si fem un anàlisi semblant per $D_+(y)$ i $D_+(z)$, comprovem que el model $\tilde{\mathfrak{C}}$ és regular i que la seva fibra sobre 2 té tres components irreductibles Γ_0, Γ_1 i Γ_2, amb $\Gamma_0 \simeq \mathbb{P}^1_{\mathbb{F}_2}$, Γ_1 una cònica llisa sobre $\mathbb{F}_4$ i $\Gamma_2 \simeq \mathbb{P}^1_{\mathbb{F}_4}$. A més, obtenim $\Gamma_2\cdot\Gamma_0=2$ i $\Gamma_2\cdot\Gamma_1=4$, on els nombres d'intersecció es calculen sobre $\mathbb{F}_2$. Es dedueix (cf. [17, p. 384]) que $\Gamma_0^2=-1$ i, per tant, que Γ_0 és un divisor excepcional. Sigui $f:\tilde{\mathfrak{C}}\to\mathfrak{C}'$ la contracció de Γ_0 i $q_1=f(\Gamma_0)$. Aleshores $q_1\in\mathfrak{C}'(\mathbb{F}_2)$, ja que $\Gamma_0\simeq\mathbb{P}^1_{\mathbb{F}_2}$. La component $\Gamma_2':=f(\Gamma_2)$ és una cònica singular sobre $\mathbb{F}_2$, ja que és birracional amb $\Gamma_2\simeq\mathbb{P}^1_{\mathbb{F}_4}$ i conté un punt racional sobre $\mathbb{F}_2$. Es dedueix que cap component de $\mathfrak{C}'$ és excepcional i per tant que $\mathfrak{C}'=\mathfrak{C}_{min}$. Aplicant la fòrmula d'adjunció (cf. Cap. 1, Teorema 4.8) es dedueix que $\Gamma_2'\cdot K_{\mathfrak{C}_{min}/\mathbb{Z}}=0$ i que el model canònic $\mathfrak{C}_{can}$ de C s'obté fent una contracció de Γ_2'. La figura 2.2 mostra el procés que hem seguit per a obtindre els models de la corba C.

2.4.1 Corbes el·líptiques i models minimals de Weierstrass

En aquesta subsecció fixem una corba el·líptica E definida sobre K amb un punt distingit o. Aleshores E ve donada

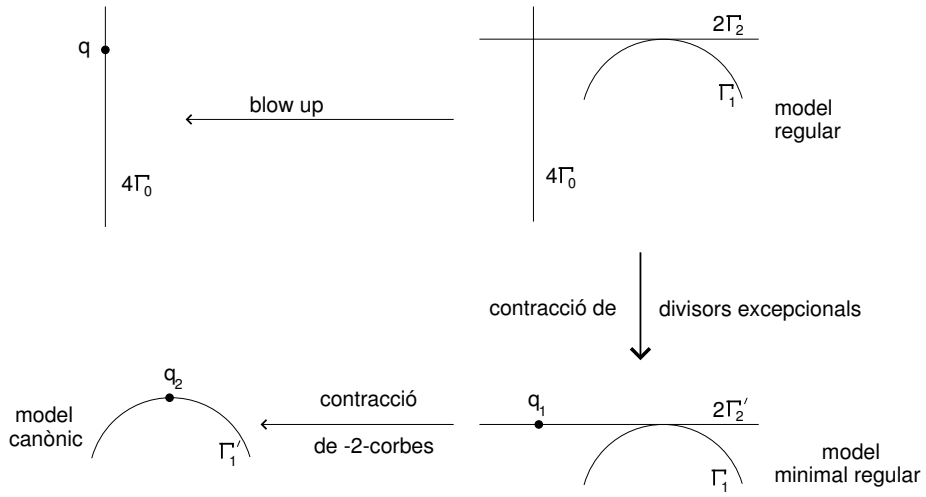


Figura 2.2: Exemple d'obtenció del model minimal regular i canònic.

per una equació de Weierstrass:

$$\text{E: } y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \quad (*)$$

on $a_1, \ldots, a_6 \in K$ i o s'identifica amb $(0, 1, 0)$.

Definició 2.4.5. Sigui E una corba el·líptica sobre K. Donada una equació de Weierstrass $(*)$ amb $a_1, \ldots, a_6 \in A$, l'esquema

$$W = \text{Proj } A[x, y, z]/I$$

amb

$$I = (y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3))$$

es diu *model de Weierstrass sobre A associat a $(*)$*.

Definició 2.4.6. Donat $s \in S$, sigui ν_s la valoració de K associada am l'anell local $\mathcal{O}_{S,s}$. Sigui W un model de Weierstrass de E sobre S, amb discriminant $\Delta_W \in A/A^*$. Es diu que W és *minimal en* s si $\nu_s(\Delta_W)$ és mínim dins del conjunt de valoracions en s dels discriminants de les equacions integrals de E. Es diu que W es *minimal sobre* S o simplement *minimal* si és minimal per a tot $s \in S$. És obvi que sempre existeix un model de Weierstrass minimal per a un s donat. Altrament, no sempre existeix un model de Weierstrass minimal.

Donada una corba el·líptica E sobre K, hem definit el seu model regular minimal i el seu model minimal de Weierstrass sobre S (encara que aquest últim no sempre existeix). Tots dos són importants, i el següent teorema ens dóna la relació entre ells i una manera d'obtindre l'un a partir de l'altre. Per a la demostració, cf. [17, p. 447].

Teorema 2.4.7. *Sigui (E, o) una corba el·líptica sobre K i $\rho : \mathfrak{C}_{min} \to S$ el model regular minimal de E sobre S. Aleshores es compleix:*

a) El conjunt $\mathcal{E}$ dels divisors primers verticals Γ de $\mathfrak{C}_{min}$ tal que $\Gamma \cup \overline{\{o\}} = \emptyset$ és finit i existeix un morfisme de contracció $f : \mathfrak{C}_{min} \to W'$ d'aquests divisors.

b) Si el feix invertible $\rho_*(\omega_{X/S})$ és lliure sobre S, aleshores $W' \to S$ és un model minimal de Weierstrass sobre S.

c) Si E admet un model minimal de Weierstrass W, aleshores $\rho_*(\omega_{X/S})$ és lliure sobre S i $W \simeq W'$. En particular, el model minimal de Weierstrass és únic.

Remarca 2.4.8. A partir del model regular minimal $\mathcal{C}_{min}$ de E, podem obtindre un altre model molt important per a l'estudi de l'aritmètica de E: el *model de Néron* $\mathcal{E}/A$. De fet, $\mathcal{E}/A$ s'obté com el subesquema més gran de $\mathcal{C}_{min}$ que és llis sobre A. Per a la definició i propietats d'aquest model, cf. Cap. 5, §2.

2.5 Models semiestables i estables

2.5.1 Reducció

Definició 2.5.1. Sigui C una corba normal i projectiva sobre K i s un punt de S. Una fibra $\mathfrak{C}_s$ d'un model $\mathfrak{C} \to S$ de C es diu una *reducció de C en s*. Si s correspon a un ideal $\mathfrak{p}$, una reducció $\mathfrak{C}_s$ es diu *reducció de C mòdul $\mathfrak{p}$*.

Per tant, la noció de reducció depén del model escollit per a C.

Definició 2.5.2. Sigui C una corba normal i projectiva sobre K i s un punt de S. Es diu que C *té bona reducció en s* si existeix un model llis de C sobre $\mathrm{Spec}(\mathcal{O}_{S,s})$.

Exemple 2.5.3. Sigui $p \neq 2$ i considerem la corba projectiva sobre $\mathbb{Q}$:

$$\mathrm{Proj}\ \mathbb{Q}[x,y,z]/(xy - p^2z^2).$$

Aquesta corba admet com a models els següents esquemes:

$$\mathfrak{C}_1 = \mathrm{Proj}\ \mathbb{Z}[x,y,z]/(xy - p^2z^2)$$

$$\mathfrak{C}_2 = \mathrm{Proj}\ \mathbb{Z}[x,y,z]/(xy - z^2)$$

És clar que el esquema $\mathfrak{C}_2$ és llis, mentre que el esquema $\mathfrak{C}_1$ no ho és. Es dedueix que C té bona reducció per a tot $p \in \mathbb{Z}$.

Proposició 2.5.4. *Sigui C una corba llisa i projectiva sobre K, amb gènere $g \geq 1$. Aleshores:*

a) La corba C té bona reducció en $s \in S$ excepte en un nombre finit de punts de S.

b) La corba C té bona reducció sobre S si i solament si el model minimal regular $\mathfrak{C}_{min}$ és llis. En aquest cas, $\mathfrak{C}_{min}$ és l'únic model llis de C sobre S.

c) Sigui $S' \to S$, on $S' = \operatorname{Spec} A'$ és l'espectre d'un anell de Dedekind A' amb cos de fraccions K', tal que S' és étale sobre S o $S' = Spec(\widehat{\mathcal{O}_{S,s}})$. Sigui $s' \in S'$ i s la seva imatge en S. Aleshores $C_{K'}$ té bona reducció en s' si i solament si C té bona reducció en s.

Demostració. a) Raonant com al exemple 2.3.17, és clar que existeix un esquema projectiu $\mathcal{C}$ amb fibra genèrica $\mathcal{C}_\eta \simeq C$ i una aplicació exhaustiva $\mathcal{C} \to U$, on U és un subesquema obert no buit de S. La clausura de Zariski de C en $\mathcal{C}$ és un esquema integral i per tant pla sobre U (cf. [17, p. 137]). Com $\mathcal{C}_\eta \simeq C$ és llisa per hipòtesi, es dedueix (cf, [17, p. 352]) que existeix un subesquema obert no buit V de U tal que $\mathcal{C}_V \to V$ és llis, és a dir, que C té bona reducció sobre V. Com S té dimensió 1, és clar que $S - V$ és finit.
b) Suposem que C té bona reducció sobre S (l'altra implicació és òbvia). Sigui $\mathfrak{C}_{min}$ el model regular minimal de C (cf. Prop. 2.3.18) i $s \in S$. Sigui $\mathcal{C}' \to \operatorname{Spec}(\mathcal{O}_{S,s})$

un model llis de C. Aleshores $\mathcal{C}'$ és minimal (cf. exemple 2.3.7) i $\mathcal{C}_{min} \times_S \mathcal{O}_{S,s}$ també ho és, aplicant la prop. 2.3.15. De la unicitat del model regular minimal es dedueix que $\mathcal{C}_{min} \times_S \mathcal{O}_{S,s} \simeq \mathcal{C}'$ i per tant $\mathcal{C}_{min}$ és llis. Com els models llisos són relativament minimals, tots són isomorfs a $\mathcal{C}_{min}$. La part c) es dedueix de b) utilitzant la proposició 2.3.15. □

Com a conseqüència immediata d'aquesta proposició, vegem a continuació que per a corbes el·líptiques la condició de bona reducció es pot formular en termes del discriminant.

Corol·lari 2.5.5. *Sigui E una corba el·liptica sobre $K = K(S)$. Sigui $s \in S$, W un model minimal de Weierstrass de E sobre Spec$(\mathcal{O}_{S,s})$ i Δ el discriminant de W. Les següents afirmacions són equivalents:*

a) E té bona reducció en s.

b) W_s és llis sobre $k(s)$.

c) $\Delta \in \mathcal{O}_{S,s}^*$.

Demostració. L'equivalència $b) \Leftrightarrow c)$ és ben coneguda (cf. [33, Prop. 1.4]) i la implicació $b) \Rightarrow a)$ és certa per definició. Si E té bona reducció, aleshores el model minimal $\mathcal{C} = \mathcal{C}_{min} \to \text{Spec}(\mathcal{O}_{S,s})$ és llis per la proposició anterior, en particular $\mathcal{C}_s$ és llis i aplicant el teorema 2.4.7 es dedueix que $\mathcal{C} = W$. □

Aquest corol·lari ens dóna una caracterització de la bona reducció en $s \in S$ per a corbes de gènere $g = 1$. Veiem a continuació una condició suficient per a la bona reducció en

$s \in S$ per a corbes de gènere $g \geq 2$. Per a la demostració, veure [17, p. 464].

Corol·lari 2.5.6. *Sigui C una corba projectiva llisa i connexa sobre K de gènere $g \geq 2$ i $s \in S$ un punt tancat. Sigui W^0 un esquema quasi-projectiu sobre S tal que:*

i) W^0_η sigui un subsesquema obert de C,

ii) W^0_s sigui llisa sobre $k(s)$ i

iii) $K(W^0_s)$ sigui el cos de funcions d'una corba projectiva llisa de gènere g.

Aleshores C té bona reducció en s i, reemplaçant si és necessari S per un entorn obert de s, W^0 és un subesquema obert del model llis de C sobre S.

Una noció que serà important en els capítols posteriors és la de *bona reducció potencial*. Com hem vist (cf. prop. 2.5.4), els canvis de base étales no canvien les propietats de bona o mala reducció. Això no és cert per a canvis de base més generals.

Definició 2.5.7. Sigui C una corba projectiva llisa sobre K. Diem que C té *bona reducció potencial en $s \in S$* si existeix un anell de Dedekind A' amb cos de fraccions L, un morfisme $f : \mathrm{Spec}(A') \to S$ i $s' \in \mathrm{Spec}(A')$ amb $f(s') = s$ tal que C_L té bona reducció en s'.

És obvi que la bona reducció implica bona reducció potencial.

2.5.2 Estabilitat de corbes

Començem per introduir la noció de punts múltiples ordinaris. Intuitivament, aquests punts són singulars, però amb direccions tangents distintes.

Definició 2.5.8. Sigui C una corba algebraica sobre un cos algebraicament tancat K i sigui $x \in C(K)$. Diem que x és un *punt múltiple ordinari* si existeix $m = m_x \geq 1$ tal que $\widehat{\mathcal{O}_{C,x}} \simeq K[[T_1, \ldots, T_m]]/(T_i T_j)_{i \neq j}$. Si $m_x = 2$, es diu que x és un *punt doble ordinari o node* de C.

Amb la mateixa notació que a la definició, sigui $\pi : C' \to C$ el morfisme de normalització de C, m_x el nombre de punts de $\pi^{-1}(x)$ i $\mathcal{O}'_{C,x}$ la clausura integral de $\mathcal{O}_{C,x}$ en el seu cos de fraccions. Es pot probar que la definició de punt múltiple ordinari és equivalent a la igualtat $\dim_k \mathcal{O}'_{C,x}/\mathcal{O}_{C,x} = m_x - 1$ (cf [17, p. 310]).

Definició 2.5.9. Sigui C una corba algebraica sobre un cos algebraicament tancat k. Diem que C és *semiestable* si és reduïda i els seus punts singulars són punts dobles ordinaris. Diem que C és *estable* si és semiestable i es compleix:

i) La corba C és connexa i projectiva amb gènere aritmètic $p_a(C) \geq 2$.

ii) Sigui Γ una component irreductible de C i suposem que $\Gamma \simeq \mathbb{P}^1_k$. Aleshores Γ interseca a les altres components irreductibles en com a mínim tres punts.

Definició 2.5.10. Diem que una corba C sobre un cos k és *semiestable* (resp. *estable*) si l'extensió $C_{\overline{k}}$ a la clausura algebraica $\overline{k}$ de k és una corba semiestable (resp. estable) sobre $\overline{k}$.

Exemple 2.5.11. Anem a veure quines són les corbes estables de gènere 2 sobre un cos algebraicament tancat K. Sigui C una corba projectiva reduïda sobre K i siguin X_1, ..., X_n les seves components irreductibles. Denotem per X_i' la normalització de X_i i per $\mathcal{O}'_{X,x}$ la clausura integral de $\mathcal{O}_{X,x}$ en el seu cos de fraccions. Aleshores es compleix (cf. [17, p. 304] per a la demostració):

$$p_a(X) + n - 1 = \sum_{i=1}^{n} p_a(X_i') + \sum_{x \in X} \dim_k \mathcal{O}'_{X,x}/\mathcal{O}_{X,x}$$

Si C és estable, aleshores $\dim_k \mathcal{O}'_{X,x}/\mathcal{O}_{X,x} = 1$ per a tot punt singular x, per tant, si S denota el nombre de punts singulars de C, obtenim

$$p_a(X) + n - 1 = \sum_{i=1}^{n} p_a(X_i') + S$$

Amb aquesta relació es dedueix que tenim únicament set possibilitats per a corbes de gènere 2 sobre K. A la figura 2.3 hem representat aquestes configuracions. Els nombres denotan el gènere de la normalització de la component corresponent, i les components sense nombre ssn racionals.

Definició 2.5.12. Sigui $f : X \to S$ una superfície aritmètica. Es diu que és *semiestable*, o que X és una *corba semiestable sobre* S, si per cada $s \in S$, la fibra X_s és una corba semiestable sobre $k(s)$. Es diu que f és *estable* de gènere $g \geq 2$, o que X és una *corba estable sobre* S de gènere $g \geq 2$, si f és propi, amb fibres estables de gènere aritmètic g.

La següent proposició ens diu que la semiestabilitat es manté quan fem un canvi de base. La prova depén únicament

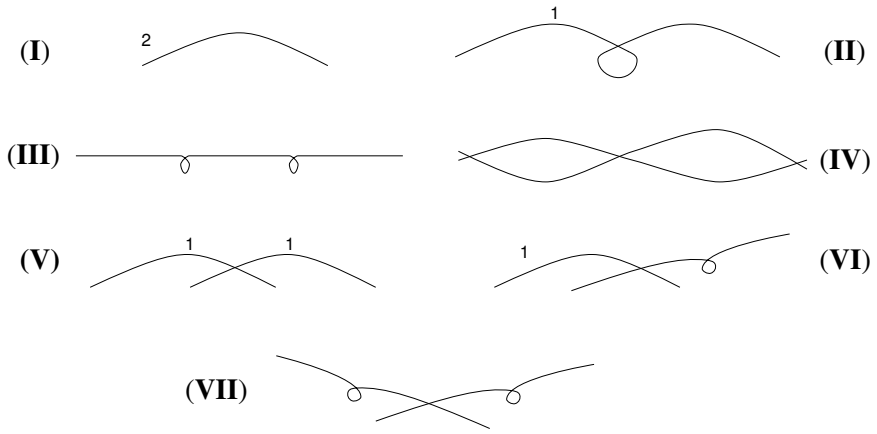


Figura 2.3: Corbes estables de gènere 2.

de propietats elementals de canvi de base de morfismes plans i propis.

Proposició 2.5.13. *Sigui $f : X \to S$ una corba semiestable sobre un esquema S. Aleshores es compleix:*

a) Sigui $S' \to S$ un morfisme. Aleshores $X \times_S S' \to S'$ és semiestable. Si f és estable, aleshores $X \times_S S' \to S'$ també ho és.

b) Si la fibra genèrica X_η de X és normal, aleshores X és normal.

2.5.3 Reducció estable i semiestable

Definició 2.5.14. Sigui C una corba projectiva estable sobre K. Diem que C *té reducció semiestable* (resp. *reducció estable*) *en* $s \in S$ si existeix un model $\mathfrak{C} \to \mathrm{Spec}(\mathcal{O}_{S,s})$ de C que sigui semiestable (resp. estable). Veurem a continuació que, per a corbes de gènere $g \geq 2$, el model estable

és únic (el semiestable no). La fibra especial $\mathfrak{C}_s$ del model semiestable (resp. estable) $\mathfrak{C}$ es diu *la reducció semiestable* (resp. *estable*) *de* C *en* $s \in S$. Diem que C *té reducció semiestable* (resp. *estable*) *sobre* S si té aquesta propietat per a tot $s \in S$. Un model $\mathfrak{C} \to S$ és diu *model estable* si $\mathfrak{C} \to S$ és una corba estable.

Obviament, si C té bona reducció en $s \in S$, aleshores C té reducció estable en S.

Teorema 2.5.15. *Sigui* C *una corba projectiva llisa sobre* K*, de gènere* $g \geq 1$*. Suposem que* C *té reducció semiestable sobre* S*. Aleshores es compleix:*

a) El model regular minimal $\mathfrak{C}_{min}$ *de* C *sobre* S *és semiestable sobre* S*.*

b) Suposem que $g \geq 2$ *i que* C *és geomètricament connexa sobre* K*. Aleshores el model canònic* $\mathfrak{C}_{can}$ *de* C *sobre* S *és una corba estable sobre* S *i és l'únic model estable sobre* S*.*

c) La corba C *té un model semiestable sobre* S*. Si* C *té reducció estable sobre* S*, aleshores té un model estable sobre* S*.*

Com a conseqüència immediata d'aquest teorema i de resultats enunciats anteriorment, obtenim:

Corol·lari 2.5.16. *Sigui* C *una corba llisa i projectiva sobre* K *amb* $p_a(C) \geq 1$ *i* $S' = \operatorname{Spec} A'$ *tal que* S' *domina a* S*. Sigui* $K' = Frac(A')$*. Aleshores:*

a) Si C *té reducció semiestable (resp. estable) sobre* S*, aleshores* $C_{K'}$ *té reducció semiestable (resp. estable)*

sobre S'. Si $\mathfrak{C}$ és un model semiestable (resp. estable) de C sobre S, aleshores $\mathcal{C} \times_S S'$ és un model semiestable (resp.estable) de $C_{K'}$ sobre S'.

b) Si C té reducció estable $\mathfrak{C}_s$ en $s \in S$ i $f(s') = s$, aleshores $\mathfrak{C}_s \times_{Spec(k(s))} Spec(k(s'))$ és la reducció estable de $C_{K'}$ en s'.

c) Suposem a més que es compleix un dels següents: i) $S' \to S$ és étale i exhaustiu, ii) $S = Spec(A)$ és local i $S' = Spec(\hat{A})$. Si $C_{K'}$ té reducció semiestable (resp. estable) sobre S', aleshores C té reducció semiestable (resp. estable) sobre S.

Corol·lari 2.5.17. *Sigui C una corba llisa i projectiva sobre K i suposem que C admet un model estable $\mathfrak{C}$ sobre S. Aleshores els automorfismes de C sobre K s'estenen de manera única a $S-$automorfismes de $\mathfrak{C}$.*

Proposició 2.5.18. *Sigui $X \to S$ una corba estable amb fibra genèrica X_η llisa i $s \in S$. Aleshores l'aplicació canònica $Aut(X_\eta) \to Aut(X_s)$ és injectiva.*

2.5.4 El teorema de Deligne-Mumford

Donat un anell de Dedekind A amb cos de fraccions K i una extensió finita L de K, denotarem per A' la clausura integral de A en L. Aleshores, la normalització S' de S en L (cf. [17, p. 120]) és l'esquema afí $S' = \text{Spec } A'$. Per exemple, si $S = \text{Spec}(\mathcal{O}_K)$, aleshores $S' = \text{Spec}(\mathcal{O}_L)$. Considerem una corba projectiva llisa i geomètricament connexa C sobre K.

Teorema 2.5.19 (Deligne-Mumford, [6]). *Sigui C una corba llisa, projectiva i geomètricament connexa de gènere*

$g \geq 2$ sobre K. Aleshores existeix una extensió finita i separable L/K tal que C_L té un únic model estable sobre S'. A més, L/K es pot triar de Galois.

Capítol 3

Tipus de Reduccions de Corbes

Xavier Guitart[1]

3.1 Introducció

Sigui C/K una corba projectiva llisa definida sobre el cos de fraccions d'un anell de valoració discreta R. Si $\mathcal{C}/R$ és un model enter de la corba sobre R, aleshores té sentit reduir-lo mòdul el primer $\mathfrak{p}$ de l'anell, obtenint així una corba sobre el cos residual. L'objectiu d'aquest capítol és estudiar les possibles corbes que es poden obtenir d'aquesta manera, en funció del gènere de C i en el cas en què el model enter de la corba sigui regular, propi i minimal.

Com que la reducció mòdul $\mathfrak{p}$ de $\mathcal{C}$ és la seva fibra especial (i.e. la seva fibra en $\mathfrak{p}$, que denotarem $\mathcal{C}_{\mathfrak{p}}$), tenim un morfisme d'esquemes $\pi : \mathcal{C} \to \mathrm{Spec}(R)$ tal que la seva fibra

[1]Dep. Matemàtica Aplicada II, Universitat Politècnica de Catalunya.
E-mail: xevi.guitart@gmail.com

en el punt genèric de Spec(R) és la corba C i volem determinar les possibilitats per a la fibra en el punt tancat $\mathfrak{p}$. Això és l'anàleg aritmètic del problema geomètric següent: donat un morfisme $\pi : V \to F$ on V és una superfície i F una corba tal que la fibra genèrica de π és un corba no singular C (podem pensar per exemple que V és una corba sobre el cos de funcions de F), determinar les possibilitats per a les fibres de π en cada punt de F. Aquest problema geomètric és el que va resoldre Kodaira a [12] en el cas en què C sigui una corba el·líptica; com que el seu argument només utilitzava resultats de teoria de la intersecció que també són vàlids en el context aritmètic, Néron el va adaptar al problema de la reducció de corbes a [23]. Posteriorment Ogg va tractar el problema amb C una corba de gènere 2 a [25], i Artin i Winters ho van fer amb C una corba de gènere g arbitrari [1].

El cas en què la corba sigui una corba el·líptica és el més senzill i serà el que tractarem a la primera secció. El que obtindrem serà una classificació completa de les possibles reduccions (la classificació de Kodaira-Néron), a partir d'un raonament purament combinatori estudiant de manera exhaustiva les interseccions entre les diferents components irreductibles de la reducció mòdul $\mathfrak{p}$ de la corba.

El contingut de la segona secció serà mostrar com aquest mateix raonament es pot traslladar a les corbes de gènere 2 per a obtenir també en aquest cas una llista amb totes les configuracions possibles (classificació d'Ogg). En aquest cas, però, el nombre de configuracions ja és considerablement més gran, la qual cosa fa inviable repetir la mateixa estratègia per a corbes de gènere superior.

A la tercera secció introduirem una certa estructura combinatòria al problema que servirà alhora per a clarificar una mica els raonaments dels dos primers apartats, i també per a poder dir alguna cosa sobre quina és la situació per a gèneres superiors a 2. En particular, tot i no obtenir una classificació completa sí que veurem que el nombre de configuracions possibles per a cada gènere és, en un cert sentit, finit.

Notacions: En tot el capítol R serà un anell de valoració discreta amb ideal maximal $\mathfrak{p}$, K el seu cos de fraccions i $k = R/\mathfrak{p}$ el seu cos residual, que suposarem algebraicament tancat.

3.2 Classificació de Kodaira-Néron per a corbes el·líptiques

Si E/K és una corba el·líptica donada per una equació de Weierstrass, un model sobre R de la corba que sempre podem considerar és el model minimal de Weierstrass, que sabem que en reduir-lo mòdul $\mathfrak{p}$ obtindrem una corba sobre k que serà, o bé una corba el·líptica, o bé una corba racional amb un node o una cúspide. En aquesta secció farem la mateixa classificació però no per al model minimal de Weierstrass, sinó per a un model propi regular minimal, de manera que apareixeran altres possibilitats a part de les tres ja esmentades, que consistiran totes elles en unions de corbes racionals amb diverses multiplicitats. Recordem que el fet que el model sobre R sigui minimal vol dir que no té

divisors excepcionals (i.e. isomorfs a $\mathbb{P}^1$ i amb autointersecció -1), i que sigui propi implica que hi ha una bijecció entre punts K-valuats de E i punts R-valuats de $\mathcal{C}$.

Sigui doncs E/K una corba el·líptica i sigui $\mathcal{C}/R$ un model propi regular minimal de E/K amb fibra especial

$$\mathcal{C}_{\mathfrak{p}} = \sum_{i=1}^{r} n_i \Gamma_i$$

on $\Gamma_1, \ldots, \Gamma_r$ són les seves components irreductibles i n_1, $\ldots$, n_r les multiplicitats amb què apareixen. L'estratègia per a trobar totes les configuracions possibles per a $\mathcal{C}_{\mathfrak{p}}$ consisteix en utilitzar la teoria de la intersecció per a, en primer lloc, trobar quin tipus de corbes poden ser les Γ_i i, seguidament, limitar les configuracions segons les interseccions permeses entre elles. Comencem doncs amb un lema que ens servirà per a fer aquests càlculs:

Lema 3.2.1. *Sigui E/K una corba el·líptica i sigui $\mathcal{C}/R$ un model regular propi minimal amb fibra especial*

$$\mathcal{C}_{\mathfrak{p}} = \sum_{i=1}^{r} n_i \Gamma_i$$

i denotem per $K_{\mathcal{C}}$ el divisor canònic de $\mathcal{C}$. Aleshores:

1. *algun dels n_i és 1*
2. *$K_{\mathcal{C}} \cdot \mathcal{C}_{\mathfrak{p}} = 0$*
3. *$K_{\mathcal{C}} \cdot \Gamma_i = 0$ per a tot i.*

Demostració. (1) Si tots els n_i fossin almenys 2, aleshores tots els punts de $\mathcal{C}_{\mathfrak{p}}$ serien singulars, però sabem que la

fibra genèrica de $\mathcal{C}$ és la corba el·líptica E/K, que té un punt racional; com que el model és propi $\mathcal{C}(R) \cong E(K)$ i per tant $\mathcal{C}$ té almenys un punt R-valuat P, per tant $P(\mathfrak{p})$ és un punt no singular de $\mathcal{C}_\mathfrak{p}$ ja que $\mathcal{C}/R$ és regular (cf. [34], capítol IV, proposicions 4.3 i 4.4).

(2) Aplicant la fòrmula d'adjunció a $\mathcal{C}_\mathfrak{p}$ tenim:

$$\mathcal{C}_\mathfrak{p}^2 + K_\mathcal{C} \cdot \mathcal{C}_\mathfrak{p} = 2p_a(\mathcal{C}_\mathfrak{p}) - 2$$

i com que $\mathcal{C}_\mathfrak{p}^2 = 0$ i $p_a(\mathcal{C}_\mathfrak{p}) = p_a(E) = 1$ per Capítol 1 proposició 4.7, obtenim que $K_\mathcal{C} \cdot \mathcal{C}_\mathfrak{p} = 0$.

(3) La fòrmula d'adjunció per a cada Γ_i ens diu que

$$\Gamma_i^2 + K_\mathcal{C} \cdot \Gamma_i = 2p_a(\Gamma_i) - 2$$

Si per algun i es té que $\Gamma_i^2 = 0$, aleshores per Capítol 1 proposició 4.7 resulta que Γ_i és múltiple racional de $\mathcal{C}_\mathfrak{p}$ i aleshores només pot ser $\mathcal{C}_\mathfrak{p} = \Gamma_i$ i per tant $K_\mathcal{C} \cdot \Gamma_i = K_\mathcal{C} \cdot \mathcal{C}_\mathfrak{p} = 0$.

Si per contra $\Gamma_i^2 < 0$ per a tot i, aleshores necessàriament també s'ha de complir que $K_\mathcal{C} \cdot \Gamma_i \geq 0$ per a tot i. En efecte, si tinguéssim que $K_\mathcal{C} \cdot \Gamma_i < 0$ per algun i, aleshores $2p_a(\Gamma_i) - 2 = \Gamma_i^2 - K_\mathcal{C} \cdot \Gamma_i < 0$ i per tant només pot ser $p_a(\Gamma_i) = 0$ i $\Gamma_i^2 = -1$, cosa que no és possible pel criteri de Castelnuovo ja que estem suposant que $\mathcal{C}$ és un model minimal. Així doncs, el fet que $K_\mathcal{C} \cdot \mathcal{C}_\mathfrak{p} = 0$ ens diu que

$$\sum_{i=1}^{r} n_i K_\mathcal{C} \cdot \Gamma_i = 0$$

i com que hem vist que $K_\mathcal{C} \cdot \Gamma_i \geq 0$ ha de ser $K_\mathcal{C} \cdot \Gamma_i = 0$ per a tot i. □

La següent proposició és la que ens diu quines possibilitats tenim per a les components irreductibles de la fibra especial.

Proposició 3.2.2. *Sigui E/K una corba el·líptica i $\mathcal{C}/R$ un model regular propi minimal de E/K amb fibra especial*

$$\mathcal{C}_{\mathfrak{p}} = \sum_{i=1}^{r} n_i \Gamma_i$$

1. *Si $r = 1$ aleshores $\mathcal{C}_{\mathfrak{p}} = \Gamma_1$, $p_a(\Gamma_1) = 1$ i $\Gamma_1^2 = 0$*
2. *Si $r > 1$ aleshores $p_a(\Gamma_i) = 0$ i $\Gamma_i^2 = -2$ per a tot i*

Demostració. (1) És clar que si $r = 1$ aleshores n_1 ha de ser 1 pel primer apartat del lema anterior. A més, ja sabem que el gènere aritmètic de $\mathcal{C}_{\mathfrak{p}}$ ha de ser 1 i que $\mathcal{C}_{\mathfrak{p}}^2 = 1$.

(2) La fòrmula d'adjunció aplicada a Γ_i diu que

$$\Gamma_i^2 = 2p_a(\Gamma_i) - 2$$

Però Γ_i^2 no pot ser zero perquè aleshores segons Capítol 1 proposició 4.7, Γ_i seria múltiple de $\mathcal{C}_{\mathfrak{p}}$, que és impossible si $r > 1$. Per tant $\Gamma_i^2 < 0$ i això només pot ser si $p_a(\Gamma_i) = 0$ i per tant $\Gamma_i^2 = -2$. □

Per tant, la fibra especial és, o bé una corba de gènere aritmètic 1, o bé una unió de corbes isomorfes a $\mathbb{P}_k^1$ que tenen autointersecció -2. Una vegada sabem com són les possibles components irreductibles de la fibra especial, el que queda fer és veure com són les interseccions entre aquestes fibres; més concretament el que ens fa falta és saber quants cops talla una component Γ_i amb la resta de la fibra. Això

ens ho dóna directament la proposició 4.7 del Capítol 1 que ens diu que $\mathcal{C}_\mathfrak{p} \cdot \Gamma_i = 0$ i per tant

$$\sum_{j \neq i} n_j \Gamma_j \cdot \Gamma_i = 2n_i \tag{3.2.1}$$

Teorema 3.2.3 (Classificació de Kodaira-Néron). *Sigui E/K una corba ell·íptica. Si $\mathcal{C}/R$ és un model regular propi minimal de E/K aleshores $C_\mathfrak{p}$ correspon a un dels tipus següents:*

Tipus I_0 *corba no singular de gènere 1.*

Tipus I_1 *corba racional singular amb un node.*

Tipus I_n *n corbes isomorfes a $\mathbb{P}^1_k$ en forma de polígon de n costats.*

Tipus II *corba racional amb una cúspide.*

Tipus III *dues corbes isomorfes a $\mathbb{P}^1_k$ que es tallen en un punt amb multiplicitat 2.*

Tipus IV *tres corbes isomorfes a $\mathbb{P}^1_k$ que es tallen en un punt.*

Tipus I_0^* *cinc corbes isomorfes a $\mathbb{P}^1_k$ disposades tal com s'indica a la figura 3.1.*

Tipus I_n^* *$n+1$ corbes isomorfes a $\mathbb{P}^1_k$ de multiplicitat 2 que es tallen com indica la figura 3.1, amb dues corbes isormorfes a $\mathbb{P}^1_k$ de multiplicitat 1 que tallen les dels extrems.*

Tipus IV^* *set corbes isomorfes a $\mathbb{P}^1_k$ disposades tal com s'indica a la figura 3.1.*

Tipus III^* *cinc corbes isomorfes a* $\mathbb{P}^1_k$ *disposades tal com s'indica a la figura 3.1.*

Tipus II^* *nou corbes isomorfes a* $\mathbb{P}^1_k$ *disposades tal com s'indica a la figura 3.1.*

Remarca 3.2.4. Per tal d'interpretar correctament la figura 3.1 notem que els nombres que apareixen al costat de cada component indiquen la seva multiplicitat i que totes les interseccions entre les components irreductibles de $\mathcal{C}_\mathfrak{p}$ són simples, llevat de la del tipus III que és doble.

Demostració. No donarem tots els detalls de la prova, que es poden trobar per exemple a [34], secció 8 del capítol IV, però sí que n'indicarem els primers passos per a donar una idea del tipus d'argument combinatori que s'utilitza.

Escrivim com sempre la fibra especial de $\mathcal{C}$ com

$$\mathcal{C}_\mathfrak{p} = \sum_{i=0}^{r} n_i \Gamma_i.$$

Ara cal distingir segons si $r = 1$, $r = 2$ o $r \geq 3$.

Si $r = 1$ el lema anterior ens diu que $\mathcal{C}_\mathfrak{p}$ és una corba de gènere aritmètic 1, i en aquest cas només pot ser una corba no singular de gènere 1, una corba racional singular amb un node o una corba racional singular amb una cúspide. Això ens dóna els tipus I_0, I_1 i II. A més, aquests seran els únics casos on $\mathcal{C}_\mathfrak{p}$ té divisors irreductibles de gènere aritmètic 1. Per 3.2.2 si $r > 1$ totes les components irreductibles de $\mathcal{C}_\mathfrak{p}$ seran de gènere aritmètic 0 (i.e. isomorfes a $\mathbb{P}^1_k$) i amb autointersecció -2.

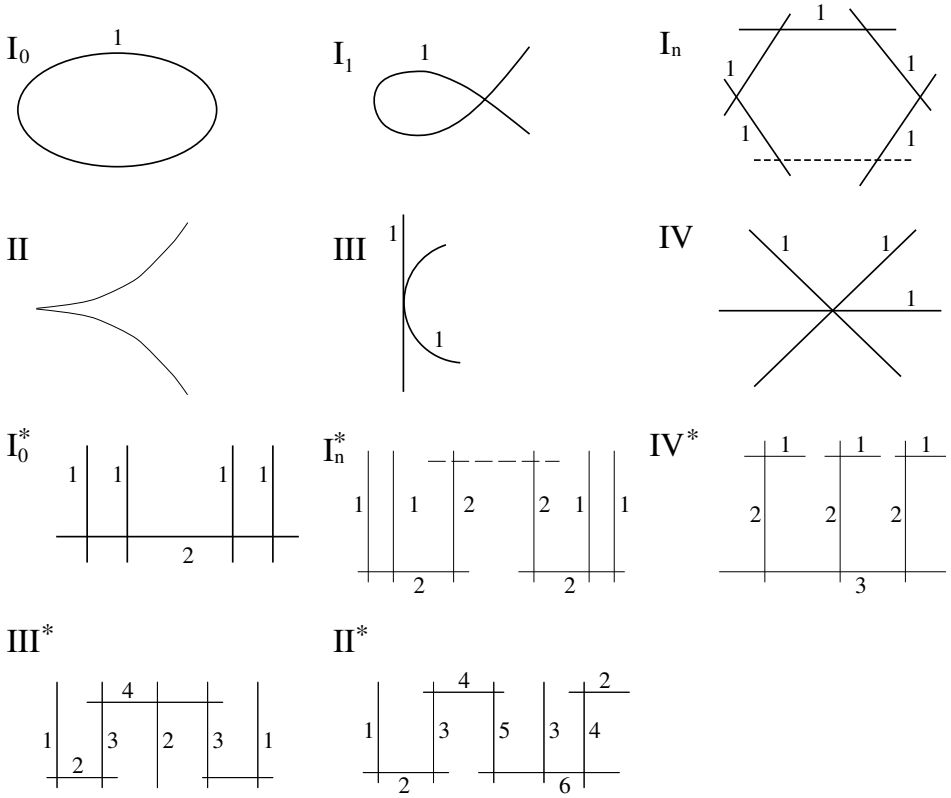


Figura 3.1: Classificació de Kodaira-Néron per a la fibra especial del model regular propi minimal d'una corba el·líptica

Suposem doncs a partir d'ara que $r > 1$. Sabem que alguna de les components de $\mathcal{C}_{\mathfrak{p}}$ apareix amb multiplicitat 1, i el que cal fer ara és començar per aquesta component, diguem-ne Γ_1 i mirar quina és la seva intersecció amb la resta de la fibra segons la fòrmula (3.2.1). Això ens donarà totes les possibilitats per a les components de la fibra que tallin Γ_1. Aleshores si pot haver-hi alguna component que no talli Γ_1, a aquesta component cal aplicar-li novament (3.2.1) i tornar a mirar com són les components que tallen

aquesta, i així successivament.

Si $r = 2$ aleshores $\mathcal{C}_\mathfrak{p} = \Gamma_1 + n_2\Gamma_2$ i aplicant (3.2.1) a Γ_1 tenim que $n_2\Gamma_2 \cdot \Gamma_1 = 2$. Aquí hi podria haver dues opcions, però aplicant novament (3.2.1) aquest cop a Γ_2 resulta $\Gamma_1 \cdot \Gamma_2 = 2n_2$ amb la qual cosa ha de ser $\Gamma_1 \cdot \Gamma_2 = 2$ i $n_2 = 1$. Això dóna els tipus III si Γ_1 i Γ_2 es tallen en un punt de multiplicitat 2 i el tipus I_2 si es tallen en 2 punts de multiplicitat 1.

Si $r \geq 3$, aleshores es pot provar que $\Gamma_i \cdot \Gamma_{i'} \leq 1$ per a tot $i \neq i'$. Com que $\mathcal{C}_\mathfrak{p}$ és connexa algun $\Gamma_i \cdot \Gamma_1$ serà positiu; suposem que és Γ_2, amb la qual cosa $\Gamma_1 \cdot \Gamma_2 = 1$. Aleshores convé distingir entre els casos $n_2 = 1$ i $n_2 > 1$.

Si $n_2 = 1$ aplicant (3.2.1) a Γ_2 obtenim que

$$\sum_{j=3}^{r} n_j \Gamma_j \cdot \Gamma_2 = 1$$

i per tant només hi ha una altra component que talla Γ_2, posem Γ_3 i a més $n_3 = 1$. Si Γ_3 talla Γ_1, pot ser que talli en el mateix punt que talla Γ_2 o en un altre de diferent. Si ho fa en el mateix, aleshores la fibra és de tipus IV, i si ho fa en un punt diferent aleshores tenim el tipus I_3. Si Γ_3 no talla Γ_1 apliquem (3.2.1) a Γ_3 i veiem també que Γ_3 talla la resta de la fibra un sol cop. Per tant hi ha una sola fibra amb multiplicitat 1 que talla Γ_3, diem-ne Γ_4. Si Γ_4 talla Γ_1 tenim el tipus I_4 i sinó hi ha una única component que talli Γ_4, i així successivament. Com que no poden haver-hi infinites components en algun moment s'haurà d'arribar a una component que talli Γ_1 i tindrem I_n.

Queda el cas en què $n_2 > 1$, que es fa de manera molt semblant a l'anterior, tot i que s'han d'analitzar més casos,

i que dóna lloc als tipus que falten. □

3.3 Classificació d'Ogg per a corbes de gènere 2

En aquesta secció descriurem la classificació de la fibra especial d'un model propi regular minimal d'una corba de gènere 2 donada per Ogg a [25]. En aquest article Ogg repeteix el mateix tipus d'argument combinatori que hem vist a la secció anterior, però trobant un nombre molt més gran de possibles configuracions (més d'un centenar); de fet, es va oblidar tres casos que van completar Namikawa i Ueno a [24].

Igual que en el cas de corbes el·líptiques, la tasca de trobar totes les possibles configuracions per a la fibra especial la podem dividir en 2 parts: en primer lloc dir com pot ser cada component irreductible de la fibra especial i, en segon lloc, estudiar les interseccions permeses entre aquestes components irreductibles.

La fòrmula d'adjunció aplicada a tota la fibra $\mathcal{C}_{\mathfrak{p}}$, juntament amb el fet que $\mathcal{C}_{\mathfrak{p}}^2 = 0$ ens proporciona la relació $K_{\mathcal{C}} \cdot \mathcal{C}_{\mathfrak{p}} = 2g - 2 = 2$, és a dir

$$\sum_{i=1}^{r} n_i K_{\mathcal{C}} \cdot \Gamma_i = 2g - 2 = 2 \tag{3.3.2}$$

Aquesta fòrmula imposa restriccions (també en el cas $g > 2$ com veurem a la propera secció) sobre la intersecció que pot tenir cada Γ_i amb el divisor canònic, i serà la que utilitzarem a la següent proposició per a trobar totes les possibilitats per a cada Γ_i.

Proposició 3.3.1. *Sigui C/K una corba projectiva no singular de gènere 2, $\mathcal{C}/R$ un model regular propi minimal de C/K i sigui*

$$\mathcal{C}_\mathfrak{p} = \sum_{i=1}^{r} n_i \Gamma_i$$

la seva fibra especial. Aleshores

1. *Si $\mathcal{C}_\mathfrak{p} = n_1\Gamma_1$ aleshores forçosament $n_1 = 1$ i $p_a(\Gamma_1) = 2$.*

2. *Si $r > 1$ cada Γ_i és d'algun d'aquests tipus*

$$\begin{array}{lllll}
\textit{Tipus A:} & K_\mathcal{C} \cdot \Gamma_i = 1, & \Gamma_i^2 = -1, & p_a(\Gamma_i) = 1 \\
\textit{Tipus B:} & K_\mathcal{C} \cdot \Gamma_i = 1, & \Gamma_i^2 = -3, & p_a(\Gamma_i) = 0 \\
\textit{Tipus C:} & K_\mathcal{C} \cdot \Gamma_i = 2, & \Gamma_i^2 = -2, & p_a(\Gamma_i) = 1 \\
\textit{Tipus D:} & K_\mathcal{C} \cdot \Gamma_i = 2, & \Gamma_i^2 = -4, & p_a(\Gamma_i) = 0 \\
\textit{Tipus E:} & K_\mathcal{C} \cdot \Gamma_i = 0, & \Gamma_i^2 = -2, & p_a(\Gamma_i) = 0
\end{array}$$

Demostració. (1) Si $\mathcal{C}_\mathfrak{p} = n_1\Gamma_1$, com que $K_\mathcal{C} \cdot \mathcal{C}_\mathfrak{p} = 2$ tenim que $\Gamma_1 \cdot K_\mathcal{C} = 2/n_1$; d'altra banda

$$p_a(\Gamma_1) = 1 + \frac{1}{2}\Gamma_1 \cdot \mathcal{C}_\mathfrak{p} = 1 + \frac{1}{2}\frac{2}{n_1}$$

i com que $p_a(\Gamma)$ és un enter ha de ser $n_1 = 1$. A més $p_a(\Gamma_1) = p_a(\mathcal{C}_\mathfrak{p}) = g(C) = 2$.

(2) Sigui Γ una component irreductible de $\mathcal{C}_\mathfrak{p}$, de manera que $\mathcal{C}_\mathfrak{p} = n\Gamma + D$.

En primer lloc $\Gamma^2 < 0$ ja que Γ no és múltiple racional de $\mathcal{C}_\mathfrak{p}$.

D'altra banda tenim que $\Gamma \cdot K_\mathcal{C} \geq 0$: si per contra tinguéssim $\Gamma \cdot K_\mathcal{C} < 0$ de la fòrmula d'adjunció aplicada a Γ

tindríem que

$$p_a(\Gamma) = 1 + \frac{1}{2}(\Gamma^2 + \Gamma \cdot K_{\mathcal{C}})$$

i donat que $\Gamma^2 < 0$ i $p_a(\Gamma) \geq 0$ només podria ser $\Gamma \cdot K_{\mathcal{C}} = -1$, $\Gamma^2 = -1$ i $p_a(\Gamma) = 0$, la qual cosa voldria dir que Γ és un divisor excepcional i això no pot ser ja que suposem que $\mathcal{C}$ és minimal.

Ara la fòrmula d'adjunció aplicada a $\mathcal{C}_{\mathfrak{p}}$ ens diu que:

$$\sum_{i=1}^{r} n_i K_{\mathcal{C}} \cdot \Gamma_i = 2,$$

per tant $\Gamma \cdot K_{\mathcal{C}}$ pot ser només 0, 1 o 2. A més la fòrmula

$$1 + \frac{1}{2}(\Gamma_i^2 + \Gamma_i \cdot K_{\mathcal{C}}) = p_a(\Gamma) \geq 0$$

fa que Γ^2 i $\Gamma \cdot K_{\mathcal{C}}$ tinguin la mateixa paritat i que

$$\Gamma^2 \geq -2 - \Gamma \cdot K_{\mathcal{C}}.$$

Per tant, si $K_{\mathcal{C}} \cdot \Gamma_i = 0$, Γ_i^2 ha de ser ≥ -2, negatiu i parell, per tant només pot ser -2. Si $K_{\mathcal{C}} \cdot \Gamma_i = 1$, Γ_i^2 ha de ser senar, ≥ -3 i negatiu, per tant pot ser -3 o -1. De la mateixa manera si $K_{\mathcal{C}} \cdot \Gamma_i = 2$ aleshores Γ_i^2 només pot ser -2 o -4 i per tant obtenim la taula 2. □

A la secció anterior, hem vist com per al cas de corbes el·líptiques, la fibra especial d'un model minimal podia ser, o bé una corba de gènere aritmètic 1 (tipus I_0, I_1 i II) o bé una unió de corbes de gènere aritmètic 0 que podien aparèixer amb diverses configuracions (els vuit tipus restants). En el cas de corbes de gènere 2 hi ha bastants més

casos possibles, i per a descriure'ls Ogg en el seu article utilitza la següent notació: si F és una corba, un dibuix com el de la figura 3.2 indica un divisor com qualsevol dels

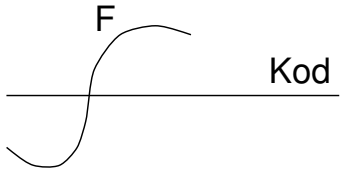


Figura 3.2:

vuit de la classificació de Kodaira-Néron que estan formats per corbes de gènere aritmètic 0, però amb una de les corbes que allà hi apareix amb multiplicitat 1 substituida per F. És a dir, indica un divisor com per exemple els de la figura 3.3.

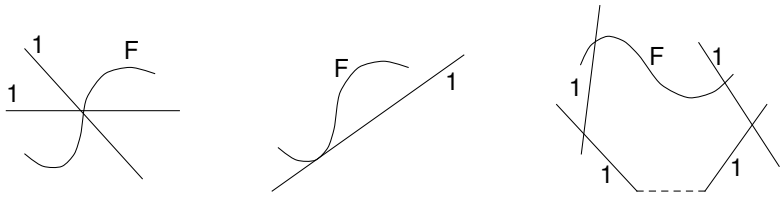


Figura 3.3:

Ogg també utilitza la notació de la figura 3.4 per indicar que la fibra de multiplicitat 3 en qüestió és completada amb alguna de les possibilitats que es veuen a la figura 3.5.

La fibra especial $\mathcal{C}_{\mathfrak{p}}$ pot ser, o bé una corba irreductible de gènere aritmètic 2, o bé una de les que apareixen a les figures 3.6 i 3.7. Aquestes figures reprodueixen la taula de

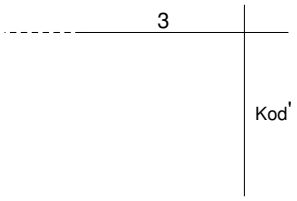


Figura 3.4:

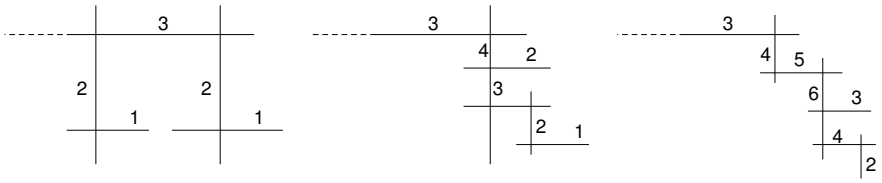


Figura 3.5:

l'article d'Ogg, tot i que els tipus $41a$, $41b$ i $41c$ són els tres casos que Ogg no va tenir en compte i que van completar Namikawa i Ueno a [24].

Per a obtenir aquesta classificació, el primer pas és observar que degut a la fòrmula

$$\sum_{i=1}^{r} n_i K_{\mathcal{C}} \cdot \Gamma_i = 2,$$

la fibra $\mathcal{C}_{\mathfrak{p}}$ conté una component de tipus C o D amb multiplicitat 1, o bé una de tipus A i una de tipus B cadascuna amb multiplicitat 1, o bé una de tipus A o B amb multiplicitat 2; la resta de components són de tipus E.

Tot seguit, cal distingir cada un d'aquests casos i aplicar en cada un d'ells raonaments semblants als de la secció anterior, mirant la possible intersecció de la component que

estem considerant amb la resta de la fibra.

Així doncs, si suposem que la fibra conté una component Γ de tipus C amb multiplicitat 1, el fet que $\Gamma^2 = -2$ fa que la intersecció de Γ amb la resta de la fibra sigui 2 i es pugui repetir el mateix argument que en el cas de les corbes el·líptiques. Per tant s'obté la configuració 1 de la figura 3.6, que en realitat agrupa diferents tipus.

Si la fibra conté una component de tipus D amb multiplicitat 1, aleshores s'obtenen fibres de tipus 2 al 11. Si conté una component A de multiplicitat 2, tenim el tipus 12. Si té dues components A cadascuna amb multiplicitat 1 s'obté el tipus 13. Una component A i una B donen lloc al tipus 14. Una component de tipus B amb multiplicitat 2 dóna lloc als tipus 15 a 33. Finalment si la fibra conté dues components de tipus B la configuració obtinguda és de la 34 a la 44.

Remarca 3.3.2. En aquest article hem emprat la notació de [25] per a fer referència als tipus de reducció, que és una notació molt compacta però també molt simplificada i on no s'hi reflecteix tota la informació del tipus de reducció. En canvi Namikawa i Ueno a [24] utilitzen una nomenclatura més precisa; no donarem tota la correspondència entre les dues notacions però sí d'aquells tipus que apareixeran al capítol 5. El tipus I_{e-0-0} és el tipus corresponent a e corbes isomorfes a $\mathbb{P}^1$ en forma de polígon, però amb un dels $\mathbb{P}^1$ substituit per una corba de tipus C (cauria dins el tipus 1 amb la notació d'Ogg). El tipus $I_{e_1-e_2-0}$ és el mateix però amb polígons de e_1 i e_2 costats respectivament i amb una corba de tipus D (seria de tipus 2 segons Ogg). $I_{e_1-e_2-e_3}$ correspon al tipus 40, on el nombre de $\mathbb{P}^1$ indicats pels

punts suspensius és $e_1 - 1$, $e_2 - 1$ i $e_3 - 1$. $I_0 - I_0 - e_0$ correspon al tipus 13 amb $e_0 - 1$ corbes de tipus $\mathbb{P}^1$ en els punts suspensius. $I_{e_1} - I_0 - e_0$ és de tipus 14 amb $e_0 - 1$ corbes de tipus $\mathbb{P}^1$ i la part de la fibra que és tipus Kodaira és un polígon de e_1 costats. $I_{e_1} - I_{e_2} - e_0$ és el tipus 39 amb $e_0 - 1$ corbes de tipus $\mathbb{P}^1$ en els punts suspensius i polígons de e_1 i e_2 costats en les terminacions tipus Kodaira.

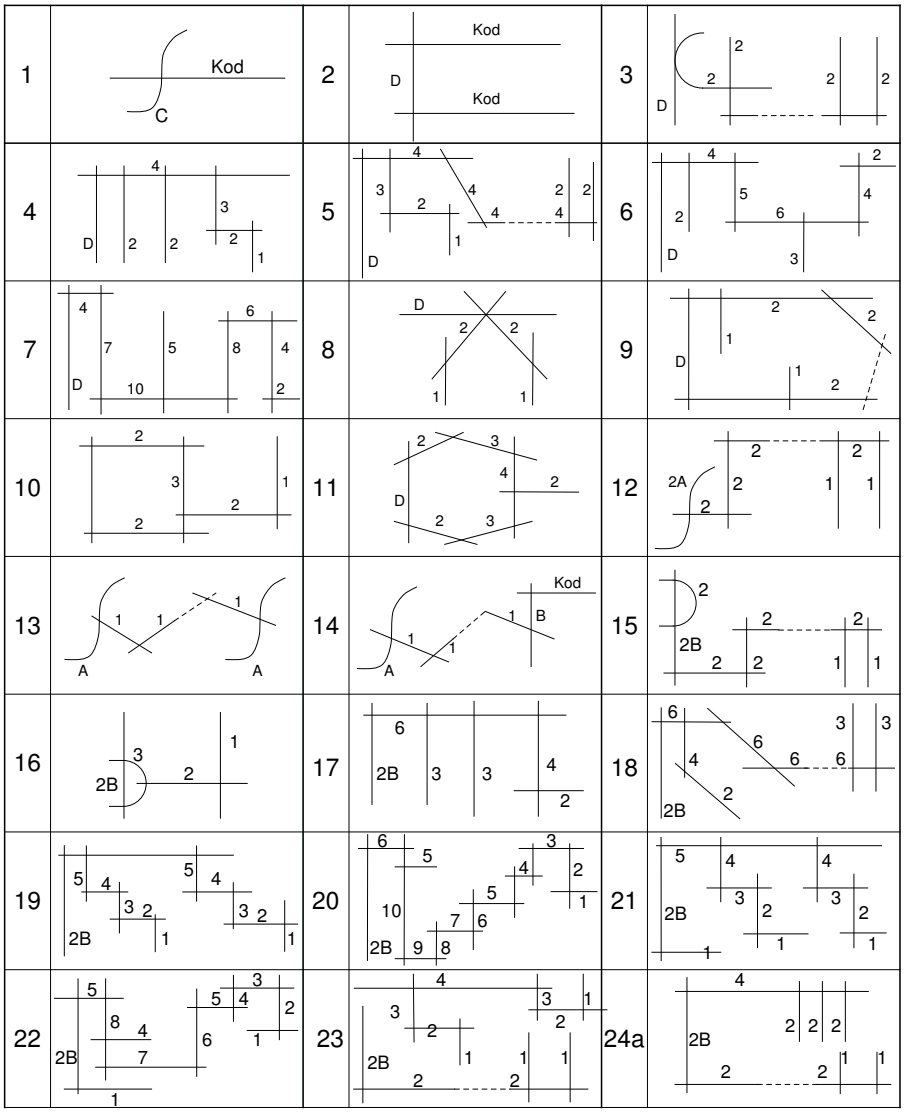


Figura 3.6: Classificació d'Ogg per a la fibra especial del model regular propi minimal d'una corba de gènere 2

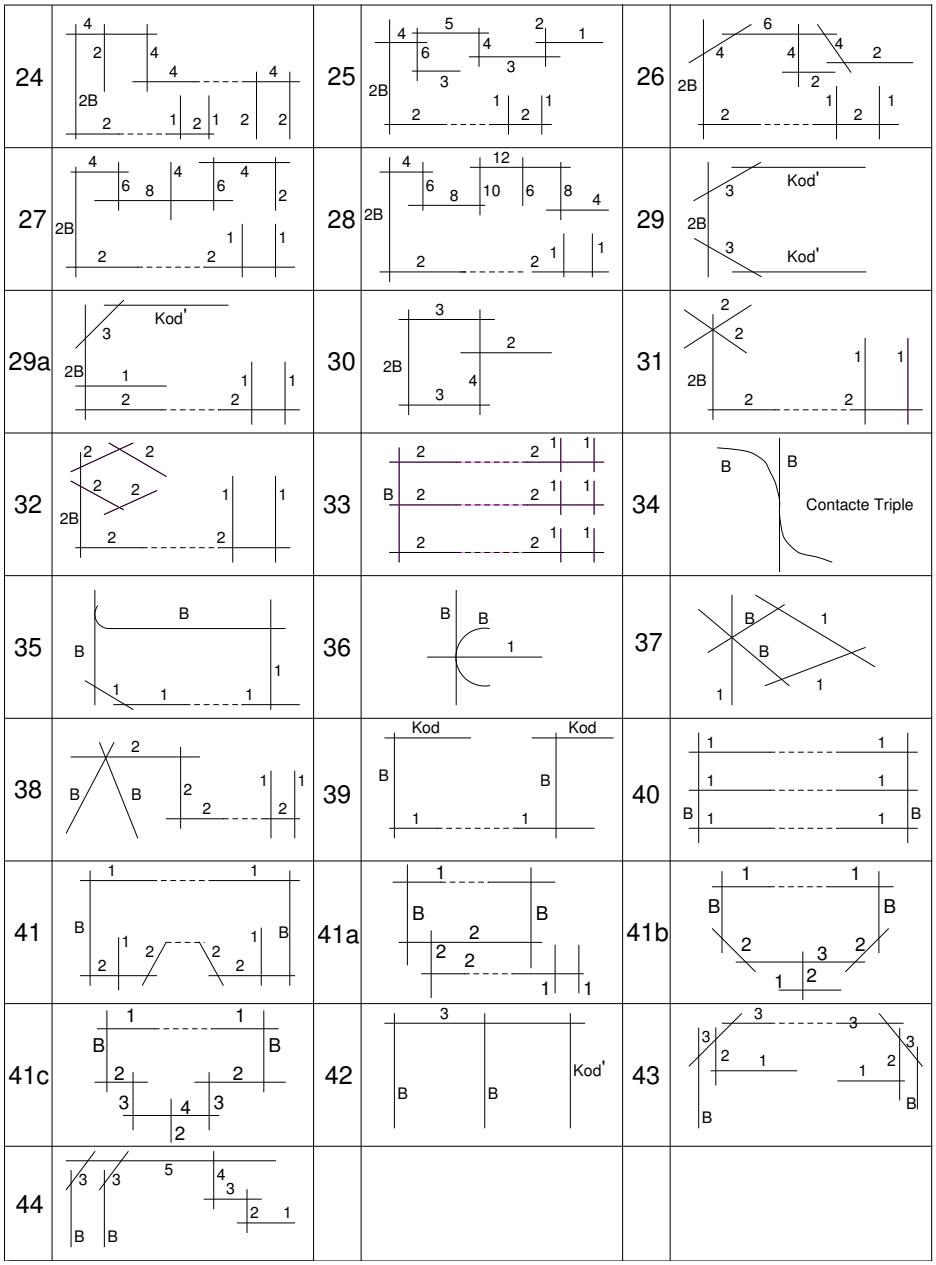


Figura 3.7: Classificació d'Ogg per a la fibra especial del model regular propi minimal d'una corba de gènere 2

3.4 Cas general: corbes de gènere arbitrari

En les dues seccions anteriors hem vist com, en el cas que la corba sigui de gènere 1 o 2, hi ha una classificació completa de la fibra especial d'un model minimal de la corba. En el cas general no podem donar una llista exhaustiva dels tipus de reducció, però sí que podem assegurar que hi ha un nombre finit de configuracions possibles (entenent que hi ha configuracions que agrupen un nombre infinit de casos, tal com passava per exemple amb la configuració I_n en la classificació de Kodaira- Néron) i podem dir com serà aquesta configuració per a una part de la fibra. Més concretament, tal com suggeria la fòrmula (3.3.2), convé distingir entre aquelles components de la fibra que tenen intersecció 0 amb el divisor canònic i aquelles que tenen intersecció diferent de 0; per a aquelles components amb intersecció 0 en sabrem donar totes les possibles configuracions.

Sigui doncs C/K una corba projectiva llisa de gènere $g > 1$ i $\mathcal{C}/R$ un model propi regular minimal de C. Com és habitual notem per

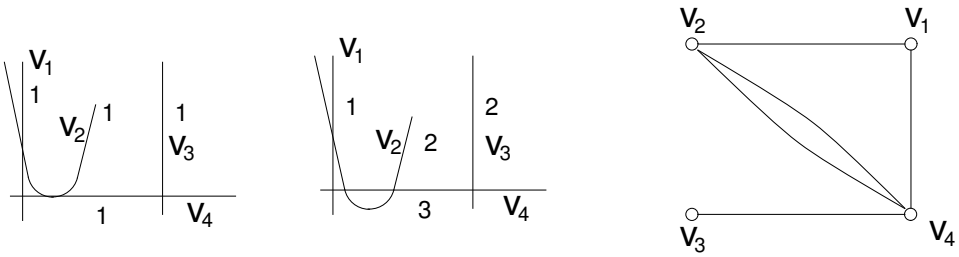
$$\mathcal{C}_{\mathfrak{p}} = \sum_{i=1}^{r} n_i \Gamma_i$$

la seva fibra especial. Un objecte que és convenient introduir per a descriure $\mathcal{C}_{\mathfrak{p}}$ (o un divisor fibral qualsevol) és el seu graf dual.

Definició 3.4.1. El graf dual de $\mathcal{C}_{\mathfrak{p}}$ que denotarem per $G(\mathcal{C}_{\mathfrak{p}})$ és el graf que té un vèrtex v_i per a cada component irreductible Γ_i i el nombre d'arestes entre v_i i v_j per a $i \neq j$

és $\Gamma_i \cdot \Gamma_j$. La definició s'extén de manera òbvia al graf dual de qualsevol divisor fibral.

Com que els vèrtexs entre arestes corresponen a les interseccions entre fibres, el graf dual d'un divisor és connex si i només si el divisor és connex. Observem també que el graf associat al divisor conté informació sobre el nombre de components i el nombre d'interseccions entre elles, però es perd la informació sobre la multiplicitat de les components i el tipus d'interseccions. Per exemple els dos divisors següents tenen com a graf dual el graf de la dreta:



Com que el model $\mathcal{C}$ és minimal, per a tota component irreductible Γ_i es compleix que $K_{\mathcal{C}} \cdot \Gamma_i \geq 0$ (pel mateix raonament que a la demostració de la proposició 3.3.1). Aleshores de la fòrmula d'adjunció i del fet que $\mathcal{C}_{\mathfrak{p}}^2 = 0$ en resulta que

$$\sum_{i=1}^{r} n_i \, K_{\mathcal{C}} \cdot \Gamma_i = 2g - 2 \tag{3.4.3}$$

amb la qual cosa el nombre de components Γ_i amb $K_{\mathcal{C}} \cdot \Gamma_i \neq 0$ està fitat per $2g - 2$.

La següent proposició ens diu com són les components Γ_i amb $K_{\mathcal{C}} \cdot \Gamma_i = 0$ i les interseccions entre elles. En particular

tota la informació sobre les interseccions entre components d'aquesta mena sí que queda reflectida en el graf dual ja que totes elles són transverses.

Proposició 3.4.2. *Si Γ_i és una component irreductible de $\mathcal{C}_\mathfrak{p}$ tal que $K_\mathcal{C} \cdot \Gamma_i = 0$, aleshores $p_a(\Gamma_i) = 0$ i $\Gamma_i^2 = -2$. A més, si Γ_j és una altra component satisfent $K_\mathcal{C} \cdot \Gamma_j = 0$ aleshores $\Gamma_i \cdot \Gamma_j \leq 1$.*

Demostració. Com que $K_\mathcal{C} \cdot \Gamma_i = 0$ la fòrmula d'adjunció és

$$0 > \Gamma_i^2 = 2p_a(\Gamma_i) - 2 \geq -2$$

i per tant només pot ser $p_a(\Gamma_i) = 0$ i $\Gamma_i^2 = -2$.

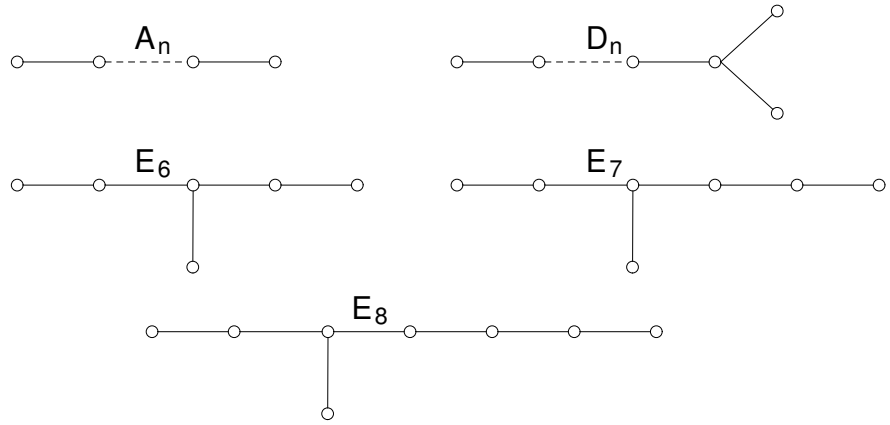
Si p i q són enters aleshores $(p\Gamma_i + q\Gamma_j)^2 < 0$. Si desenvolupem aquesta relació, fem servir que $\Gamma_i^2 = \Gamma_j^2 = -2$ i posem $t = p/q$ aleshores

$$t^2 - t(\Gamma_i \cdot \Gamma_j) + 1 < 0$$

i com que això és vàlid per a tot t, ha de ser $(\Gamma_i \cdot \Gamma_j)^2 < 4$, és a dir, $\Gamma_i \cdot \Gamma_j \leq 1$. □

Per tant si a $\mathcal{C}_\mathfrak{p}$ ens oblidem de les components que tenen intersecció no nul·la amb el divisor canònic i ens quedem només amb aquelles que hi tenen intersecció nul·la, el que ens queda és un divisor on totes les components irreductibles són corbes isomorfes a $\mathbb{P}^1_k$, amb autointersecció -2 i que quan es tallen entre elles ho fan transversalment. En el graf dual aquest divisor correspon a eliminar de $G(\mathcal{C}_\mathfrak{p})$ tots els vèrtexs associats a les components amb intersecció no nul·la amb el divisor canònic i totes les arestes que surten d'ells. El que queda llavors és un graf possiblement no connex on l'estructura de cada component connexa ve donada per la seguent proposició.

Proposició 3.4.3. *Sigui $G(\mathcal{C}_\mathfrak{p})$ el graf dual de $\mathcal{C}_\mathfrak{p}$ i sigui $G_1(\mathcal{C}_\mathfrak{p})$ el graf obtingut a partir de $G(\mathcal{C}_\mathfrak{p})$ suprimint tots els vèrtexs associats a components Γ_i amb $K_\mathcal{C} \cdot \Gamma_i \neq 0$ i totes les arestes que surten d'aquests vèrtexs. Aleshores tota component connexa de $G_1(\mathcal{C}_\mathfrak{p})$ és d'algun dels tipus següents, on la n indica el nombre de vèrtexs i $n \geq 4$ per a D_n.*



Demostració. Sigui A una component connexa qualsevol de $G_1(\mathcal{C}_\mathfrak{p})$ i suposem que hem etiquetat les components irreductibles de $\mathcal{C}_\mathfrak{p}$ de manera que $D = \Gamma_1 + \cdots + \Gamma_s$ és el divisor reduït format pels cicles associats a vèrtexs de A. Com que estem suposant $g > 1$ per (3.4.3) no pot ser que D contingui tots els divisors irreductibles de $\mathcal{C}_\mathfrak{p}$ i per tant la $\mathbb{Q}$-forma quadràtica associada a la matriu $(\Gamma_i \cdot \Gamma_j)_{i,j}$ és definida negativa en la base $\Gamma_1, \ldots, \Gamma_s$.

Per la proposició 3.4.2 sabem que les interseccions en D són transversals, per tant en $G(D)$ entre dos vèrtexs hi ha com a molt una aresta. En primer lloc, observem que $G(D)$ és un arbre, ja que si tingués un camí tancat contindria un

subgraf del tipus $\tilde{A}_n$ amb $n \geq 3$ (figura 3.8), però aleshores el divisor N amb multiplicitats en cada Γ_i les indicades en els vèrtexs de la figura compliria que $N^2 = 0$.

Ara, si $G(D)$ no té cap node, aleshores és del tipus A_n. Veiem que com a molt té un node: si en tingués més d'un, contindria un subgraf del tipus $\tilde{D}_n$, i amb el mateix raonament que abans aplicat al divisor associat a $\tilde{D}_n$ amb les multiplicitats que indica la figura veiem que això no és possible. Amb el divisor associat a $\tilde{D}_5$ veiem que de cada node com a molt hi surten 3 vèrtexs.

Amb el divisor associat a $\tilde{E}_6$ veiem que dels camins que surten del node, almenys un té longitud 1. Si hi ha dos camins que surten del node de longitud 1 alehores $G(D)$ és de tipus D_n. Si hi ha dos camins de longitud ≥ 2, el divisor associat a $\tilde{E}_7$ prova que almenys un dels camins té longitud exactament 2; si l'altre és de longitud 2 tenim E_6, si és de longitud 3 tenim E_7 i si és de longitud 4 tenim E_8. Amb $\tilde{E}_8$ veiem que el tercer camí no pot ser de longitud ≥ 5. □

Aquest darrer resultat es pot il·lustrar a partir de la classificació d'Ogg per a corbes de gènere 2: si prenem qualsevol dels tipus que allà hi apareixen, n'eliminem les corbes de tipus A, B, C o D i fem el graf dual, aleshores obtenim per a cada component connexa un dels grafs de la figura 3.4.3. Per exemple, si al tipus 32 de la figura 3.7 li treiem la component $2B$, el divisor que queda té graf dual la unió disjunta d'un A_n i un D_m. Ja hem vist que el nombre de components irreductibles Γ_i amb $K_{\mathcal{C}} \cdot \Gamma_i \neq 0$ és fitat per $2g-2$ i que les seves multiplicitats n_i també. Per finalitzar enunciem la següent proposició que ens diu que

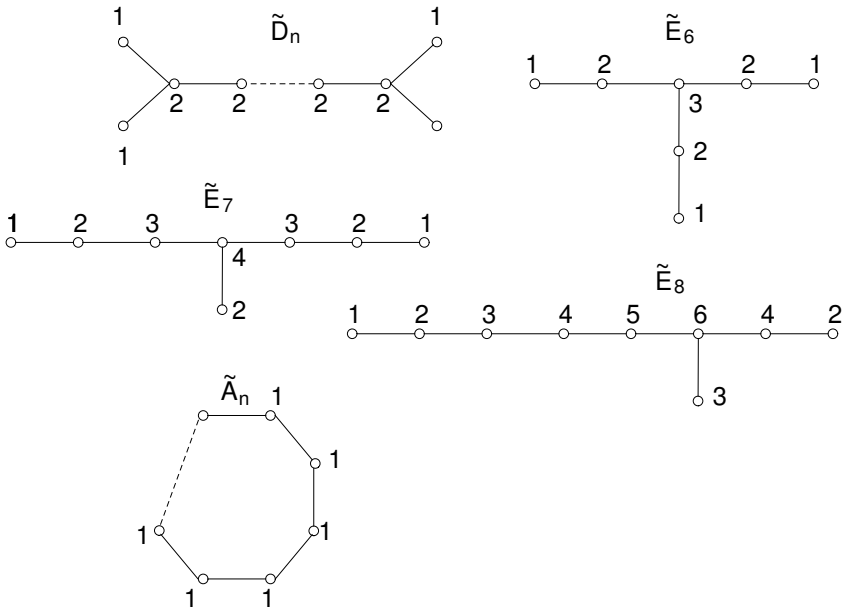


Figura 3.8:

per al graf $G_1(\mathcal{C}_\mathfrak{p})$ el nombre de components connexes i la multiplicitat dels vèrtexs també està fitada; la demostració es pot trobar a [17], proposició 1.57 del capítol 10.

Proposició 3.4.4. *Sigui $G(\mathcal{C}_\mathfrak{p})$ el graf dual de $\mathcal{C}_\mathfrak{p}$ i sigui $G_1(\mathcal{C}_\mathfrak{p})$ com en la proposició 3.4.3. Existeix una constant c que només depèn de g tal que*

1. *$n_i \leq c$ per a tot i.*
2. *El nombre de components connexes de $G_1(\mathcal{C}_\mathfrak{p})$ és menor que c.*

Capítol 4

Invariants modulars i reducció estable

Francesc Bars[1]

4.1 Introducció

Sigui R un anell de valoració discreta, K el seu cos de fraccions, $\wp$ el seu ideal maximal i $k = R/\wp$ el seu cos residual. Sigui C/K una corba llisa geomètricament connexa de gènere $g \geq 1$. Pel teorema de Deligne-Mumford, existeix una extensió finita K'/K i un model estable $\mathfrak{C}$ sobre R' de $C \times_K K'$, on R' denota la clausura integral de R en K'. Sigui $\tilde{\mathfrak{C}} = \mathfrak{C} \times_{R'} \bar{k}$ la corba estable obtinguda en considerar la fibra especial de $\mathfrak{C}$ sobre una clausura algebraica $\bar{k}$ de k.

Si C és una corba el·líptica, la corba $\tilde{\mathfrak{C}}$ està completament determinada per l'invariant j modular de C. Més concretament si $j \in R$ llavors $\tilde{\mathfrak{C}}$ és llissa, on l'invariant modular és la imatge de j dins el cos residual de R; si $j \notin R$

[1]Dep. Matemàtiques, Universitat Autònoma de Barcelona 08193 Bellaterra, Catalonia, Spain. Supported by MTM2006-11391. E-mail: francesc@mat.uab.cat

llavors $\tilde{\mathfrak{C}}$ és una corba racional amb un sol punt doble ordinari.

Si C té gènere 2, Liu en [13] dona una caracterització de $\tilde{\mathfrak{C}}$ en funció dels invariants d'Igusa.

Aquesta expossició es centra primer en definir els invariants d'Igusa, introduits in [11]. Cal comentar que aquests invariants estan fortament relacionats amb els invariants d'un polinomi de grau 6, "de la sexta", invariants coneguts ja en el s.XIX per Salmon (veieu [3, p.479]) i per A.Clebsch [5], diem aquests últims, invariants de Clebsch-Salmon. Deixem constància aquí que A. Clebsch troba com obtenir invariants per a qualsevol sistema de formes binàries (1872) i no necessàriament d'una sexta, aquests últims invariants clàssics, els anomenarem invariants de Clebsch. Després explicitarem com en gènere 2 els invariants d'Igusa classifiquen $\tilde{\mathfrak{C}}$ de forma semblant al resultat per a corbes de gènere 1 amb l'invariant j descrit anteriorment. Cal comentar que Igusa en [11] ja va donar una caracterització per tal que $\tilde{\mathfrak{C}}$ sigui llis, però és el treball de Liu [13] el qual completa totes les situacions. Comentem aquí que Mestre [21] obté diverses situacions (extenent el resultats d'Igusa) que el Liu tanca en generalitat. En [21] s'expressa el resultat usant els invariants de Clebsch-Salmon enlloc d'usar els d'Igusa.

4.2 Invariants d'Igusa (o Salmon-Clebsch) de corbes de gènere 2

Una corba C de gènere 2 sempre és una corba hiperel·líptica, és a dir té un morfisme $\phi : C \to \mathbb{P}^1$ de grau 2. A més C té $2g + 2 = 6$ punts de Weierstrass que corresponen als punts on ϕ ramifica i els punts de Weierstrass caracteritzen fortament la corba C. Suposem C està definida sobre K. Si $\text{car}(K) \neq 2$ tenim que C té un model de la forma

$$y^2 = f(x),$$

on $f(x)$ és un polinomi de grau 6, on els zeros donen la component x dels punts de Weierstrass. Si suposem que un dels punts de Weierstrass és infinit tenim una expressió amb $grau(f(x)) = 5$. Ambdues expressions són equivalents en la clausura algebraica, però no necessàreament sobre K ja que en portar un dels punts de Weierstrass a infinit podem pujar de cos. En aquesta expossició definirem primer els invariants en la clausura de K, i a posteriori observarem que són elements expressats mitjançant els coeficients del polinomi $f(x)$.

Pel cas de característica arbitrària podem considerar un model afí de la forma següent

$$Y^2 + g(X)Y = h(X)$$

amb grau de $g \leq 3$ i grau de $h \leq 6$. Els punts de Weierstrass en aquest model son les arrels múltiples i definim per a $f(x)$ en aquesta situació si $\text{car}(K) \neq 2$ mitjançant,

$$f(x) = g^2(x) + 4h(x).$$

Si pensem que posem un punt de Weierstrass a ∞ (possiblement llavors canviant de cos) podem considerar el model anomenat normal

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0.$$

Observem que el model normal, els valors de X que corresponen als 5 punts de Weierstrass que falten (a part de ∞) són els valors on l'equació en Y té arrels dobles, per tant definim $f(x)$ per a aquest model si $\mathrm{car}(K) \neq 2$ mitjançant

$$f(x) = (1 + aX + bX^2)^2 - 4X^3(c + dX + X^2).$$

En els dos models (per a $\mathrm{car}(K) \neq 2$) tenim que les sis arrels d'aquests polinomis considerats com equacions de grau 6 no homogènies són projectivament equivalents. Les arrels de f ens donen cert control sobre els punts de Weierstrass de C, i per tant cert control sobre classificació de corbes de gènere 2.

Quan $\mathrm{car}(K) = 2$ prenem un aixecament en l'anell de Witt $W(K)$ de K pels polinomis g i h, o per a $(1+aX+bX^2)$ i $X^3(c + dX + X^2)$ respectivament (que els denotarem per una tilde). Definim llavors $f(x) = \tilde{g} + 4\tilde{h}$, o bé $f(X) = \left(1 + a\tilde{X} + bX^2\right)^2 - 4X^3(c + \tilde{d}X + X^2) \in W(K)[X]$ en el cas normal.

Considerem en general a partir d'ara un polinomi d'una variable de grau 6 arbitrari,

$$f(x) = u_0x^6 + u_1x^5 + ... + u_6,$$

pensant que els zeros de $f(x)$ són la component x dels punts de Weierstrass per a certa corba de gènere 2.

Associem a $f(x)$ uns invariants que ens caracteritzin en particular les seves arrels llevat de la relació de ser projectivament equivalents.

Això és molt clàssic. Sembla que el primer en fer-ho va ser Salmon y Clebsch. Anem en el seminari a introduir com Clebsch a finals del segle XIX defineix aquests invariants. Clebsch introducirà invariants per un polinomi arbitrari de grau n:

Definició 4.2.1. *Sigui $f(x)$ un polinomi de grau n a coeficients en un cos F,*

$$a_0x^n + a_1zx^{n-1} + a_2z^2x^{n-2} + \ldots + a_nz^n,$$

(que ho escrivim com una forma binària homogènea).

Un **covariant** *de f d'ordre ℓ és un polinomi $C(a_0, \ldots, a_n, x, z)$ que satisfà donat $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\overline{F})$, amb $(x, z) = M(x', z')$, $x = \alpha x' + \beta z'$, $z = \gamma x' + \delta z'$, escrivint*

$$\sum_{i=0}^{n} a_{n-i}(\alpha x+\beta z)^i(\gamma x+\delta z)^{n-i} = \sum_{i=0}^{n} a'_{n-i}x^iz^{n-i} \text{ es compleix :}$$

$$C(a'_0, \ldots, a'_n, x', z') = det(M)^{-k}C(a_0, \ldots, a_n, x, z),$$

on $k = \frac{nr-\ell}{2}$ on r és el grau de C respecte a_i's i ℓ l'ordre de C com a polinomi en x, z.

Un **invariant** *de f és un covariant d'ordre 0.*

Clebsch [5] va definir l'operador Überschiebung, el qual li permetia trobar els invariants associats a f (almenys per

a car$(F) = 0$). Aquest operador Überschiebung ve donat per:

$$(fg)_k := \frac{(m-k)!(n-k)!}{m!n!}(\frac{\delta f}{\delta x}\frac{\delta g}{\delta z} - \frac{\delta f}{\delta z}\frac{\delta g}{\delta x})^k,$$

on f, g formes binàries $f(x,z), g(x,z)$ de graus n i m respectivament, on $(\frac{\delta f}{\delta x})^l(\frac{\delta f}{\delta z})^m$ és per definició $\frac{\delta^{l+m} f}{\delta x^l \delta z^m}$ la derivada parcial de f derivant l cops per la variable x i m per la variable z.

Lema 4.2.2 (Clebsch). *Tenim*

1. $(fg)_k$ *és un covariant simultani per les formes* f *i* g *d'ordre* $m + n - 2k$.
2. $(ff)_k$ *és un covariant per la forma* f.
3. *Tots els covariants per a* f *poden obtenir-se a partir de l'operació Überschiebung.*

La situació en que f és de grau 6 va obtenir:

covariants	ordre	grau
$i := (ff)_4$	4	2
$\Delta := (ii)_2$	4	4
$y_1 := (fi)_4$	2	3
$y_2 := (iy_1)_2$	2	5
$y_3 := (iy_2)_2$	2	7
$A := (ff)_6$	0	2
$B := (ii)_4$	0	4
$C := (i\Delta)_4$	0	6
$D := (y_3y_1)_2$	0	10
...		

Observem que aquests resultats van ser pensats en característica zero, però que fàcilment s'obtenen per a quasi tota carecterística del cos fixant el grau de f (per a grau 6, característiques 2 i 3 són patològiques).

Clebsch i pensem que també Salmon proven que A, B, C, D formen una base d'invariants de grau parell per a f de grau 6. (Sabem que Clebsch troba una base d'invariants tan grau parell com senar i una base de coinvariants). Sabem que Clebsch demostra sota una hipòtesi (hipòtesi que elimina Bolza (alumne de Klein) en la publicació de la seva dissertació [3]):

Si tenim dos polinomis de grau 6: f, f_1, i existeix $r \neq 0$ complint

$$A_1 = r^2 A,\ B_1 = r^4 B,\ C_1 = r^6 C,\ D_1 = r^{10} D$$

on $*_1$ denota els invariants de f_1, llavors f, f_1 són GL_2-equivalents i en particular les arrels són projectivament equivalents.

Salmon, Clebsch i Bolza no proven que tot A, B, C, D corresponen a un polinomi f de grau 6 tenint A, B, C i D com a invariants, resultat obtingut per Igusa.

Aquests invariants van estar estudiats per molts matemàtics buscant l'anàleg del j invariant per a corbes de gènere 2, finalment trobats per Igusa. Denotant per $\mathfrak{M}_2 \otimes \mathbb{Q}$ l'espai de moduli de corbes de gènere 2 sobre els racionals, és fàcil trobar que la seva dimensió és 3 i els 4 invariants obtinguts amb la propietat de ser projectivament equivalents ens han de donar 3 funcions algebraicament independents que ens dona el grau de trascendència del cos $\mathbb{Q}(\mathfrak{M}_2 \otimes \mathbb{Q})$. Això sembla clàssicament conegut. No obstant si volem

inmersionar $\mathfrak{M}_2 \otimes \mathbb{Q}$ en un espai afí controlant-hi tots els punts patològics, és un problema de gran interés que va ser tancat per Igusa (1960). Un resultat intermedi, d'aquest problema tancat per Igusa, el trobem en la disertació de E. Hecke "Höhere Modulfunktionen und ihre Anwendung auf die Zahlentheorie"(1912). Hecke va construir 6 invariants i demostra que $\mathfrak{M}_2 \otimes \mathbb{Q}$ és birracional amb una varietat usant aquests 6 invariants, però que no és a tot arreu biregular, la varietat de Hecke no és normal. És Igusa que usarà 8 funcions cap d'elles irredundants per a obtenir l'immersió buscada, observem que l'espai tangent al punt singular de $\mathfrak{M}_2 \otimes \mathbb{Q}$ té dimensió 8. Aquests arguments són també correctes canviant el cos $\mathbb{Q}$ per un cos de característica no 2, i per car $= 2$ Igusa obté el resultat anàleg necessitant 10 funcions, (l'espai tangent en el singular locus té dimensió 10 per car $= 2$).

Igusa (1960) troba l'anàleg del j invariant per a corbes de gènere 2. Anem a definir-ne els seus invariants que són certes eleccions dels invariants ja coneguts per Clebsch.

Definició 4.2.3. *Sigui* $f = u_0x^n + \ldots + u_n \in F[u_0, \ldots, u_n][x]$ *amb* F *cos. Un invariant* **injectiu** *de tipus* $(\ell, d) \in \mathbb{Z}^2$ *de* f *és un polinomi homogeni* $H \in F[u_0, \ldots, u_n]$ *de grau* d *que verifica la següent propietat:*

1. *Per a tot* $a, b \in \overline{F}$, $a \neq 0$ *si un escriu,*

$$\sum_{0 \leq j \leq n} u_j(ax+b)^{n-j} = \sum_{0 \leq j \leq n} u'_j x^{n-j} \in F^{alg}[u_0, \ldots, u_n][x],$$

llavors es té $H(u'_0, \ldots, u'_n) = a^\ell H(u_0, \ldots, u_n)$.

Diem que H *és un invariant* **projectiu** *de grau* d *de* f *si*

és un invariant injectiu del tipus $(dn/2, d)$ *i satisfà:*

$$H(u_0, \ldots, u_n) = (-1)^{dn/2} H(u_n, \ldots, u_0).$$

Observem aquí que els invariants projectius són els invariants d'ordre parell de'n Clebsch.

Remarca 4.2.4. *Si* $\mathrm{car}(F) = 2$*, recordeu que* f *és un polinomi a coeficients en* $W(F)$*, l'anell de Witt de* F*, i per tant busquem els seus invariants en el cos de fraccions de* $W(F)$*.*

Per a característica no 2, recordem que si ∞ és racional obtenim un model per a la corba hiperel·líptica $y^2 = f(x)$ amb $grau(f) = 5$, però si ∞ no ho és per a obtenir un model amb $grau(f) = 5$ pugem el cos de definició. Això pot dependre fortament del punt ∞ i de l'aritmètica. Els invariants injectius tenen en compte l'elecció d'aquest punt. Els invariants projectius no el tenen en compte.

Comencem pels invariants injectius (veieu la seva aplicació en el Cap. 6):

Exemple 4.2.5. *Per a tot* $2 \leq i \leq n$*, considerem* $\mathcal{P} := u_0 x^n + u_1 x^{n-1} + u_2 x^{n-2} + \ldots + u_{n-1} x + u_n$*. Definim*

$$A'_i := i(nu_0)^{i-1} \frac{\mathcal{P}^{(n-i)}}{(n-i)!} \left(-\frac{u_1}{nu_0} \right) \in \mathbb{Z}[u_0, \ldots, u_n]$$

on $\mathcal{P}^{(j)}$ *denota la derivada* j*-èssima de* $\mathcal{P}$*.*

A'_i *és un invariant afí del tipus* $(i(n-1), i)$*.*

El primer coeficient u_0 *és un invariant afí de tipus* $(n, 1)$*.*

Prenem $n = 6$, posem:

$$\begin{cases} A_2 := A_2' = -5u_1^2 + 12u_0u_2 \\ A_3 := \frac{A_3'}{4} = 5u_1^3 + 9u_0(-2u_2u_1 + 3u_0u_3) \\ A_4 := \frac{A_4'}{6} = -5u_1^4 + 24u_0(u_2u_1^2 - 3u_3u_0u_1 + 6u_4u_0^2) \\ A_5 := \frac{A_5'}{20} = u_1^5 + 3u_0(-2u_2u_1^3 + 9u_0u_3u_1^2 - 36u_0^2u_4u_1 + 108u_0^3u_5) \\ B_2 := \frac{A_2^2+5A_4}{72u_0^2} \\ B_6 := \frac{8A_3^4-5A_4^3+A_2^3A_6'+5A_3^2A_6'+6A_2^2A_4^2-15A_2A_3^2A_4}{5832u_0^6} \end{cases}$$

Tenim A_i invariants afins de tipus $(5i, i)$, i B_{2j} del tipus $(8j, 2j)$. Es coneix per a *car* $\neq 2, 3$ que tot invariant afí és un element de:

$$F[u_0, u_0^{-1}, A_2, \ldots, A_5, A_6'].$$

Anem ara a introduir invariants projectius, que necessàriament seran combinacions dels A, B, C i D.

Lema 4.2.6 (Igusa). *Siguin $\alpha_1, \ldots, \alpha_n$ les arrels de la sexta $u_0x^6 + \ldots + u_6$. Llavors una expressió de la forma*

$$H(u_0, \ldots, u_n) := u_0^m \sum (\alpha_i - \alpha_j)(\alpha_k - \alpha_l) \ldots$$

on cada α_i apareix m cops en cada producte i que és simètric en $\alpha_1, \ldots, \alpha_6$ defineix invariants enters homogenis de grau m, on enter significa que $H \in \mathbb{Z}[u_0, \ldots, u_n]$.

En particular tenim els següents invariants enters, on denotem per (ij) a l'expressió $(\alpha_i - \alpha_j)$:

$$A' := u_0^2 \sum (12)^2(34)^2(56)^2 = -120A$$

$$B' := u_0^4 \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 = -720A^2 + 6750B$$

$$C' := u_0^6 \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2 =$$
$$8640A^3 - 108000AB + 202500C,$$
$$D' := u_0^{10} \prod (ij)^2 = -62208A^2 + 972000A^3B + 1620000A^2C -$$
$$3037500AB^2 - 6075000BC - 4556250D.$$

Anem tot seguit a definir els invariants d'Igusa $J_{2i} \in \mathbb{Z}[\frac{1}{2}, u_0, \ldots, u_6]$ amb $grau(J_{2i}) = 2i$ amb $i = 1, \ldots, 5$. Seran polinomis en A, B, C i D, amb la propietat que dos polinomis de grau 6 sense arrels múltiples són projectivament equivalents si i només si els invariants d'Igusa associats satisfant que $J_{2i} \to r^{2i} J_{2i}$ per a $i = 1, 2, 3, 5$ per a cert $r \neq 0$.

Podem considerar primer que una de les arrels és ∞ llavors obtenim un polinomi de grau 5, i podem pendre per a qualsevol característica el polinomi f associat a la forma normal,

$$f = (1 + aX + bX^2)^2 - 4X^3(c + dX + X^2).$$

Els zeros d'aquest polinomi són la component x en el 6 punts de Weierstrass associats a la corba de gènere 2 $XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$.

Calculem ara A' com a polinomi en a, b, c i d. Es té que el màxim comú divisor dels coeficients és 2^3. Definim

$$J_2 := \frac{1}{2^3} A'$$

com el primer invariant d'Igusa.

Remarca 4.2.7. *Si* $\mathrm{car}(K) = 2$ *definirem aquest resultat i tots els invariants* J_{2*} *que definirem via mòdul* $2W(K)$ *pels seus coeficients.*

Considerem ara el discriminant del polinomi. El màxim comú divisor dels coeficients com a polinomi en a, b, c i d és igual a 2^{12}. Definim

$$J_{10} := 2^{-12}D,$$

on D denota el discriminant de f.

Anem a definir 3 invariants més d'Igusa.

Sigui m un enter i considerem $mJ_2^2 - B'$ d'ordre 4. Llavors el maxim comú divisor dels coeficients de $mJ_2^2 - B'$ com un polinomi en a, b, c i d és maximal amb valor $2^5 3 = 96$ quan $m \equiv 4 (mòdul\ 96)$. Definim

$$J_4 := \frac{1}{96}(4J_2^2 - B').$$

Considerem ara $mJ_2^3 + nJ_2J_4 - C'$ com un polinomi en a, b, c i d, amb m, n enters. S'obté que el valor màximal pel màxim comú divisor dels coeficients de $mJ_2^3 + nJ_2J_4 - C'$ s'obté quan $m \equiv 8$ i $n \equiv -160 (mòdul\ 576)$ amb valor igual a $576 = 2^6 3^2$. Definim

$$J_6 := \frac{1}{576}(8J_2^3 - 160J_2J_4 - C').$$

Es comprova que $J_2J_6 - J_4^2$ és zero mòdul 2, i el màxim comú divisor d'aquesta expressió en a, b, c i d és 2^2. Definim

$$J_8 := \frac{1}{4}(J_2J_6 - J_4^2).$$

4.3 Altres expressions dels invariants d'Igusa per a $\mathrm{car}(K) \neq 2$.

Potser que el nostre model sobre K no prén la forma normal, i tenim una altra expressió. Anem a expressar els

invariants d'Igusa en les possibles expressions per a característica diferent de 2.

Si prenem una sexta amb característica diferent de 2 de la forma

$$f(X) = v_0X^5 - v_1X^4 + v_2X^3 - v_3X^2 + v_4X - v_5$$

com a model per a la corba hiperel·líptica $y^2 = f(x)$, ∞ és un punt de Weierstrass, obtenim que els anteriors invariants d'Igusa s'escriuen en funció dels v_i's de la forma següent:

$$J_2 = 5v_0v_1 - 2v_1v_3 + 2^{-2}3v_2^2$$

$$J_4 = -2^3[5^2v_0^2v_3v_5 - 15v_0^2v_4^2 - 15v_0v_1v_2v_5 + 7v_0v_1v_3v_4 + 2^{-1}v_0v_2^2v_4 -$$
$$v_0v_2v_3^2 + 2^3v_1^3v_5 - v_1^2v_2v_4 - v_1^2v_3^2 + v_1v_2^2v_3 - 2^{-4}3v_2^4]$$

$$J_6 = -2^{-4}[2^{-1}5^3v_0^3v_2v_5^2 - 5^2v_0^3v_3v_4v_5 + 5v_0^3v_4^3 -$$
$$5^3v_0^2v_1^2v_5^2 - 10v_0^2v_1v_2v_4v_5 + 10v_0^2v_1v_3^2v_5 - v_0^2v_1v_3v_4^2 -$$
$$\frac{5}{4}v_0^2v_2^2v_3v_5 - \frac{11}{4}v_0^2v_2^2v_4^2 + \frac{7}{2}v_0^2v_2v_3^2v_4 - v_0^2v_3^4 + 6v_0v_1^3v_4v_5 - 3v_0v_1^2v_2v_3v_5 +$$
$$\frac{7}{2}v_0v_1^2v_2v_4^2 - 2v_0v_1^2v_3^2v_4 + \frac{3}{4}v_0v_1v_2^3v_5 -$$
$$\frac{7}{4}v_0v_1v_2^2v_3v_4 + v_0v_1v_2v_3^3 + \frac{7}{2^4}v_0v_2^4v_4 - 2^{-2}v_0v_2^3v_3^2 - v_1^4v_4^2 +$$
$$v_1^3v_2v_3v_4 - 2^{-3}v_1^2v_2^3v_4 - 2^{-2}v_1^2v_2^2v_3^2 + 2^{-3}v_1v_2^4v_3 - 2^{-6}v_2^6]$$

Per a J_8 substituiu $\frac{1}{4}(J_1J_6 - J_4^2)$, i $J_{10} = 2^{-12}a_1^2 disc(P)$ amb $disc(P)$ és el discriminant del polinomi f.

Si ∞ no és un punt de Weierstrass en el model sobre K, obtenim un model $y^2 = f(x)$ amb $f(x)$ un polinomi de grau 6

$$f(x) = a_0x^6 + a_1x^5 + \ldots + a_6 \in K[x].$$

Fem llavors a $f(x)$ una transformació homogràfica que porti una arrel de $f(x)$ a infinit i de la fórmula anterior per a un polinomi de grau 5 obtenim:

$$J_2 = 2^{-2}(-120a_0a_6 + 20a_1a_5 - 8a_2a_4 + 3a_3^3),$$

$$J_4 = 2^{-7}(240(a_0a_3a_4a_5 + a_1a_2a_3a_6) - 400(a_0a_2a_5^2 + a_1^2a_4a_6) -$$
$$64(a_0a_4^3 + a_2^3a_6) + 16(a_1a_3a_4^2 + a_2^2a_3a_5) - 672a_0a_3^2a_6 +$$
$$240a_1^2a_5^2 - 112a_1a_2a_4a_5 - 8a_1a_3^2a_5$$
$$+16a_2^2a_4^2 - 16a_2a_3^2a_4 + 3a_3^4 + 2640a_0^2a_6^2 - 880a_0a_1a_5a_6 + 1312a_0a_2a_4a_6),$$

$$J_6 = 2^{-10}(1600(a_0^2a_4^2a_5^2 + a_1^2a_2^2a_6^2) +$$
$$1600(a_0a_1a_2a_5^3 + a_1^3a_4a_5a_6) + 640(a_0a_1a_3a_4a_5^2 + a_1^2a_2a_3a_5a_6) -$$
$$4000(a_0^2a_3a_5^3 + a_1^3a_3a_6^2) - 384(a_0a_1a_4^3a_5 + a_1a_2^3a_5a_6)$$
$$-640(a_0a_2^2a_4a_5^2 + a_1^2a_2a_4^2a_6) + 80(a_0a_2a_3^2a_5^2 + a_1^2a_3^2a_4a_6)$$
$$+192(a_0a_2a_3a_4^2a_5 + a_1a_2^2a_3a_4a_6) - 48(a_0a_3^3a_4a_5 + a_1a_2a_3^3a_6)$$
$$-224(a_1^2a_3a_4^2a_5 + a_1a_2^2a_3a_5^2) + 64(a_1^2a_4^4 + a_2^4a_5^2)$$
$$-64(a_1a_2a_3a_4^3 + a_2^3a_3a_4a_5) + 16(a_1a_3^3a_4^2 + a_2^2a_3^3a_5)$$
$$-4096(a_0^2a_4^3a_6 + a_0a_2^3a_6^2) + 6400(a_0^2a_2a_5^2a_6 + a_0a_1^2a_4a_6^2)$$

$$+10560(a_0^2a_3a_4a_5a_6+a_0a_1a_2a_3a_6^2)+2624(a_0a_1a_3a_4^2a_6+a_0a_2^2a_3a_5a_6)$$
$$-4432a_0a_1a_3^2a_5a_6-8a_2a_3^4a_4+a_3^6-320a_1^3a_5^3+64a_1^2a_2a_4a_5^2+176a_1^2a_3^2a_5^2$$
$$+128a_1a_2^2a_4^2a_5+112a_1a_2a_3^2a_4a_5-28a_1a_3^4a_5+16a_2^2a_3^2a_4^2+5120a_0^3a_6^3-$$
$$2544a_0^2a_3^2a_6^2+312a_0a_3^4a_6-14336a_0^2a_2a_4a_6^2+$$
$$1024a_0a_2^2a_4^2a_6-2560a_0^2a_1a_5a_6^2-2240a_0a_1^2a_5^2a_6$$
$$-6528a_0a_1a_2a_4a_5a_6-1568a_0a_2a_3^2a_4a_6),$$

i $J_{10}=2^{-12}disc(P)$.

Lema 4.3.1 (Igusa, Salmon, Clebsch, Bolza,...). *Suposem que $F(X):=F(X_1,X_2,X_3,X_4,X_5)$ un element homogeni de $k[X_1,\ldots,X_5]$. Llavors*

$$F(J_2,J_4,J_6,J_8,J_{10})=0$$

si i només si $F(X)$ és un múltiple de $X_1X_3-X_2^2-4X_4$.

Lema 4.3.2 (Igusa). *Si $J_2',\ldots,J_{10}'$ son invariants d'Igusa de la corba C de gènere 2 associats a una altra equació hiperel·líptica, llavors existeix $a\in F\setminus\{0\}$ tal que $J_{2i}'=a^{2i}J_{2i}$. Inversament, si dos corbes C,C' de gènere 2, els invariants d'Igusa verifiquen l'anterior igualtat llavors són isomorfes en F^{alg}, la clausura algebraica.*

Recordem que $\mathfrak{M}_2\times K$ denota l'espai de moduli de corbes de gènere 2 sobre K. Si $\mathrm{car}(K)\neq 2$ Igusa va demostrar que s'immersiona en espai afí dimensió 8 usant les funcions:

$$J_2^5J_{10}^{-1},\ J_4^5J_{10}^{-2},\ J_6^5J_{10}^{-3}$$
$$J_2^3J_4J_{10}^{-1},\ J_2J_4^2J_{10}^{-1},\ J_2^2J_6J_{10}^{-1},\ J_4J_6J_{10}^{-1},\ J_2J_6^3J_{10}^{-2},$$

i si $\mathrm{car}(K)=2$ es necessiten 10 funcions. Les funcions $J_2^5J_{10}^{-1}$, $J_4^5J_{10}^{-2}$, $J_6^5J_{10}^{-3}$ són transcendents i generen el cos de funcions de l'espai de moduli llevat d'una extensió finita.

Qüestió 4.3.3. *Considerem $\mathfrak{M}_g$ l'espai de moduli de les corbes de gènere g. Hi sabem calcular la seva dimensió. Podem trobar-hi uns invariants que almenys ens calculin el cos de funcions de $\mathfrak{M}_g$ per a gènere 3?*

Agraeixo aquí una conversa amb C. Ritzenthaler sobre aquesta qüestió, la qual aporta les següents remarques en aquest manuscrit.

Remarca 4.3.4. *El que si que sembla factible contestar a la següent situació. Considerem $\mathfrak{M}_g^{hyper}$ l'espai de moduli de les corbes de gènere g que són hiperel·líptiques. Llavors tenim un model de la forma $y^2 = f(x)$ amb f un polinomi de grau $2g+2$ o $2g+1$. A aquest polinomi $f(x)$, que pensarem de grau $2g+2$ i que el pensarem com una forma binària hi tenim associats els invariants de Clebsch que obtenim mitjançant l'operació Überschiebung (són els invariants de formes binàries de grau $2g+2$). Per a gènere $g=3$, també es té calculat aquests generadors per als invariants d'una forma binària de grau 8, resultats obtinguts per Shioda [32]. Anem aquí a resumir-ho:*
escrivim $f(x,z)$ una forma binària de grau 8 per un cos F de característica zero o suficientment gran (igual que hem fet per a gènere 2 podem pensar f un polinomi de grau 8), definim mitjançant Überschiebung els següents covariants:

$$\underline{H} := (ff)_8,\ \underline{g} := (ff)_4,\ \underline{k} := (ff)_6,\ \underline{m} := (f\underline{k})_4,\ \underline{n} := (f\underline{h})_4,$$
$$\underline{p} := (\underline{gk})_4,\ \underline{q} := (\underline{gh})_4,\ \underline{h} := (\underline{kk})_2.$$

Considerem ara els invariants de f:

$$\underline{I}_2 := (ff)_8,\ \underline{I}_3 := (f\underline{g})_8,\ \underline{I}_4 := (\underline{kk})_4,\ \underline{I}_5 := (\underline{mk})_4,\ \underline{I}_6 := (\underline{kh})_4,$$
$$\underline{I}_7 := (\underline{mh})_4,\ \underline{I}_8 := (\underline{ph})_4,\ \underline{I}_9 := (\underline{nh})_4,\ \underline{I}_{10} := (\underline{qh})_4.$$

Teorema 4.3.5 (Shioda). *Siguin C_1, C_2 dos corbes hiperel.líptiques sobre K de gènere 3, amb equacions $y^2 = f_i(x)$ per $i = 1, 2$. Denotem per $\underline{I}_k^{(i)}$ l'invariant $\underline{I}_k$ associat a la corba C_i. Llavors s'obté: les dos corbes són isomorfes si i sol si existeix $r \in \overline{F}$ complint $\underline{I}_k^{(1)} = r^k \underline{I}_k^{(2)}$ per a $k = 2, 3, \ldots, 10$.*

Remarca 4.3.6. *En quan a la pregunta original per a $\mathfrak{M}_3$, restringim-nos a $\mathfrak{M}_3^{no-hyper}$ l'espai de moduli de les corbes de gènere 3 no hiperel.líptiques. Totes elles tenen una expressió d'una corba plana projectiva de grau 4. Aquest fet permet calcular-ne invariants, veieu Shioda [32]. En [32] dona certes condicions com han de ser aquesta algebra d'invariants per a característica zero en forma de conjectura. La primera conjectura en quan al sistema de paràmetres va ser demostrada per Dixmier [9] (en característica zero). Després Ohno [28] descriu un conjunt complert d'invariants (útil possiblement per característica zero o* $\mathrm{car}(F) > 7$*). Els invariants de Ohno estàn implementals en MAGMA per Kohel, consulteu la seva pàgina web. Si* $\mathrm{car}(F) = 2$ *Müller i Ritzenthaler [22] descriuen un conjunt complet d'invariants.*

4.4 Teorema de Liu de classificació per a $\tilde{\mathfrak{C}}$

Sigui d'ara i en endavant C una corba projectiva llissa sobre K geomètricament connexa i de gènere 2, K cos complet de valoració discreta. Siguin J_{2i} els invariants d'Igusa associats

a C associats a una equació

$$y^2 + Q(x)y = P(x),$$

(recordeu que $Q = 0$ si $\text{car}(K) \neq 2$). Sabem que té reducció estable sobre una extensió finita de K, diem-li M i per R_M el seu anell d'enters, ζ_M l'ideal maximal. Tenim $\mathfrak{C} \to Spec(R_M)$ model estable, i la seva fibra especial $\mathfrak{C} \times R_M/\zeta_M$ té les propietats provinents de esser reducció de model estable; aquestes es mantenen en la clausura algebraica de R_M/ζ_M i denotem aquesta fibra especial per a $\mathfrak{C}$ en la clausura algebraica de k (també de R_M/ζ_M) mitjançant $\tilde{\mathfrak{C}}$. Pel fet de provenir d'un model estable tenim

$$dim_{k^{alg}}(H^1(\tilde{\mathfrak{C}}, \mathcal{O}_{\tilde{\mathfrak{C}}})) = 2,$$

d'aquí s'obté set possibilitats per a $\tilde{\mathfrak{C}}$:

1. $\tilde{\mathfrak{C}}$ és llisa i per tant de gènere 2,
2. $\tilde{\mathfrak{C}}$ és no llissa e irreductible amb un sol punt doble, (la normalització de $\tilde{\mathfrak{C}}$ és una corba el·líptica).
3. $\tilde{\mathfrak{C}}$ és irreductible amb dos punts dobles.
4. $\tilde{\mathfrak{C}}$ està format per dos rectes projectives que es tallen en tres punts,
5. $\tilde{\mathfrak{C}}$ és la unió de dos components irreductibles que es tallen en un punt,
   (a) les components son llises,
   (b) un sola de les components és llisa,
   (c) les dos components de $\tilde{\mathfrak{C}}$ són singulars.

Recordem que una corba el·líptica Y (si $\mathrm{car}(k) \neq 2$) té una expressió:

$$y^2 = x^4 + ax^2 + bx + c$$

definim

$$I_4 := J_2^2 - 2^3 \cdot 3J_4,\ I_{12} := -2^3 J_4^3 + 3^2 J_2 J_4 J_6 - 3^3 J_6^2 - J_2^2 J_8,$$

observem que aplicant aquestes fórmules als invariants d'Igusa per aquest polinomi de grau 4 un obté

$$I_4 = 2^{-4} c_4(Y),\ I_{12} = 2^{-12}\Delta(Y)$$

on c_4, Δ són les formes automorfes clàssiques associades a Y, i per tant obtenim

$$j(Y) = I_4^3 I_{12}^{-1}.$$

Aquests invariants permetran estudiar els casos en que la reducció apareix una corba amb gèrere 1.

Definim $I_2 := 12^{-1} J_2$, $I_6 := J_6$, $I_8 := J_8$.

Teorema 4.4.1 (Liu).

1. *(Igusa)* $\tilde{\mathfrak{C}}$ *és llissa si i només si* $J_{2i}^5 J_{10}^{-i} \in R$ *per a tot* $i \leq 5$,
2. $\tilde{\mathfrak{C}}$ *és irreductible amb un sol punt doble, (la normalització de* $\tilde{\mathfrak{C}}$ *és una corba el·líptica)*$\Leftrightarrow$ $J_{2i}^6 I_{12}^{-i} \in R$ *per a tot* $i \leq 5$ *i* $\overline{J_{10}^6 I_{12}^{-5}} \in \wp$. *L'invariant* j *de la corba eliptica és* $j = \overline{(I_4^3 I_{12}^{-1})}$.
3. $\tilde{\mathfrak{C}}$ *és irreductible amb dos punts dobles* $\Leftrightarrow$ $J_{2i}^2 I_4^{-i} \in R$ *per a tot* $i \leq 5$, $J_{10}^2 I_4^{-5} \in \wp$, $I_{12} I_4^{-3} \in \wp$ *i és té que* $J_4 I_4^{-1}$ *o bé* $J_6^2 I_4^{-3}$ *invertible en* R.

4. $\tilde{\mathfrak{C}}$ *està format per dos rectes projectives que es tallen en tres punts* $\Leftrightarrow J_{2i}^2 I_4^{-i} \in \wp$ *per a tot* $2 \leq i \leq 5$.

5. $\tilde{\mathfrak{C}}$ *és la unió de dos components irreductibles que es tallen en un punt si i sol si*

$$I_4^\epsilon I_{2\epsilon}^{-2} \in \wp,\ J_{10}^\epsilon I_{2\epsilon}^{-5} \in \wp,\ I_{12}^\epsilon I_{2\epsilon}^{-6} \in \wp. \tag{4.4.1}$$

on $\epsilon = 1$ *si* $\mathrm{car}(k) \neq 2, 3$ *(sino* ϵ *és 4 ó 3 respectivament).*

(a) *les components són llisses,* $\Leftrightarrow$ *és compleix (4.4.1) i a més* $I_4^{3\epsilon} J_{10}^{-\epsilon} I_{2\epsilon}^{-1} \in R$, $I_{12}^\epsilon J_{10}^{-\epsilon} I_{2\epsilon}^{-1} \in R$. *Siguin* j_1, j_2 *els invariants modulars de les dues components, es té:*

$$\begin{cases} (j_1 j_2)^\epsilon = \overline{(I_4^{3\epsilon} J_{10}^{-\epsilon} I_{2\epsilon}^{-1})}, \\ (j_1 + j_2)^\epsilon = 2^6 \cdot 3^3 + \overline{(I_{12}^\epsilon J_{10}^{-\epsilon} I_{2\epsilon}^{-1})} \end{cases}$$

(b) *un sola de les components és llissa,* $1 \Leftrightarrow$ *es compleix (4.4.1) i a més* $I_4^3 I_{12}^{-1} \in R$, $J_{10}^\epsilon I_{2\epsilon} I_{12}^{-\epsilon} \in \wp$. *L'invariant modular de la component llissa és* $j = \overline{(I_4^3 I_{12}^{-1})}$.

5.3 les dos components de $\tilde{\mathfrak{C}}$ *són singulars* $\Leftrightarrow$ *es compleix (4.4.1) i a més* $I_{12} I_4^{-3} \in \wp$ *i* $J_{10}^\epsilon I_{2\epsilon} I_4^{-3\epsilon} \in \wp$.

Esboç de la prova. Sense pèrdua de generalitat podem pendre R estrictament henselià i k algebraicament tancat. Suposem que $\mathrm{car}(K) \neq 2, 3$, (en el cas $\mathrm{car}(K) = 3$ pocs canvis són necessaris). Com $g(C) = 2$ és hiperel·líptica, tenim

$$C \to \mathbb{P}^1_K$$

definint una involució hiperel·líptica σ. Per Deligne-Mumford σ, automorfisme en C, s'esten a una involució en el model

$\mathfrak{C}$. Sigui

$$f : \mathfrak{C} \to \mathfrak{Z} := \mathfrak{C}/ < \sigma > .$$

Tenim $\mathfrak{Z}$ és normal amb fibra especial reduïda i conexa per ser-ho la de $\mathfrak{C}$ i fibra genèrica $\mathfrak{Z}_\eta \cong \mathbb{P}^1_K$. Un té llavors que les components de la fibra especial $\mathfrak{Z}_s$ de $\mathfrak{Z}$ són isomorfs a $\mathbb{P}^1_k$, i es pot comprovar que $\mathfrak{C}_s/ < \sigma > \cong \mathfrak{Z}_s$ i f no ramifica en cap punt genèric de $\tilde{\mathfrak{C}}$.

1. Suposem que $\mathfrak{Z}_s$ és irreduible. Llavors és demostra que $\mathfrak{Z} \cong \mathbb{P}^1_R$. Podem triar un $Spec(R)$-punt Γ on f ramifica sobre el punt Γ_η i si $\tilde{\mathfrak{C}}$ no és llissa Γ_s sigui un punt doble de $\tilde{\mathfrak{C}}$. Llavors escrivint l'obert $U = \mathfrak{Z} \setminus \Gamma$, $U = Spec(R[x])$ tenim que $f^{-1}(U)$ és un revestiment de grau 2 de Galois, amb $f^{-1}(U) = Spec(R[x, y])$ complint

   $$y^2 = P(x),\ P(x) \in R[x],$$

   on com f_η és ramificat en ∞, tenim $deg(P) = 5$.

   Suposem primer que $\tilde{\mathfrak{C}}$ és llissa, tenim $\overline{P(x)}$ és un polinomi separable del mateix grau que P, d'aquí és suficient $J_{10} \in R^*$, i d'aquí el primer apartat expressant-ho com a funcions enlloc dels invariants:

   $$J_{10} \in R^* \Leftrightarrow J_{2i}^5 J_{10}^{-i} \in R,\ i \leq 5$$

   Observeu $\Leftarrow$ segueix que si $J_{10} \in \wp$ tenim $J_{2i} \in \wp$ for all i, per tant la corba és $y^2 = x^4(x-1)$ ([11]) i no pot ser. (Arguments similars s'usen per a traslladar el resultat sobre els invariants a la forma de l'enunciat del teorema, és a dir mitjançant funcions).

   Si $\tilde{\mathfrak{C}}$ no és llissa, mitjançant un canvi de variables podem escriure

   $$P(x) = \pi x^5 + x^4 + ax^2 + bx + c$$

amb $\pi \in \wp$. Tenim ara $J_{10} \in \wp$ i càlculs en l'anterior expressió de P obtenim en la reducció per $\wp$:

$$\overline{J_2} = -2\overline{a},\ \overline{J_4} = 2^{-3}(\overline{a}^2 - 4\overline{c}),\ \overline{I_4} = \overline{a}^2 + 12\overline{c},$$

$$\overline{J_6} = 2^{-4}\overline{b}^2,\ \overline{I_{12}}2^{-8}disc(\overline{P}).$$

Si $\overline{I_{12}} \neq 0$ llavors la normalització de $\tilde{\mathfrak{C}}$ és una corba el·líptica d'equació $y^2 = \overline{P}(x)$, i $j(E) = \overline{(I_4^3 I_{12}^{-1})}$. Considerem ara $\overline{J_{10}} = \overline{I_{12}} = 0$ i $\tilde{\mathfrak{C}}$ irreductible. Per la irreductibilitat $\overline{J_4}$ o $\overline{J_6}$ no son zero. Un comprova que per estabilitat $\overline{I_4} \neq 0$, obtenint la tercera situació. Per la quarta, considerem llavors $\overline{J_{2i}} = 0$ per a tot $2 \leq i \leq 5$, i es comprova que $\overline{I_4} \neq 0$, obtenim l'última situació pel cas que $\mathfrak{Z}_s$ és irreductible.

2. Suposem ara que $\mathfrak{Z}_s$ té dos components irreductibles. $\mathfrak{Z}_s$ són dues rectes projectives que es tallen en un punt. Podem triar (possiblement fent una extensió) dues $Spec(R)$-seccions Γ_1, Γ_2 amb $(\mathfrak{Z} \setminus (\Gamma_1 \cup \Gamma_2))_s$ afí i connex, amb Γ_i dins la ramificació de f i de la part llissa $\mathfrak{C}$. Denotem per $U = \mathfrak{Z} \setminus (\Gamma_1 \cup \Gamma_2)$ i tenim $U = Spec(R[x, v])$ amb $xv = \pi^2$, $\pi \in \wp \setminus \{0\}$.

   S'obté $f^{-1}(U) = Spec(R[x, v, y, z])$ complint,

$$y^2 = x^3 + ax^2 + x + b\pi^2 + \pi^2 v,\ a, b \in R$$

$$z^2 = v^3 + bv^2 + v + a\pi^2 + \pi^2 x,\ yz = \pi(x^2 + ax + 1 + bv + v^2).$$

   Les components irreductibles de $\tilde{\mathfrak{C}}$ són els completats projectius de les corbes afins

$$y^2 = x^3 + \overline{a}x^2 + x,\ z^2 = v^3 + \overline{b}v^2 + v.$$

Si la primera component (per exemple) és llisa, el seu invariant modular és $2^8(\overline{a}^2-3)^3/(\overline{a}^2-4)$. De les anteriors expressions, tenim una equació afí per a C:

$$w^2 = x^5 + ax^4 + x^3 + b\pi^2x^2 + \pi^4x$$

d'on obtenim que $J_{2i} \in R$, $I_2 - 2^{-4} \in \wp$ si $\mathrm{car}(k) \neq 2, 3$, $I_6 - 1 \in \wp$ si $\mathrm{car}(k) = 3$ i es té:

$$I_4 - (a^2-3)(b^2-3)\pi^4 \in \pi^5 R,\ J_{10} -$$

$$2^{-12}(a^2-4)(b^2-4)\pi^{12} \in \pi^{13}R,$$

$$I_{12} - 2^{-10}\{4(a^2-3)^3(b^2-4) + 4(b^2-3)^3(a^2-4) -$$

$$27(a^2-4)(b^2-4)\}\pi^{12} \in \pi^{13}R$$

Les conclusions de l'enunciat del teorema per a les últimes situacions s'obtenen a partir d'aquí.

□

Capítol 5

El model estable d'una corba de gènere 2

Victor Rotger[1]

5.1 Introducció

Sigui R un anell de valoració discreta, K el seu cos de fraccions, $\mathfrak{m}$ el seu ideal maximal i $k = R/\mathfrak{m}$ el seu cos residual. Denotem $\nu : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ la valoració normalitzada de K.

Sigui C/K una corba llisa geomètricament connexa de gènere $g = 2$. Pel teorema de Deligne-Mumford, existeix una extensió finita K'/K i un model estable $\mathfrak{C}$ sobre R' de $C \times_K K'$, on R' denota la clausura integral de R en K' (cf. Cap. 2). Recordem que en general $\mathfrak{C}$ no és un esquema regular.

Sigui $\tilde{\mathfrak{C}} = \mathfrak{C} \times_{R'} \bar{k}$ la corba estable obtinguda en considerar la fibra tancada de $\mathfrak{C} \times_R R'$ sobre una clausura algebraica

[1]Dep. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya. E-mail: vrotger@ma4.upc.edu

$\bar{k}/k'$ del cos residual k' de R'.

La classe d'isomorfisme de la corba $\tilde{\mathfrak{C}}$ no depèn de la tria de K'. De fet, a l'anterior capítol vam explicar de quina manera $\tilde{\mathfrak{C}}$ està completament determinada en funció dels invariants d'Igusa de C i per tant $\tilde{\mathfrak{C}}$ tan sols depèn de la classe de $\bar{K}$-isomorfisme de $C \times_K \bar{K}$.

L'objectiu d'aquest capítol és discutir els resultats de Liu [13] sobre la geometria i l'aritmètica de $\mathfrak{C}$.

En el cas que K és estrictament henselià, mostrarem en el següent Capítol 6 de quina manera es pot utilitzar aquest material per a determinar la fibra especial $\tilde{\mathfrak{C}}_{min}$ del model minimal regular $\mathfrak{C}_{min}/R$ de C, segons la classificació d'Ogg i Namikawa-Ueno que hem discutit al Capítol 3.

Més precisament, si K és estrictament henselià, existeix una extensió minimal L/K tal que $C \times_K L$ admet un model estable sobre l'anell d'enters de L (cf. Secció 5.2). L'extensió L/K es de Galois i el grup $\mathrm{Gal}(L/K)$ actua en $\tilde{\mathfrak{C}}$; de fet, aquesta acció indueix un monomorfisme $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(\tilde{\mathfrak{C}})$.

Si a més $\mathrm{car}(k) \neq 2, 3, 5$, Viehweg [36] mostra que $\tilde{\mathfrak{C}}_{min}$ està completament determinat per:

(i) $\tilde{\mathfrak{C}}$.

(ii) Les *espessors* dels punts singulars de $\mathfrak{C}$.

(iii) L'acció de $\mathrm{Gal}(L/K)$ en $\tilde{\mathfrak{C}}$.

Pel que fa a (i), al Capítol 4 acabem de veure com es pot descriure $\tilde{\mathfrak{C}}$ en funció dels invariants d'Igusa de C. En aquest capítol ens centrarem en (ii) i encetarem l'estudi de (iii), que conclourem al Capítol 6.

A la Secció 5.2 recordem alguns conceptes fonamentals sobre anells henselians i grups algebraics que farem servir posteriorment. Més endavant, fem la hipòtesi que K és estrictament henselià i justifiquem per què podem fer-ho. Introduïm l'extensió minimal L/K esmentada anteriorment, mostrem que $\mathrm{Gal}(L/K)$ admet una immersió en $\mathrm{Aut}(\tilde{\mathfrak{C}})$ i trobem condicions suficients per a què L/K sigui moderadament ramificada (i per tant cíclica).

A la Secció 5.4 determinem quins són els possibles grups d'automorfismes d'una corba estable (no necessàriament llisa) de gènere aritmètic 2 sobre un cos algebraicament tancat.

A la Secció 5.3 introduïm el concepte d'*espessor* d'una singularitat de l'esquema $\mathfrak{C}$ i al Teorema 5.3.2 discutim un teorema de Liu [13, §5] que determina les espessors dels punts singulars de $\tilde{\mathfrak{C}}$ en funció de les valoracions dels invariants d'Igusa de C.

Pel que hem comentat abans, el coneixement de (i) i (ii) basta per a conèixer el tipus $t(C)$ de $\tilde{\mathfrak{C}}_{min}$ quan K és estrictament henselià i $L = K$. En el mateix Teorema 5.3.2 oferim el resultat. Quan $[L : K] > 1$, hom necessita conèixer (iii) l'acció de $\mathrm{Gal}(L/K)$ sobre $\tilde{\mathfrak{C}}$ per a poder determinar $\tilde{\mathfrak{C}}_{min}$ i això ho estudiem al següent capítol.

A la Secció 5.5 obtenim criteris explícits per a la bona reducció de C sobre K en termes de qualsevol equació hiperel·líptica definidora. En el cas que K sigui estrictament henselià, fixem-nos que això és equivalent a què $\mathfrak{C}$ sigui un esquema llis sobre R i que $L = K$.

5.2 Extensió minimal de la reducció estable

Com a la introducció, sigui R un anell de valoració discreta, K el seu cos de fraccions i $k = R/\mathfrak{m}$ el seu cos residual.

Sigui K^s una clausura separable de K, R^s la clausura integral de R en K^s i triem un ideal $\mathfrak{m}^s$ de R^s a sobre de $\mathfrak{m}$. Siguin $D = \{\sigma \in \mathrm{Gal}(K^s/K) : \sigma(\mathfrak{m}^s) = \mathfrak{m}^s\}$ i $I = \{\sigma \in D : \sigma(x) - x \in \mathfrak{m}^s \,\mathrm{forall}\, x \in R^s\}$ els grups de descomposició i d'inèrcia.

Sigui $\hat{R}$ l'anell completat de R i $\hat{K}$ el seu cos de fraccions.

Sigui R^{sh} el henselianitzat estricte de R, és a dir, el mínim anell de valoració discreta que conté R tal que

- El cos residual k^{sh} de R^{sh} és separablement tancat.
- Per tot $p(x) \in R^{sh}[x]$ i tot $a \in R^{sh}$ tals que $\bar{p}(a) \equiv 0$, $\bar{p}'(a) \not\equiv 0 \in k^{sh}$ existeix un únic element $\alpha \in R^{sh}$ tal que $p(\alpha) = 0$ i $\bar{\alpha} = \bar{a} \in k^{sh}$.

Denotem per K^{sh} el cos de fraccions de R^{sh}. L'anell R^{sh} es pot construir explícitament com la localització del subanell $R^s(I) \subseteq R^s$ fix per I en l'ideal maximal $\mathfrak{m}^s \cap R^s(I)$. Remarquem que hi ha un isomorfisme natural

$$\mathrm{Gal}(K^{sh}/K) \xrightarrow{\simeq} \mathrm{Gal}(\bar{k}/k).$$

Sigui C/K una corba llisa geomètricament connexa de gènere $g = 2$. Sigui $\mathfrak{C}_{min}$ el model minimal regular de C sobre R que hem introduït al Capítol 2.

Sigui $J(C) = \mathrm{Pic}^0(C)$ la varietat Jacobiana de C; essent $g = 2$, $J(C)$ és una superfície abeliana sobre K. Denotem per $\mathfrak{N}$ el model de Néron de $J(C)$ sobre R; $\mathfrak{N}$ és un

grup algebraic separat, llis i de tipus finit sobre R, la fibra genèrica del qual és $J(C)$.

Està caracteritzat llevat d'únic isomorfisme per la següent *propietat d'aixecament*:

Sigui X un esquema llis sobre $S = \mathrm{Spec}(R)$ i $f_K : X \times_S \mathrm{Spec}(K) \dashrightarrow J(C)$ un morfisme racional. Aleshores existeix un morfisme $f : X \to \mathfrak{N}$ que estén f_K a tot X.

Prenent $X = Spec(R)$ es segueix de la propietat d'aixecament que tot punt racional de $J(C)$ sobre K s'estén a un punt enter de $\mathfrak{N}$ sobre R.

Referim a [4] per a detalls sobre l'existència i unicitat de $\mathfrak{N}$.

La component connexa $\tilde{\mathfrak{N}}^0$ de l'element neutre de la fibra tancada $\tilde{\mathfrak{N}}/k$ de $\mathfrak{N}$ és un esquema en grups sobre k. Com a tal, per un resultat fonamental de la teoria de grups algebraics existeix una isogènia

$$\tilde{\mathfrak{N}}^0 \xrightarrow{\sim} A \times T \times U$$

on A és una varietat abeliana, T és un tor i U és un grup unipotent.

Recordem que un tor és un grup algebraic T/k tal que $T \times_k \bar{k} \simeq \mathbb{G}_m \overset{t)}{\times} \cdots \times \mathbb{G}_m$ per algun $t \geq 0$, on $\mathbb{G}_m$ denota el grup multiplicatiu tal que $\mathbb{G}_m(\bar{k}) = \bar{k}^*$.

Un grup unipotent és un grup algebraic U/k tal que $U(\bar{k}) \subset \mathrm{GL}_n(\bar{k})$ és un subgrup del grup de matrius triangulars superiors amb zeros a la diagonal.

Notem per $u = \dim_k(U) \geq 0$. Diem que $J(C)$ té reducció semiestable si $u = 0$. En aquest cas també diem que $\tilde{\mathfrak{N}}^0$ és una varietat semiabeliana.

Sigui $\Phi = \tilde{\mathfrak{N}}/\tilde{\mathfrak{N}}^0$ el grup de components connexes de la

fibra especial $\tilde{\mathfrak{N}}$ de $\mathfrak{N}$.

Escrivim la fibra tancada del model minimal com $\tilde{\mathfrak{C}}_{min} = \sum_{i=1}^{n} r_i \cdot C_i$, on C_i són les seves components irreductibles i r_i les seves multiplicitats; denotem $R = (r_1, ..., r_n)$. Podem formar també la matriu d'intersecció $M = (C_i \cdot C_j) \in \mathrm{M}_n(\mathbb{Z})$. Un resultat de Lorenzini [19, Teorema 1.3] mostra que Φ es pot calcular explícitament de la següent manera.

Lema 5.2.1. $\Phi \simeq \mathrm{Ker}(R)/\mathrm{Im}(M)$.

Posem $R' = R^{sh}$ o $\hat{R}$ i K' el cos de fraccions de R'. Recollim a continuació i sense demostració alguns resultats fonamentals sobre el comportament del model minimal de C, del model estable de C i del model de Néron de $J(C)$ sota canvi de base de R a R'.

Lema 5.2.2.

(i) $\mathfrak{C}_{min} \times_R R'$ *és el model minimal regular de* $C \times_K K'$.

(ii) [4, 7.2] $\mathfrak{N} \times_R R'$ *és el model de Néron de* $J(C) \times_K K'$.

(iii) [13, p. 218] C *admet un model estable sobre* R *si i només si* $C \times_K K'$ *l'admet sobre* R'.

(iv) [6, 2.4] C *admet un model estable sobre* R *si i només si* $u = 0$.

(v) [7, 5.15] Existeix una extensió de Galois L/K^{sh} *tal que per tota extensió finita* L'/K^{sh}, $C \times_K L'$ *té reducció estable si i només si* $L \subseteq L'$.

Motivats per $(i), (ii), (iii)$, suposem durant la resta de la secció que R és estrictament henselià, és a dir, $R^{sh} = R$. En particular, k és separablement tancat. D'acord amb (v),

sigui L/K l'extensió minimal de K on C adquireix reducció estable, sigui R_L l'anell d'enters de L i $\mathfrak{C}$ el model estable de $C \times_K L$ sobre R_L. Com més amunt, denotem per $\tilde{\mathfrak{C}}$ la fibra especial de $\mathfrak{C}$ sobre una clausura algebraica $\bar{k}$ de k.

El grup de Galois $G = \mathrm{Gal}(L/K)$ actua en l'esquema $\mathfrak{C}$; en efecte, si $\sigma \in G$, ${}^{\sigma}\mathfrak{C}$ és de nou un model estable de $C \times_K L$ sobre R_L. Tal i com hem vist al Capítol 2, $\mathfrak{C}$ és únic llevat d'isomorfisme i per tant existeix un isomorfisme $\varphi_\sigma : {}^{\sigma}\mathfrak{C} \to \mathfrak{C}$. Obtenim així un automorfisme

$$\varrho_\sigma : \mathfrak{C} \xrightarrow{\simeq} \mathfrak{C}, \quad x \mapsto \varphi_\sigma({}^{\sigma}x).$$

De fet,

$$\varrho : G \hookrightarrow \mathrm{Aut}(\tilde{\mathfrak{C}})$$

és un monomorfisme de grups.

En efecte, [7, Lema 5.16] mostra que $J(C)$ té reducció semiestable sobre $L_0 = L^{Ker\varrho}$. Per (iv), això és equivalent a l'existència d'un model estable de C sobre L_0. Com L/K és minimal amb aquesta propietat, $L_0 = L$ i per tant ϱ és injectiu.

Sigui d el factor de $[L : K]$ més gran coprimer amb $p = \mathrm{car}(k) \geq 0$. Sigui K^{nr}/K la màxima sub-extensió de L no ramificada; el grup $\mathrm{Gal}(K^{nr}/K)$ és canònicament isomorf a $\mathrm{Gal}(k'/k)$, on k' és una extensió finita de k. Com k és separablement tancat, $f = |\mathrm{Gal}(K^{nr}/K)|$ és una potència de p. Per tant d divideix l'ordre de ramificació $e = [L_K]/f$ de L/K i existeix un grup quocient de $\mathrm{Gal}(L/K^{nr})$ que té ordre d. És conegut que totes les extensions moderadament ramificades de K^{nr} en L són cícliques i per tant *existeix un element en G d'ordre d.*

De fet, $d = [L : K]$ i per tant L/K moderadament ramificada i cíclica, sempre que $p = 0$ o $p > 2g(C) + 1$.

Si $p = 0$ això es deu a què en aquest cas tota extensió de k és separable i per tant k és algebraicament tancat.

Si $p > 2g(C) + 1$, una anàlisi cas per cas tot seguint els resultats de la Secció 5.4 permet veure que no hi ha cap automorfisme de $\tilde{\mathfrak{C}}$ d'ordre p. Com ϱ és un monomorfisme de G en $\mathrm{Aut}(\tilde{\mathfrak{C}})$, obtenim que $p \nmid [L : K]$.

Introduïm les corbes excepcionals

$$C_0 : y^2 = x^5 - 1 \text{ si } \mathrm{car}(k) \neq 5;\ C_0 : y^2 = x^5 - x \text{ si } \mathrm{car}(k) = 5,$$

caracteritzada per $J_2 = J_4 = J_6 = 0$, $J_{10} \neq 0$ i

$$C_1 : y^2 = x^5 - x \text{ si } \mathrm{car}(k) \neq 5,$$

amb $J_2 \neq 0$, $J_4/J_2^2 = 3/40$, $J_6/J_2^3 = -1/400$, $J_{10}/J_2^5 = 1/2^4 \cdot 5^5$.

Corol·lari 5.2.3. *Suposem que* $\mathrm{car}(k) \neq 2, 3$. *Si* $\mathrm{car}(k) = 5$, *suposem que* $\tilde{\mathfrak{C}} \not\cong C_0$. *Aleshores* L/K *és cíclica, moderadament ramificada.*

Demostració. És una conseqüència directa del Teorema 5.4.1 que mostra que, en els casos esmentats, tots els factors primers dels ordres dels elements d'$\mathrm{Aut}(\tilde{\mathfrak{C}})$ (i per tant de G) són diferents de $\mathrm{car}(k)$. Els raonaments anteriors s'apliquen de nou per a concloure el corol.lari. □

Remarca 5.2.4. Lorenzini demostra a [18, 2.7] que si $\tilde{\mathfrak{C}}$ és llisa i L/K és moderadament ramificada, aleshores $[L : K] \leq 2(2u + 1)$.

5.3 Les espessors dels punts singulars de $\mathfrak{C}$

En aquesta secció suposem que k és separàblement tancat i que C/K *és la fibra genèrica d'una corba estable* $\mathfrak{C}$ *sobre* R. Una situació on això es dóna és per exemple quan K és estrictament henselià i $L = K$.

Recordem que en general no sempre succeeix que C admet un model estable sobre el mateix anell R, sinó sobre una extensió finita R'/R.

Sigui $q \in \tilde{\mathfrak{C}}(k)$ un punt singular de la fibra especial de $\mathfrak{C}$. En ser q un punt ordinari doble, la completació $\mathfrak{m}$-àdica de l'anell local $\mathcal{O}_{\mathfrak{C},q}$ verifica

$$\hat{\mathcal{O}}_{\mathfrak{C},q} \simeq \hat{R}[[u,v]]/(uv - \pi)$$

per algun element $\pi \in \mathfrak{m} \setminus \{0\}$ (cf. [17, Cap. 10, Corollari 3.22]).

Definició 5.3.1. L'espessor de q és l'enter positiu $e(q) := \nu(\pi)$.

Sigui $\mathfrak{C}_{min}$ el model minimal regular de C sobre R. Denotem per $t(C)$ el tipus de la reducció de $\mathfrak{C}_{min}$ segons la classificació de Namikawa-Ueno que hem detallat al Capítol 3.

Per a simplificar la notació del següent teorema, sigui $\varepsilon = 1$ si $\mathrm{car}(k) \neq 2, 3$; $\varepsilon = 4$ si $\mathrm{car}(k) = 2$, $\varepsilon = 3$ si $\mathrm{car}(k) = 3$. Donats tres nombres e_1, e_2, e_3, definim d_1 i d_2 per les relacions $d_1 = gcd(e_1, e_2, e_3)$ i $d_1 d_2 = e_1 e_2 + e_1 e_3 + e_2 e_3$.

Teorema 5.3.2. *[13, p. 215-216]*

(I) Si $\tilde{\mathfrak{C}}$ *és llisa, aleshores* $\mathfrak{C}_{min} = \mathfrak{C}$ *i* $\tilde{\mathfrak{N}}$ *és la Jacobiana de* $\tilde{\mathfrak{C}}$.

(II) Si $\tilde{\mathfrak{C}}$ *és irreductible amb un sol punt doble* q,

$$e = e(q) = \frac{1}{6}\nu(J_{10}^6 \cdot I_{12}^{-5}), \quad t(C) = I_{e-0-0}, \quad \Phi = \mathbb{Z}/e\mathbb{Z}.$$

(III) Si $\tilde{\mathfrak{C}}$ *és irreductible amb dos punts dobles* q_1, q_2,

$$e_1 = \inf\{\nu(I_{12}\cdot I_4^{-3}), \frac{1}{4}\nu(J_{10}^2\cdot I_4^{-5})\}, \;\; e_2 = \frac{1}{2}\nu(J_{10}^2\cdot I_4^{-5}) - e_1,$$

$$t(C) = I_{e_1-e_2-0}, \quad \Phi = \mathbb{Z}/e_1\mathbb{Z} \times \mathbb{Z}/e_2\mathbb{Z}.$$

(IV) Si $\tilde{\mathfrak{C}}$ *és la unió de dues rectes projectives que es tallen transversalment en tres punts* q_1, q_2, q_3, *sigui* $l = \nu(J_{10} \cdot J_2^{-5})$, $n = \nu(I_{12} \cdot J_2^{-6})$, $m = \nu(J_4 \cdot J_2^{-2})$. *Aleshores*

$$e_1 = \inf\{l/3, n/2, m\},\ e_2 = \inf\{\frac{l-e_1}{2}, n - e_1\},\ e_3 = l - e_1 - e_2$$

i

$$t(C) = I_{e_1-e_2-e_3}, \quad \Phi = \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}.$$

(V) Si $\tilde{\mathfrak{C}}$ *és la unió de dues corbes el·líptiques que es tallen en un sol punt* q_0,

$$e_0 = \frac{1}{12\varepsilon}\nu(J_{10}^{\varepsilon} \cdot I_{2\varepsilon}^{-5}), \quad t(C) = I_0 - I_0 - e_0, \quad \Phi = \{0\}.$$

(VI) Si $\tilde{\mathfrak{C}}$ *és la unió d'una corba el·líptica i una corba birracional a* $\mathbb{P}_k^1$ *amb un node* q_1 *que es tallen en un sol punt* q_0,

$$e_0 = \frac{1}{12\varepsilon}\nu(I_{12}^{\varepsilon} \cdot I_{2\varepsilon}^{-6}), \quad e_1 = \frac{1}{\varepsilon}\nu(J_{10}^{\varepsilon} \cdot I_{2\varepsilon} \cdot I_{12}^{-\varepsilon}),$$

$$t(C) = I_{e_1} - I_0 - e_0, \quad \Phi = \mathbb{Z}/e_1\mathbb{Z}.$$

(VII) Si $\tilde{\mathfrak{C}}$ és la unió de dues corbes birracionals a $\mathbb{P}^1_k$ amb nodes q_1, q_2 que es tallen en un sol punt q_0,

$$e_0 = \frac{1}{4\varepsilon}\nu(I_4^{\varepsilon} \cdot I_{2\varepsilon}^{-2}),$$

$$e_1 = \inf\{\nu(I_{12}\cdot I_4^{-3}), \frac{1}{2\varepsilon}\nu(J_{10}^{\varepsilon}\cdot I_{2\varepsilon} I_4^{-3\varepsilon})\},\ e_2 = \frac{1}{\varepsilon}\nu(J_{10}^{\varepsilon}\cdot I_{2\varepsilon}\cdot I_4^{-3\varepsilon}) - e_1,$$

i

$$t(C) = I_{e_1} - I_{e_2} - e_0, \quad \Phi = \mathbb{Z}/e_1\mathbb{Z} \times \mathbb{Z}/e_2\mathbb{Z}.$$

Demostració. Pel que hem vist al Capítol 4, la reducció del model estable de C tan sols depèn de la classe de $\bar{K}$-isomorfisme de C i per tant, per a demostrar el teorema, podem utilitzar el model que desitgem de C sobre qualsevol extensió K' de K. Ens limitarem a oferir la prova en el cas (IV) sota la hipòtesi que $\mathrm{car}(k) \neq 2$; per a la resta es procedeix de manera similar.

Llevat de $\bar{K}$-isomorfisme, la corba C està definida per una equació

$$y^2 = x(x-2a)(x-1)(x-1-2b)(2cx-1),\ 0 < \nu(a) \leq \nu(b) \leq \nu(c) < \infty.$$

En efecte, sabem prou que $C/\bar{K}$ admet un model de la forma $y^2 = p(x)$ on $p \in \bar{K}[x]$ és un polinomi de grau 5. Efectuant un canvi de variables podem suposar a més que

dues de les arrels de $p(x)$ a $\bar{K}$ són 0 i 1, mentre que les altres són enters algebraics. La mateixa equació aleshores defineix un model enter de C; que la reducció de C és la unió de dues rectes projectives implica que podem triar la resta d'arrels $\alpha, \beta, \gamma \in \bar{K}$ de $p(x)$ de manera que la seva reducció és 0, 1 i ∞ respectivament. Això és equivalent a dir que $p(x)$ es pot escriure com més amunt.

Sigui $q_1 \in \tilde{\mathfrak{C}}$ l'especialització del punt $(0,0)$. Amb canvis de variable adequats (cf. [13, p. 216]), hom pot veure que $\hat{\mathcal{O}}_{\mathfrak{C},q_1} \simeq \hat{R}[[u,v]]/(u \cdot v - a^2)$. Per tant, $e_1 = 2\nu(a)$. De manera similar obtenim que $e_2 = 2\nu(b)$ i $e_3 = 2\nu(c)$.

D'altra banda, amb la mateixa equació que tenim per a C i les fórmules explícites de què disposem per al càlcul dels invariants d'Igusa, obtenim que

$$\bar{J}_2 = 1, \quad \bar{J}_4 = \frac{1}{4} \cdot (a^2 + b^2 + c^2),$$

$$\bar{J}_{10} = 2^{-6} \cdot (abc)^2, \quad \bar{I}_{12} = 2^{-4} \cdot (a^2b^2 + a^2c^2 + b^2c^2).$$

Comparant els dos càlculs deduïm el resultat enunciat a (IV) per a $e(q_i)$, ordenats de manera que $e_1 \leq e_2 \leq e_3$.

Un cop conegut el model estable $\mathfrak{C}$ de C sobre R, sabem que $\mathfrak{C} = \mathfrak{C}_{can}$ i que $\mathfrak{C}_{min}$ s'obté a partir de $\mathfrak{C}_{can}$ tot fent explotar les singularitats de $\tilde{\mathfrak{C}}$ tantes vegades com sigui necessari (veure Cap. 2).

Més concretament, en el cas (IV) tenim que $\tilde{\mathfrak{C}}$ és la unió de dues rectes projectives que es tallen en tres punts q_1, q_2, q_3, amb espessors e_1, e_2, e_3 respectivament. Explotant $e_i - 1$ vegades cada punt q_i obtenim que $\mathfrak{C}_{min}$ és un esquema sobre $\mathrm{Spec}(R)$ tal que

- $\mathfrak{C}_{min} \times_R K = C$,
- $\tilde{\mathfrak{C}}_{min}$ s'obté a partir de $\tilde{\mathfrak{C}}$ tot substituint el punt q_i per $e(q_i) - 1$ rectes projectives, tal i com mostra la configuració $I_{e_1-e_2-e_3}$. Veure el cas (40) del Cap. 3 o [24, p. 182].

Finalment, per a calcular el grup de components Φ on pot emprar el Lema 5.2.1, ja que tenim un coneixement explícit de les matrius R i M introduïdes a la Secció 2. Concretament, $n = e_1+e_2+e_3-1$, $R = (1, ..., 1)$. Si A, B són les components irreductibles centrals i $C_1^{(i)}, ..., C_{e_i-1}^{(i)}$ les components obtingudes en explotar q_i, tenim que les úniques interseccions no nules són

$$A \cdot C_1^{(i)} = 1, \quad B \cdot C_{e_i-1}^{(i)} = 1, \quad C_j^{(i)} \cdot C_{j+1}^{(i)} = 1$$

per $i = 1, 2, 3$ i $1 \leq j < e_i$,

$$A \cdot A = B \cdot B = -3, \quad C_j^{(i)} \cdot C_j^{(i)} = -2$$

per $i = 1, 2, 3$ i $1 \leq j \leq e_i$.

Un càlcul per inducció mostra que $\Phi \simeq \prod_i \mathbb{Z}/d_i\mathbb{Z}$, $d_1 = gcd(e_1, e_2, e_3)$ i $d_2 = (e_1e_2 + e_1e_3 + e_2e_3)/d_1$, que és el que volíem demostrar. □

Remarca 5.3.3. Si C no admet un model estable sobre R sinó sobre la clausura entera R' d'una extensió finita K'/K aleshores les espessors dels punts singulars són les mateixes de l'enunciat del teorema anterior, multiplicades per l'índex de ramificació de K'/K. Si el cos residual de K és algebraicament tancat, l'índex de ramificació és $[K' : K]$.

Sigui σ la involució hiperel·líptica de C. Per Cap. 2, Cor. 4.3, s'estén a una involució en $\mathfrak{C}$ que seguim denotant σ. Sigui $\mathfrak{Z} = \mathfrak{C}/\langle\sigma\rangle$, una corba sobre R_L amb fibra genèrica $\mathbb{P}^1_L$ i $f : \mathfrak{C} \to \mathfrak{Z}$ el morfisme natural de projecció.

Lema 5.3.4. *En els casos* $(I) - (IV)$, $\mathfrak{Z} \simeq \mathbb{P}^1_{R_L}$. *En els casos* $(V) - (VII)$, $\tilde{\mathfrak{Z}}$ *és la unió de dues rectes projectives que es tallen en un punt d'espessor* $2e_0$, *on* $e_0 = e(q_0)$ *i* q_0 *és el punt d'intersecció de les dues components irreductibles de* $\tilde{\mathfrak{C}}$.

Demostració. La fibra genèrica de $\mathfrak{Z}$ és isomorfa a $\mathbb{P}^1_L$. La fibra tancada té gènere aritmètic 0 i per tant es segueix del Cap. 1, §3.4, que $\tilde{\mathfrak{Z}} = \tilde{\mathfrak{C}}/\langle\sigma\rangle$ és la unió d'un nombre finit de rectes projectives. Com la imatge d'un esquema irreductible és irreductible, $\tilde{\mathfrak{Z}} \simeq \mathbb{P}^1_k$ en els casos $(I) - (III)$. En el cas (IV), $\tilde{\mathfrak{C}}$ és la unió de dues rectes projectives tallant-se en tres punts. Necessàriament σ les permuta: altrament $\tilde{\mathfrak{Z}}$ seria la unió de dues rectes projectives tallant-se en com a mínim dos punts i contradiria que $p_a(\tilde{\mathfrak{Z}}) = 0$. Així $\tilde{\mathfrak{Z}} \simeq \mathbb{P}^1_k$ també en aquest cas i obtenim doncs el lema per als casos $(I) - (IV)$.

En els casos $(V) - (VII)$, σ no pot permutar les dues components irreductibles E_1, E_2 (de gènere aritmètic 1) de $\tilde{\mathfrak{C}}$ perquè si ho fes tindríem $E_1 \simeq E_2 \simeq \tilde{\mathfrak{Z}}$. Per tant $\tilde{\mathfrak{Z}} = E_1/\langle\sigma\rangle \cup E_2/\langle\sigma\rangle$, que ha de ser la unió de dues rectes projectives tal i com predèiem al lema. A més, com $\sigma(q_0) = q_0$, σ indueix una involució en l'anell local $\hat{\mathcal{O}}_{\mathfrak{C},q_0} \simeq \hat{R}[[u,v]]/(uv - \pi)$ que deixa invariants les dues branques analítiques. Per tant $\sigma(u) = -u$, $\sigma(v) = -v$ i el subanell d'element fixos per σ és $\hat{R}[[u^2, v^2, uv]]/(uv - \pi) \simeq$

$\hat{R}[[x,y,z]]/(z-\pi, xy-z^2) \simeq \hat{R}[[x,y]]/(xy-\pi^2)$, fet que mostra que $e(f(q_0)) = 2e_0$. $\square$

5.4 Grups d'automorfismes de corbes estables de gènere 2

L'objectiu d'aquesta secció és determinar el grup d'automorfismes $\mathrm{Aut}(\tilde{\mathfrak{C}})$ de $\tilde{\mathfrak{C}}$ definits sobre una extensió qualsevol de k i calcular els ordres dels elements de $\mathrm{Aut}(\tilde{\mathfrak{C}})$. Amb aquesta motivació, assumim que k és algebraicament tancat. Assumim també que $\mathrm{car}(k) \neq 2$.

Enunciarem aquí del teorema de Liu a [13] sobre el grup d'automorfismes i demostrarem alguns dels casos.

Teorema 5.4.1.

(I) Suposem que $\tilde{\mathfrak{C}}$ és llisa.

- *(a) Si $\tilde{\mathfrak{C}} \not\simeq C_0, C_1$, l'ordre de tot $\tau \in \mathrm{Aut}(\tilde{\mathfrak{C}})$ divideix 4 o 6.*
- *(b) Si $\mathrm{car}(k) \neq 5$, l'ordre de tot $\tau \in \mathrm{Aut}(C_1)$ divideix 6 o 8.*
- *(c) Si $\mathrm{car}(k) \neq 5$, $\mathrm{Aut}(C_0) \simeq \mathbb{Z}/10\mathbb{Z}$.*
- *(d) Si $\mathrm{car}(k) = 5$, $\mathrm{Aut}(C_0) \simeq \mathrm{PGL}_2(\mathbb{F}_5) \ltimes \mathbb{Z}/2\mathbb{Z}$.*

(II) Es satisfà $\bar{J}_{10} = 0$ i $\bar{I}_{12} \neq 0$. La normalització de $\tilde{\mathfrak{C}}$ és una corba el·líptica E/k: denotem per $j = j(E) \in k$. Es té (cf. [13, p. 203]) que $j = \bar{I}_4^3/\bar{I}_{12}$.

(a) *Si* $j \neq 0, 1728$, $\mathrm{Aut}(\tilde{\mathfrak{C}}) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & si\ \bar{J}_6 \neq 0 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & si\ \bar{J}_6 = 0. \end{cases}$

(b) *Si* $j = 1728$ *i* $\mathrm{car}(k) \neq 3$,

$$\mathrm{Aut}(\tilde{\mathfrak{C}}) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & si\ \bar{J}_6 \neq 0 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & si\ \bar{J}_2 \neq 0, \bar{J}_6 = 0 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & si\ \bar{J}_2 = \bar{J}_6 = 0. \end{cases}$$

(c) *Si* $j = 0$ *i* $\mathrm{car}(k) \neq 3$,

$$\mathrm{Aut}(\tilde{\mathfrak{C}}) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & si\ \bar{J}_2 \neq 0, \bar{J}_6 \neq 0 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & si\ \bar{J}_6 = 0 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} & si\ \bar{J}_2 = 0. \end{cases}$$

(d) *Si* $j = 0$ *i* $\mathrm{car}(k) = 3$,

$$\mathrm{Aut}(\tilde{\mathfrak{C}}) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & si\ \bar{J}_6 \neq 0 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & si\ \bar{J}_6 = 0. \end{cases}$$

(III) *Es satisfà* $\bar{J}_{10} = 0 = \bar{I}_{12} = 0$ *i es té*

$$\mathrm{Aut}(\tilde{\mathfrak{C}}) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & si\ \bar{J}_6 \neq 0 \\ \mathbb{Z}/2\mathbb{Z} \ltimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) & si\ \bar{J}_6 = 0, \end{cases}$$

on la primera involució permuta els dos punts singulars.

(IV) $\mathrm{Aut}(\tilde{\mathfrak{C}}) \simeq S_3 \times \mathbb{Z}/2\mathbb{Z}$, *on* S_3 *és el grup de permutacions dels tres punts singulars i* $\mathbb{Z}/2\mathbb{Z}$ *està generat per la permutació de les dues components irreductibles.*

(V_*) Suposem que $\tilde{\mathfrak{C}}$ té dues components irreductibles E_1, E_2 de gènere aritmètic 1 que es tallen en un únic punt p, és a dir, que ens trobem en el cas $(V), (VI)$ o (VII). Aleshores

$$\mathrm{Aut}(\tilde{\mathfrak{C}}) \simeq \begin{cases} \mathrm{Aut}_p(E_1) \times \mathrm{Aut}_p(E_2) & \text{si } E_1 \not\simeq E_2 \\ \mathbb{Z}/2\mathbb{Z} \ltimes (\mathrm{Aut}_p(E_1) \times \mathrm{Aut}_p(E_2)) & \text{si } E_1 \simeq E_2 \end{cases}$$

on $\mathrm{Aut}_p(E_i)$ indica el grup d'automorfismes d'E_i que fixen p i $\mathbb{Z}/2\mathbb{Z}$ està generat per la involució que intercanvia les components E_1 i E_2.

La demostració d'aquest teorema és clàssica (i no pas trivial) quan $\tilde{\mathfrak{C}}$ és llisa; referim el lector a [11, §8] per als detalls.

La prova per a la resta de casos $(II) - (VII)$ és més senzilla perquè la normalització de les components irreductibles de $\tilde{\mathfrak{C}}$ tenen gènere 0 o 1 i els automorfismes de $\mathbb{P}^1$ i d'una corba el·líptica són prou coneguts.

Els casos $(IV) - (V) - (VI) - (VII)$ són evidents. Mostrem com es demostra (II); el cas (III) és similar.

En el cas (II), denotem per $\pi : E \longrightarrow \tilde{\mathfrak{C}}$ el morfisme de normalització, amb $\pi^{-1}(q) = \{q_1, q_2\}$, on recordem de la secció anterior que q és el punt doble de $\tilde{\mathfrak{C}}$.

Tot automorfisme τ de $\tilde{\mathfrak{C}}$ n'indueix un en la normalització, que seguim denotant τ. Com $\tau(q) = q$, deduïm que $\tau(\{q_1, q_2\}) = \{q_1, q_2\}$. Recíprocament, tot automorfisme $\tau \in \mathrm{Aut}(E)$ que deixa invariant $\{q_1, q_2\}$ baixa a un automorfisme de $\tilde{\mathfrak{C}}$ i així tenim que

$$\mathrm{Aut}(\tilde{\mathfrak{C}}) = \{\tau \in \mathrm{Aut}(E) \,:\, \tau(\{q_1, q_2\}) = \{q_1, q_2\}\} = \mathbb{Z}/2\mathbb{Z} \times G,$$

on $G = \{\tau \in \mathrm{Aut}(E) \,:\, \tau(q_i) = q_i\}$ i $\mathbb{Z}/2\mathbb{Z}$ està generat

per una involució σ (de fet, la hiperel·líptica de $\tilde{\mathfrak{C}}$) tal que $\sigma(q_1) = q_2$.

Sigui $0 \in E$ un punt fix qualsevol de σ i considerem en E la llei de grup que té a 0 com a punt d'origen. Aleshores $\sigma \in \mathrm{Aut}(E,+)$; en ser una involució, necessàriament $\sigma = -Id$. Per tant $q_2 = -q_1$ i conjugant per la translació per $-q_1$ en E obtenim que G és conjugat al grup $G' = \{\tau \in \mathrm{Aut}(E,+) : \tau(2q_1) = 2q_1\}$. Observem que $2q_1 \neq 0$ perquè $q_1 \neq q_2$ i que $-Id(2q_1) = 2q_1$ si i només si $4q_1 = 0$.

Per a fer el càlcul explícit de G' en funció dels valors de j, $\bar{J}_2$ i $\bar{J}_6$ cal posar equacions explícites per al morfisme π. Si $\mathrm{car}(k) \neq 2, 3$, podem escriure

$$E : z^2 = f(x) = x^3 + ax + b.$$

Aleshores $\tilde{\mathfrak{C}}$ admet l'equació $y^2 = x^5 + ax^3 + bx^2$ i f no és més que la transformació de Cremona donada per $z = y/x$. Aleshores $q = (0,0) \in \tilde{\mathfrak{C}}$ i $q_1, q_2 = (0, \pm\sqrt{b}) \in E$. Com q és un punt doble ordinari, $b \neq 0$. Un petit càlcul explícit mostra que la coordenada x de $2q_1$ és $a^2/4b$.

Si $j \neq 0, 1728$, és conegut que $\mathrm{Aut}(E,+) = \{\pm Id\}$. Ja hem observat abans que $G' = \mathrm{Aut}(E,+)$ si i només si $4q_1 = 0$, o el que és el mateix:

$$0 = f(a^2/4b) = \frac{a^6 + 2^4 b^2 a^3 + 2^6 b^4}{2^6 b^3} = \frac{\bar{J}_6}{2^6 b^3}.$$

La darrera igualtat es comprova de l'expressió explícita per a J_6 que es pot trobar al Cap. 4, §2, tenint en compte que $a_0 = a_2 = a_5 = a_6 = 0$, $a_1 = 1$, $a_3 = a$ i $a_4 = b$. Això prova (II, a). La resta d'apartats s'obtenen exactament de la mateixa manera. $\square$

Corol·lari 5.4.2. *Suposem que* $\mathrm{car}(k) \neq 2, 3$. *En el cas* (V_*) *obtenim que els divisors primers possibles d'*$\mathrm{Aut}(\tilde{\mathfrak{C}})$ *són* 2 *o* 3.

Demostració. Sigui $E = E_1$ o E_2. Si E és llisa, $\mathrm{Aut}_p(E)$ són els automorfismes de la corba el·líptica E prenent p com a punt origen. És conegut que aleshores $\mathrm{Aut}_p(E)$ és un grup cíclic de 2, 3 o 6 elements.

Si E no és llisa, té una única singularitat nodal en un punt $q \neq p$. Tot automorfisme d'E fixa q i indueix un automorfisme de la normalització $\tilde{E} \simeq \mathbb{P}^1_k$ que fixa $\{q_1, q_2\}$, les dues antiimatges de q. Si a sobre demanem que fixi p obtenim que $\mathrm{Aut}_p(E) \simeq \mathbb{Z}/2\mathbb{Z}$. □

5.5 Criteris de bona reducció

Sigui R un anell de valoració discreta, K el seu cos de fraccions i k el seu cos residual. Fixem un uniformitzant t de R. Suposem que $\mathrm{car}(k) \neq 2$, però no suposem que R sigui estrictament henselià.

Definició 5.5.1. Diem que C/K té bona reducció si és la fibra genèrica d'una corba estable llisa sobre R.

Diem que té bona reducció potencial si existeix una extensió finita de K sobre la qual C adquireix bona reducció.

Definició 5.5.2. Una *equació entera* de C és una equació

$$(\mathcal{E}) \quad y^2 + Q(x)y = P(x)$$

amb $Q(x,)P(x) \in R[x]$, $\deg(Q) \leq 3$, $\deg(P) = 5$ o 6 tal que $\{1, y\}$ és una base de la clausura entera de $R[x]$ en $K(C)$.

Definim el *discriminant* de l'equació $\Delta(\mathcal{E})$ com

$$\begin{cases} 2^{-12} \cdot \operatorname{disc}(R) & \text{si } \deg R = 6 \\ 2^{-12} c^2 \cdot \operatorname{disc}(R) & \text{si } \deg R = 5, \end{cases}$$

on $R(x) = 4P(x) + Q(x)^2$ i c denota el coeficient dominant de $R(x)$.

Diem que l'equació $(\mathcal{E})$ és minimal si $\nu(\Delta(\mathcal{E}))$ és el mínim valor possible d'entre totes les equacions enteres per a C. Anomenem aleshores $\Delta(\mathcal{E})$ el discriminant minimal de C i el denotarem $\Delta_0 = \Delta_0(C)$.

La definició que donem de discriminant minimal és la que proposa Liu a [16, §2]. És natural i prou adequada per als nostres propòsits. A [15] es dóna una definició alternativa en termes del feix dualitzant de C que descrivim al Capítol 7.

En aquesta secció volem donar criteris per a la bona reducció de C sobre K a partir d'una equació qualsevol

$$y^2 = p(x) = a_0 x^6 + a_1 x^5 + ... + a_6 \in K[x]$$

de C.

Remarquem que aquesta qüestió tan sols depèn de la classe de K-isomorfisme de C, però en canvi poden existir corbes C, C' no isomorfes sobre K amb els mateixos invariants d'Igusa tals que C té bona reducció sobre K i C' no.

Per tant, els criteris que cerquem dependran no només dels invariants d'Igusa de C sinó també dels coeficients $a_i \in K$.

Lema 5.5.3. *[16, p. 4583] Sigui $y^2 = p(x)$ una equació per a C amb $P(x) \in K[x]$. Aleshores existeix un canvi de variables $x \mapsto aX + b$, $y \mapsto cY$ amb $a, c \in t^{\mathbb{Z}}$, $b \in R[1/t]$ tal que l'equació resultant*

$$Y^2 = P(X) \in R[X]$$

és minimal per a C.

De fet, C té bona reducció sobre K si i només si el seu discriminant minimal és $\nu(\Delta(\mathcal{E})) = 0$. Referim a [16, §3] per a més detalls. Notem però que $\mathrm{disc}(p)$ és un invariant projectiu de grau 10 i $\ell = 30$ en la notació de [14, §2] o el Cap. 4; per tant, si $(\mathcal{E}_0)$ és una equació minimal i $(\mathcal{E})$ és una equació entera qualsevol per a C, aleshores $\nu(\Delta(\mathcal{E})) = 30r + \nu(\Delta(\mathcal{E}_0))$ per algun $r \geq 0$.

Un fenomen interessant que succeeix aquí i no pas per a corbes el·líptiques és que es pot donar l'existència de dues equacions minimals $(\mathcal{E}), (\mathcal{E}')$ per a C que indueixin models enters no-isomorfs sobre R.

Exemple 5.5.4. Quan $\mathrm{car}(k) \neq 2, 3$, un exemple el trobem en les equacions

$$(\mathcal{E}) \quad y^2 = (x^3 + a)(x^3 + t^6),$$

$$(\mathcal{E}') \quad y^2 = (x^3 + 1)(ax^3 + t^6),$$

on $a \in R^*$ és una unitat qualsevol. Hom calcula que $\nu(\Delta(\mathcal{E})) = \nu(\Delta(\mathcal{E}')) = 12$ i per tant el discriminant és minimal. Totes dues tenen la mateixa fibra genèrica, ja que el canvi de variables $x = t^2/x$, $y = t^3y/x^3$ sobre K transforma una en l'altra; per contra, no hi ha cap transformació entre ambdues que indueixi un isomorfisme entre els dos models sobre R.

Un criteri per a la bona reducció de C el trobem en el següent resultat de Liu. En l'enunciat del següent teorema *assumim que C té bona reducció potencial.*

En efecte, una condició necessària per a la bona reducció de C és que es compleixi aquesta hipòtesi o, en altres paraules, que ens trobem en el cas (I) de la Secció 5.3. Observem que això ja ho hem caracteritzat al Teorema 5.3.2 a partir dels invariants d'Igusa de la corba.

Teorema 5.5.5. *Sigui* $C : y^2 = p(x) = a_0x^6 + a_1x^5 + ... + a_6 \in K[x]$.

1. *Suposem* $a_0 = 0$ *i que* $\mathrm{car}(k) \neq 2, 5$.

   Aleshores C té bona reducció sobre K si i només si $40 \mid \nu(a_1^{30}J_{10}^{-1})$.

2. *Suposem que* $a_0 \neq 0$ *i que* $\mathrm{car}(k) \neq 2, 3, 5$. *Sigui* $A_2 = 12a_0a_2 - 5a_1^2$, $h = A_2^{15}a_0^{-20}J_{10}^{-1}$.

   Aleshores C té bona reducció sobre K si i només si

   - $\nu(h) \geq 0$, $2 \mid \nu(a_0)$, $30 \mid \nu(a_0^{10}J_{10}^{-1})$ *o bé*
   - $\nu(h) < 0$, $2 \mid \nu(A_2)$, $40 \mid \nu(A_2^{15}J_{10}^{-1})$.

Demostració. Notem que h és invariant per les transformacions $x \mapsto ax + b$, $y \mapsto cy$ on $a, c \in K^*$ i $b \in K$,

com també ho són les propietats de divisibilitat de (1) i (2). Això es deu a què un tal canvi de variable transforma A_2 en $a^{10}c^{-4}A_2$, a_0 en $a^6c^{-2}a_0$, a_1 en $a^5c^{-2}a_1$ i J_{10} en $a^{30}c^{-20}J_{10}$ (veure Cap. 4 o bé [14, §2]).

Considerem primer el cas (1) on $a_0 = 0$. Si C té bona reducció, pel Lema 5.5.3 podem suposar que

$$y^2 = p(x) \in R[x]$$

és una equació entera minimal i per tant a_1, $\mathrm{disc}(p) \in R^*$. Com $J_{10} = 2^{-12}a_1^2\mathrm{disc}(p)$ pel Cap. 4, §2, i $\mathrm{car}(k) \neq 2$, obtenim que $a_1, J_{10} \in R^*$ i per tant $\nu(a_1^{30}J_{10}^{-1}) = 0$.

Recíprocament, suposem que $\nu(a_1^{30}J_{10}^{-1}) = 40r$ per algun $r \geq 0$ i posem $a = a_1t^{-2r}$, $b = a_1^3t^{-5r}$. El canvi de variables $x = aX - (5a_1)^{-1}a_2$, $y = bY$ proporciona l'equació

$$Y^2 = X^5 + b_3X^3 + b_4X^2 + b_5X + b_6 \in K[X],$$

que satisfà $J_{10} \in R^*$. Com $\mathrm{car}(k) \neq 5$, a més tenim que $b_i \in R$. Com $J_{10} = 2^{-12}\mathrm{disc}(X^5 + b_3X^3 + b_4X^2 + b_5X + b_6) \in R^*$, obtenim que C té bona reducció.

Considerem ara el cas (2). Com per hipòtesi C cau en el cas (I), C té bona reducció sobre K si i només admet un model estable sobre R. Per tant, si i només si C té bona reducció sobre K^{sh}, gràcies al Lema 5.2.2. Suposem doncs que $R = R^{sh}$. En particular, k és separàblement tancat. Fixem $\bar{k}/k$ una clausura algebraica de k.

Sigui L/K l'extensió minimal on C adquireix reducció estable, $\mathfrak{C}$ el model estable de C sobre R_L i $\sigma \in \mathrm{Aut}(\mathfrak{C})$ la involució hiperel·líptica. Sigui $\mathfrak{Z} = \mathfrak{C}/\langle\sigma\rangle$ i $f : \mathfrak{C} \to \mathfrak{Z}$ la projecció natural. Com $\tilde{\mathfrak{C}}$ és llisa, la fibra tancada $\tilde{\mathfrak{Z}}$ de $\mathfrak{Z}$ és isomorfa sobre $\bar{k}$ a $\mathbb{P}^1_{\bar{k}}$. Fixem un tal isomorfisme i identifiquem $\tilde{\mathfrak{Z}} \times \bar{k} = \mathbb{P}^1_{\bar{k}}$.

Sigui $\bar{\omega}$ el punt de l'infinit en $\tilde{\mathfrak{Z}}$. No essent k necessàriament algebraicament tancat, ben pot ser que $\tilde{\mathfrak{Z}}(k) = \emptyset$; per $\bar{\omega}$ ens referim al punt tancat de l'esquema $\tilde{\mathfrak{Z}}$ que sobre $\bar{k}$ correspon a l'òrbita de Galois $\mathrm{Gal}(\bar{k}/k) \cdot \infty$.

Com R és henselià, existeix un punt ω en la fibra genèrica $\mathfrak{Z}_\eta$ que s'especialitza en $\bar{\omega}$.

Demostrem ara (2). Suposem primer que C té bona reducció sobre K. Pel Lema 5.2.2, podem suposar que l'equació de l'enunciat

$$(\mathcal{E}) \quad y^2 = p(X) = a_0X^6 + ... + a_6$$

de C és minimal sobre R. Observem que el tipus de transformacions que apareixen al lema no belluguen el punt de l'infinit.

Si f és no ramificat a sobre de $\bar{\omega}$, $\bar{p}(X) \in k[X]$ té grau 6 i per tant $a_0 \in R^*$. Com C té bona reducció, $\nu(\Delta(\mathcal{E})) = 0$ i per tant $J_{10} = 2^{-12} \cdot \mathrm{disc}(p) \in R^*$. Obtenim que $\nu(h) = \nu(A_2) \geq 0$ perquè $A_2 \in R$. A més, $2 \mid \nu(a_0) = 0$ i $30 \mid \nu(a_0^{10}J_{10}^{-1}) = 0$.

Si f és ramificat a sobre de $\bar{\omega}$, $\bar{p}(X) \in k[X]$ té grau 5 i per tant $a_0 \in \mathfrak{m}$, $a_1, J_{10} \in R^*$. Deduïm que $A_2 \in R^*$ i que $\nu(h) = -20\nu(a_0) < 0$, $2 \mid \nu(A_2) = 0$ i $40 \mid \nu(A_2^{15}J_{10}^{-1}) = 0$.

Demostrem ara el recíproc: considerem només el cas $\nu(h) \geq 0$; el cas $\nu(h) < 0$ es raona de manera similar. Escrivim $\nu(a_0) = 2q$ i $\nu(a_0^{10}J_{10}^{-1}) = 30r$ amb $q, r \in \mathbb{Z}$. Posem $a = t^{-r}$, $b = t^{-3r+q}$. El canvi de variable $x = aX - (6a_0)^{-1}a_1$, $y = bY$ produeix l'equació

$$(*) \quad Y^2 = P(X) = b_0X^6 + b_2X^4 + b_3X^3 + ... + b_6 \in K[X]$$

per a C. De les lleis de transformació veiem que per a l'equació $(*)$ tenim $J_{10}, b_0 \in R^*$. Un petit càlcul també

mostra que $b_1 = 0$, $b_2 = \frac{A_2 t^{-4r}}{12 a_0 b^2}$ i que la condició $\nu(h) \geq 0$ implica que $b_2 \in R$. Per a demostrar que C té bona reducció sobre K, ens cal veure que $b_i \in R$ per a $i \geq 3$:

Observem que f no ramifica a sobre de $\bar{\omega}$: si ho fes, trobaríem una equació minimal de C de la forma $u^2 = c_0 v^2 + ... + c_6$ amb $c_i \in R$, $c_0 \in \mathfrak{m}$, $c_1 \in R^*$. Tindríem aleshores que $\nu(A_2) = 0$ i $\nu(h) < 0$, fet que contradiu la invariància de h per canvis de variable.

Sigui R_L la clausura entera de R en L i sigui t_L un uniformitzant. Pel Lema 5.2.2 existeix un canvi de variables $X \mapsto \alpha U + \beta$, $Y \mapsto \gamma V$ amb $\alpha, \gamma \in t_L^{\mathbb{Z}}$ i $\beta \in R_L[1/t_L]$ que transforma $(*)$ en una equació entera minimal $U^2 = d_0 V^6 + ... + d_6 \in R_L[V]$. Com f segueix sense ramificar a sobre de $\bar{\omega}$, $d_0 \in R_L^*$. Encara tenim també que $J_{10} \in R_L^*$ ja que C té bona reducció sobre L. De les lleis de transformació de b_0 i J_{10} deduïm que $\alpha^6/\gamma^2, \alpha^{30}/\gamma^{20} \in R_L^*$. Per tant $\alpha, \gamma \in R_L^* \cap t_L^{\mathbb{Z}}$ i doncs $\alpha = \gamma = 1$.

Obtenim que $Q(X) = P(X+\beta) \in R_L[X]$. Com $b_0 \in R^*$ i $b_1 = 0$, el terme de grau 5 de $Q(X)$ ens mostra que $\beta \in R_L$. Finalment, $P(X) = Q(X - \beta) \in K[X] \cap R_L[X] = R[X]$, que és el que volíem. $\square$

Capítol 6

El model minimal d'una corba de gènere 2

Santiago Molina[1]

6.1 Introducció

Com en el capítol anterior, sigui R un anell de valoració discreta henselià amb k cos residual algebraicament tancat (R serà llavors estrictament henselià), K el seu cos de fraccions, $\wp$ el seu ideal maximal.

Sigui C/K una corba llisa geomètricament connexa de gènere $g = 2$. Sabem que aquesta és hiperel·líptica i per tant definida per una equació

$$y^2 = a_0x^6 + a_1x^5 + \cdots + a_6 = P(x) \in K[x] \qquad (6.1.1)$$

on $a_0 \neq 0$ o $a_1 \neq 0$.

Amb el que hem vist al Capítol 2, sabem que la corba C admet un model minimal regular $\mathfrak{C}_{min}/R$. El propòsit

[1]Dep. Matemàtica Aplicada II, Universitat Politècnica de Catalunya. E-mail: santimolin@gmail.com

d'aquest capítol és descriure *l'algoritme de Liu* que calcula la fibra especial d'aquest model $\mathfrak{C}_{min,\wp}$ en funció dels coeficients a_i, l'anàleg a *l'algoritme de Tate* per a corbes el·líptiques en gènere 2. L'idea és, a partir de l'equació (6.1.1), reconèixer el tipus específic de reducció descrit en el Capítol 3.

Per fer això utilitzarem fortament els resultats desenvolupats en el capítol 5. Recordem que, pel teorema de Deligne-Mumford, existeix una extensió finita L/K i un model estable $\mathfrak{C}$ sobre R_L de $C \times_K L$, on R_L denota la clausura integral de R en L (cf. Cap. 2). I, a més, podem triar L minimal amb aquesta propietat (Cap. 5 Lema 4.1).

Tal i com s'havia comentat en el capítol anterior, si $\mathrm{char}(k) \neq 2, 3, 5$, el treball de Viehweg [36] ens diu que $\mathfrak{C}_{min,\wp}$ està completament determinat per:

- $\tilde{\mathfrak{C}} = \mathfrak{C} \times_{R_L} \bar{k}$. Que pel capítol 4 està totalment determinada pels invariants d'Igusa, i per tant per l'equació de C (6.1.1).

- Les *espessors* dels punts singulars de $\mathfrak{C}$. Que en el capítol 5 també hem posat en funció d'aquests invariants i del grau $[L : K]$ de l'extensió.

- L'acció de $\mathrm{Gal}(L/K)$ en $\tilde{\mathfrak{C}}$.

Per tant, per a tenir completament determinada la fibra $\mathfrak{C}_{min,\wp}$ a partir de l'equació hiperel·liptica (6.1.1), haurem de explicitar el grau de l'extensió $[L : K]$ i l'acció de $\mathrm{Gal}(L/K)$ sobre $\tilde{\mathfrak{C}}$, a partir dels coeficients a_i.

Per qüestions tècniques nosaltres ens restingirem a descriure el cas de que L sigui una extensió *moderadament*

ramificada, o sigui que la característica del cos residu no divideix al grau de l'extensió. Quan l'extensió es *salvatgement ramificada*, $\mathrm{char}(k)|[L:K]$, l'algoritme es complica i no escau descriure'l. Aquesta hipòtesi és bastant feble ja que pel capítol 5, L/K és moderadament ramificada sempre que $\mathrm{car}(k) \neq 2, 3, 5$.

6.2 Notacions i Hipòtesis

Com hem dit en l'introducció R serà un anell de valoració discreta henselià amb k cos residual algebraicament tancat. Suposarem durant tota la exposició que $\mathrm{char}(k) \neq 2$. Siga K el cos de fraccions de R, $\wp$ el seu ideal maximal generat per l'uniformitzador t, denotem per ν la valoració normalitzada de K ($\nu(t) = 1$).

Per l'extensió finita L/K, teníem R_L la clausura íntegra de R en L amb ideal maximal $\wp_L$ i amb valoració normalitzada ν_L ($\nu_L(t) = [L:K]$).

Per altra part fixem una familia $\{e_m|(m, \mathrm{char}(k)) = 1\}$ on e_m és una arrel primitiva m-éssima de la unitat en K, sabem que existeix ja que K és estrictament henselià i $(m, \mathrm{char}(k)) = 1$, tal que $e_p = e_{mp}^m$. La imatge de e_m a k la denotarem també per e_m. Si $[K' : K] = m$ és primer amb $\mathrm{char}(k)$, sabem que $K' = K[t_m]$, amb $t_m^m = t$. Denotem per τ el generador de $\mathrm{Gal}(K'/K)$ definit per $\tau(t_m) = e_m t_m$. Per la secció 3 del capítol 5 hi ha una immersió canònica de $\mathrm{Gal}(L/K)$ en $\mathrm{Aut}(\widetilde{\mathfrak{C}})$ i denotem $\overline{\tau}$ la imatge de τ.

Com s'explica al capítol 4, a partir de l'equació hiperel.líptica de la nostra corba (6.1.1) tenim els invariants projectius d'Igusa J_{2i} de grau $2i$, així com els invariants afins A_i, de

tipus $(5i, i)$ i els B_{2j}, de tipus $(8j, 2j)$. Si $Q(x) = b_0x^6 + b_1x^5 + \cdots + b_6 \in K[x]$, denotarem $A_i(Q) = A_i(b_0, b_1, \ldots, b_6)$ al invariant associat al polinomi Q.

6.3 Càlcul del grau de l'extensió $[L:K]$, i l'acció de $\mathrm{Gal}(L/K)$ sobre $\widetilde{\mathfrak{C}}$

Recordem que nosaltres ens restringirem al cas moderadament ramificat, es a dir $([K:L], \mathrm{car}(k)) = 1$.

Recordem del Capítol 2 Cor.4.23, que si σ és la involució hiperel.líptica de C, per unicitat del model estable, aquesta s'estén a una involució de $\mathfrak{C}$, que també denotarem per σ. A més, com hem vist en el capítol 5, el quocient $\mathfrak{Z} = \mathfrak{C}/\langle\sigma\rangle$ és una corba semi-estable sobre R_L amb fibra genèrica isomorfa a $\mathbb{P}^1_L$ i reducció $\widetilde{\mathfrak{Z}} = \widetilde{\mathfrak{C}}/\langle\sigma\rangle$.

D'ara en endavant $f : \mathfrak{C} \to \mathfrak{Z}$ serà el morfisme canònic; $\omega \in \mathfrak{Z}_\eta$ és el punt corresponent a $x = \infty$ en $\mathbb{P}^1_K$; siga $\overline{\omega} \in \widetilde{\mathfrak{Z}}$ la seua especialització. Direm que f ramifica, si f ramifica a $\overline{\omega}$. El punt ω és K-racional, i per tant $\overline{\omega}$ és invariant per $\mathrm{Gal}(L/K)$. Els canvis de la forma $x = \alpha v + \gamma$, $y = \beta z$ deixen invariants els punts ω i $\overline{\omega}$.

Remarca 6.3.1. Sigui H un invariant afí de tipus (l, d) associat a una equació $y^2 = P(x)$. Transformem aquesta en l'equació $z^2 = Q(v)$, mitjançant el canvi $x = \alpha v + \gamma$, $y = \beta z$. Diem H' al corresponent invariant però ara de la nova equació. Aleshores

$$y^2 = \beta^2 z^2 = P(x) \Rightarrow z^2 = \beta^{-2} P(x)$$

per tant els coeficients de P es veuran afectats pel factor β^{-2}, i com H és homogeni de grau d, $H(\beta^{-2}P(x)) = \beta^{-2d}H$. Ara be, per definició de invariant afí, el canvi $x = \alpha v + \gamma$ afecta de la següent forma

$$H' = \alpha^l H(\beta^{-2}P(x)) = \alpha^l \beta^{-2d} H.$$

6.3.1 Suposem que $\widetilde{\mathfrak{C}}$ és llisa

Com que $\widetilde{\mathfrak{C}}$ és llisa, si $z^2 = \overline{Q}(v)$ és l'equació de $\widetilde{\mathfrak{C}}$, sabem per la teoria de corbes hiperel.líptiques que el fet que f ramifiqui implica $\deg(\overline{Q}) = 5$, en cas contrari $\deg(\overline{Q}) = 6$.

Proposició 6.3.2. *El punt $\overline{\omega}$ ramifica si i només si $A_5 \neq 0$ i $a_0^{20} J_{10} A_5^{-6} \in \wp$. A més, en aquest cas el morfisme $C \to \mathbb{P}^1_K$ ramifica en un punt racional $x_0 \in \mathbb{P}^1(K)$*

Demostració. Pel que s'ha fet al Capítol 4 sabem que el punt $\omega \in \mathfrak{Z}(L)$ indueix una secció $\mathrm{Spec}(R_L) \to \mathfrak{Z}$ amb imatge $\Gamma \in \mathfrak{Z}$. També sabem que $\mathfrak{Z} - \Gamma = \mathrm{Spec}(R_L[v])$, $f^{-1}(\mathfrak{Z} - \Gamma) = \mathrm{Spec}(R_L[v,z]/z^2 - Q(v))$ on v i z, s'obtenen de x i y pel canvi $x = \alpha v + \gamma$, $y = \beta z$, α, β i $\gamma \in L$. Ara bé, si $Q(v) = b_0 v^6 + b_1 v^5 + \cdots + b_6$, per veure si $\overline{\omega}$ ramifica hem de veure si $b_0 \in \wp$. Si ens fixem en el tipus de a_0, J_{10} i A_5 veiem que $a_0^{20} J_{10} A_5^{-6}$ roman invariant pels canvis que hem efectuat, segons la remarca anterior 6.3.1, aquest tipus d'invariant l'anomenarem *invariant afí absolut*. Per tant $a_0^{20} J_{10} A_5^{-6} = b_0^{20} J'_{10} A'^{-6}_5$. Ara be com que $J'_{10} \in R_L^*$ per ser $\widetilde{\mathfrak{C}}$ llisa ($\overline{J'_{10}}$ és el discriminant del polinomi $\overline{Q}$), tenim que el fet de que $b_0^{20} J'_{10} A'^{-6}_5 \in \wp$ implica $b_0 \in \wp$. Suposem ara que $\overline{\omega}$ ramifica. Com que $b_0 \in \wp$, segons la seua expressió, $A'_5 \equiv b_1^5 (\mathrm{mod}\ \wp)$. Aleshores com que $\widetilde{\mathfrak{C}}$ és llisa, $b_1 \in \mathbb{R}^*$ i per tant, $A_5 \in \mathbb{R}^*$. Per consegüent $b_0^{20} J'_{10} A'^{-6}_5 \in \wp$.

Siga $x_0 \in \mathbb{P}^1_L$ el punt de $\mathfrak{Z}_\eta$ on f ramifica que s'especialitza en $\overline{\omega} \in \widetilde{\mathfrak{Z}}$. Aquest punt existeix perquè tot punt on $\widetilde{\mathfrak{Z}}$ ramifica es pot posar, després d'un canvi de variables, com imatge un punt corresponent a una arrel de polinomi $\overline{Q}$ que defineix l'equació hiperel.líptica $z^2 = \overline{Q}(v)$. Com que R_L és estrictament henselià, aquest s'estén a un punt

de $\mathfrak{C}_\eta$ per tant la seua imatge a $\mathfrak{Z}_\eta$ ramifica. Com que hem vist que $\overline{\omega}$ és invariant $\mathrm{Gal}(L/K)$, també ho serà x_0, per tant, $x_0 \in \mathbb{P}^1(K)$. □

Ara veurem una proposició que ens mostrarà en quines situacions estem en el cas moderadament ramificat (recordem que en tota la exposició $\mathrm{car}(k) \neq 2$).

Ens adrecem al capítol 5 per descriure a la corba C_0 en $\mathrm{car}(k) = 5$.

La familia de corbes Ω en $\mathrm{car}(k) = 3$ és la següent

$$\Omega = \{y^2 = x^6 + x^4 + x^2 + a,\ a \in k^*\}$$

Proposició 6.3.3. *En qualsevol d'aquestes situacions, l'extensió L és moderadament ramificada*

(a) $\mathrm{car}(k) \neq 3, 5$

(b) $f : C \to \mathbb{P}^1_K$ *ramifica en dos punts racionals de* $\mathbb{P}^1_K$

(c) $\mathrm{car}(k) = 3$, $\overline{\omega}$ *ramifica ó* $\widetilde{\mathfrak{C}} \notin \Omega$

(d) $\mathrm{car}(k) = 5$, $\overline{\omega}$ *no ramifica ó* $\widetilde{\mathfrak{C}} \not\simeq C_0$

Demostració. Es tracta de veure com $\mathrm{Gal}(L/K) \subseteq \mathrm{Aut}(\widetilde{\mathfrak{C}})$. □

Per fi, calculem el grau de l'extensió $[L : K]$ i com actua el grup $\mathrm{Gal}(L/K)$ en $\widetilde{\mathfrak{C}}$.

Teorema 6.3.4. *Suposem que L/K és moderadament ramificada. Siguin n, r i q els enters definits com es mostra*

(a) Si $\overline{\omega}$ és no ramificada, n és el minim comú denominador de $\nu(a_0^{10}J_{10}^{-1})/30$ i $\nu(a_0^5 J_{10}^{-1})/10$, $r = n\nu(a_0^{10}J_{10}^{-1})/30$ i $q = n\nu(a_0^5 J_{10}^{-1})/10$.

(b) Si $\overline{\omega}$ ramifica, n és el minim comú denominador de $\nu(A_5^{-2}J_{10})/20$ i $\nu(A_5^{-6}J_{10}^5)/40$, $r = -n\nu(A_5^{-2}J_{10})/20$ i $q = -n\nu(A_5^{-6}J_{10}^5)/40$.

Aleshores $[L:K] = n$. A més, si $\widetilde{\mathfrak{C}}$ està definit per l'equació $z^2 = \overline{Q}(v) \in k[v]$, τ (generador de $\mathrm{Gal}(L/K)$) actua sobre $\widetilde{\mathfrak{C}}$ de la següent forma: $\overline{\tau}(z) = e_n^q z$, $\overline{\tau}(v) = e_n^r v + c$, $c \in k$.

Demostració. Farem la part (b) però la primera part es fa de manera similar, per tant suposarem que $\overline{\omega}$ ramifica.

Si seguim amb les notacions de la proposició 6.3.2, $\widetilde{\mathfrak{C}}$ està definida en un obert afí per $z^2 = \overline{Q}(v)$, segons la remarca 6.3.1

$$A_5' = \alpha^{25}\beta^{-10}A_5 \in R_L^*, \quad J_{10}' = \alpha^{30}\beta^{-20}J_{10} \in R_L^*$$

Per tant, aïllant α i β respectivament

$$\alpha^{20} = A_5^{-2}J_{10}R_L^*, \quad \beta^{40} = A_5^{-6}J_{10}^5R_L^*$$

Com que $A_5, J_{10} \in K$

$$\nu_L(\alpha^{20}) = 20\nu_L(\alpha) = \nu_L(A_5^{-2}J_{10}) = \nu(A_5^{-2}J_{10})[L:K] \in \mathbb{Z}$$

$$\nu_L(\beta^{40}) = 40\nu_L(\beta) = \nu_L(A_5^{-6}J_{10}^5) = \nu(A_5^{-6}J_{10}^5)[L:K] \in \mathbb{Z}$$

llavors tenim que $n|[L:K]$, sigui $t_n \in L$ tal que $t_n^n = t$, llavors $\alpha \in t_n^r R_L^*$, $\beta \in t_n^q R_L^*$. Com que τ actua trivialment sobre Γ, ja que $\Gamma = \{\overline{\omega}, x_0\}$ invariants per $\mathrm{Gal}(L/K)$, τ actua sobre $f^{-1}(\mathfrak{Z} - \Gamma) = \mathrm{Spec}(R_L[z,v]/z^2 - Q(v))$ de la forma (τ actua trivialment sobre x i y que estan definits sobre K)

$$\tau(z) = \tau(\beta y) = \tau(\beta)y = \tau(\beta)\beta^{-1}z$$

$$\tau(v) = \tau(\alpha x + \gamma) = \tau(\alpha)x + \tau(\gamma) = \tau(\alpha)\alpha^{-1}(v - \gamma) + \tau(\gamma)$$

Aleshores sabent que τ actua sobre t_n multiplicant pel factor e_n, i actua trivialment sobre les reduccions de R_L^*, perquè estem treballant amb anells estrictament henselians, tenim

$$\overline{\tau}(z) = e_n^{-q} z, \quad \overline{\tau}(v) = e_n^{-r} v + c, \ c \in k$$

per tant,

$$\overline{\tau}^n(z) = z, \quad \overline{\tau}^n(v) = v + c(\sum_{k=0}^{n-1} e_n^{-kr})$$

Si $e_n^{-r} \neq 1$ aleshores $\overline{\tau}^n(v) = v$ i per tant $\overline{\tau}^n = 1$. Per consegüent, $n|[L : K]$ i $e_n^{-r} = 1$, i aleshores $\overline{\tau}^{n\mathrm{car}(k)}(v) = v + n\mathrm{car}(k)c = v$, per tant $n\mathrm{car}(k)|[L : K]$. Com que estem en el cas moderadament ramificat, $([L : K], \mathrm{car}(k)) = 1$, $n|[L : K]$ en qualsevol cas, i queda $n = [L : K]$. □

6.3.2 Suposem que $\widetilde{\mathfrak{C}}$ és singular i $\widetilde{\mathfrak{C}}/\langle\sigma\rangle$ irreductible

Denotem C_{000} la corba sobre k estable que consisteix en dos rectes projectives que es tallen en tres punts.

Tal i com hem vist en l'exposició del Capítol 4, el cas en el que estem correspon a tres tipus de reducció de $\widetilde{\mathfrak{C}}$:

- $\widetilde{\mathfrak{C}}$ és irreductible amb un únic punt singular.
- $\widetilde{\mathfrak{C}}$ és irreductible y racional amb dos punts singulars.
- $\widetilde{\mathfrak{C}} = C_{000}$.

Per simplificar, associem l'invariant projectiu J_{12}, de grau 12 per a cada un dels 3 casos:

$$J_{12} := \begin{cases} I_{12} \text{ si } \widetilde{\mathfrak{C}} \text{ té un únic punt singular} \\ I_4^3 \text{ si } \widetilde{\mathfrak{C}} \text{ és irreductible i racional} \\ J_2^6 \text{ si } \widetilde{\mathfrak{C}} = C_{000} \end{cases}$$

Proposició 6.3.5. *tenim les següents propietats*

(a) El punt $\overline{\omega}$ és no ramificat per $f \Leftrightarrow a_0^{-6} J_{12}^{-1} B_2^9, a_0^{-120} J_{12}^{-5} A_5^{36} \in R$.

(b) $f^{-1}(\overline{\omega})$ és regular $\Leftrightarrow a_0^{120} J_{12}^5 A_5^{-36} \in \wp, B_2^{60} J_{12}^{-5} A_5^{-12} \in R$.

(c) $f^{-1}(\overline{\omega})$ és singular $\Leftrightarrow a_0^6 J_{12} B_2^{-9} \in \wp, B_2^{-60} J_{12}^5 A_5^{12} \in \wp$.

Demostració. Segons la remarca 6.3.1, sabem que $a_0^{-6} J_{12}^{-1} B_2^9$, $a_0^{-120} J_{12}^{-5} A_5^{36}$ i $B_2^{60} J_{12}^{-5} A_5^{-12}$, són invariants afins absoluts. Per altra banda, el teorema (10) del Capítol 4 ens diu que en cadascun dels casos que ens pertoquen, existeix un canvi de variables on $J_{12} \in R_L^*$.

(a) Per tant, és clar que si $\overline{\omega}$ no ramifica $a_0^{-6} J_{12}^{-1} B_2^9$, $a_0^{-120} J_{12}^{-5} A_5^{36} \in R$. Recíprocament suposem que $\overline{a_0} = 0$, com que $a_0^{-120} J_{12}^{-5} A_5^{36} \in R$, $A_5 \in \wp$, per tant $\overline{a_1} = 0$. A més, com que $a_0^{-6} J_{12}^{-1} B_2^9 \in R$, $B_2 \in \wp$ i per tant $\overline{a_2} = 0$, absurd. Per consegüent $a_0 \notin \wp$.

Tant en (b) com en (c) $f^{-1}(\overline{\omega})$ és un punt, per tant $\overline{\omega}$ ramifica. Aleshores, després d'un canvi de variables, $\mathfrak{C}$ serà la corba amb part afí

$$y^2 = \pi x^6 + a_1 x^5 + x^4 + a_4 x^2 + a_5 x + a_6 \quad \pi \in \wp$$

Això implica, $A_5 = u_1^5 + \pi r_1$ $B_2 = 2 + \pi r_2 \in R^*$ amb $r_1, r_2 \in R$. Com que $f^{-1}(\overline{\omega})$ és regular si $\overline{u_1} \neq 0$, es a dir

$A_5 \notin \wp$, i per tant $B_2^{60} J_{12}^{-5} A_5^{-12} \in R$ i $a_0^{120} J_{12}^5 A_5^{-36} \in \wp$ per a que $\overline{\omega}$ ramifiqui.

I també, $f^{-1}(\overline{\omega})$ és singular si $\overline{u_1} = 0$, es a dir $A_5 \in \wp$, obtenim, $B_2^{-60} J_{12}^5 A_5^{12} \in \wp$ i $a_0^6 J_{12} B_2^{-9} \in \wp$ per a que $\overline{\omega}$ ramifiqui.

Recíprocament tant en un cas com en l'altre, si $a_0^6 J_{12} B_2^{-9} \in \wp$ o $a_0^{120} J_{12}^5 A_5^{-36} \in \wp$, $\overline{\omega}$ ramifica, per tant $a_0 \in \wp$. En el segon cas, si $B_2^{-60} J_{12}^5 A_5^{12} \in \wp$ aleshores $A_5 \in \wp$, per consegüent $\overline{b_1} = 0$ i $f^{-1}(\overline{\omega})$ és singular. En el cas (b), si suposem que $\overline{b_1} = 0$, com que $B_2^{60} J_{12}^{-5} A_5^{-12} \in R$, aleshores $B_2 \in \wp$ i per tant $\overline{b_2} = 0$, absurd. Per consegüent $b_1 \notin \wp$ i $f^{-1}(\overline{\omega})$ és regular. □

Com en la secció anterior, veurem una proposició que ens mostrarà en quines situacions estem en el cas moderadament ramificat.

Proposició 6.3.6. *En qualsevol d'aquestes situacions, l'extensió L és moderadament ramificada*

(a) $\mathrm{car}(k) \neq 3$ *o* $\widetilde{\mathfrak{C}} \neq C_{000}$

(b) $\mathrm{car}(k) = 3$ *o* $\widetilde{\mathfrak{C}} = C_{000}$ *i* $\overline{\omega}$ *ramifica*

Demostració. Igual com en la secció anterior, hem de veure, amb cadascuna de les hipòtesis anteriors, l'ordre de $\mathrm{Aut}(\widetilde{\mathfrak{C}})$ i com s'injecta $\mathrm{Gal}(L/K)$ en $\mathrm{Aut}(\widetilde{\mathfrak{C}})$. □

Per fi, calculem el grau de l'extensió $[L : K]$ i com actua el grup $\mathrm{Gal}(L/K)$ en $\widetilde{\mathfrak{C}}$.

Teorema 6.3.7. *Suposem que L/K és moderadament ramificada. Siguin n, r i q els enters definits com es mostra*

(a) *Si $\overline{\omega}$ és no ramificada, n és el minim comú denominador de $\nu(a_0^{12}J_{12}^{-1})/36$ i $\nu(a_0^6 J_{12}^{-1})/12$, $r = n\nu(a_0^{12}J_{12}^{-1})/36$ i $q = n\nu(a_0^6 J_{12}^{-1})/12$.*

(b) *Si $f^{-1}(\overline{\omega})$ és un punt regular, n és el minim denominador de $\nu(A_5^{36}J_{12}^{-25})/240$, $q = n\nu(A_5^{36}J_{12}^{-25})/240$ i $r = -2q$.*

(c) *Si $f^{-1}(\overline{\omega})$ és un punt singular, n és el minim comú denominador de $\nu(B_2^{-6}J_{12})/12$ i $\nu(B_2^{-9}J_{12})/12$, $r = n\nu(B_2^{-6}J_{12})/12$ i $q = n\nu(B_2^{-9}J_{12})/12$.*

Aleshores $[L : K] = n$. A més, si $\widetilde{\mathfrak{C}}$ està definit per l'equació $z^2 = \overline{Q}(v) \in k[v]$, τ actua sobre $\widetilde{\mathfrak{C}}$ de la següent forma: $\overline{\tau}(z) = e_n^q z$, $\overline{\tau}(v) = e_n^r v + c$, $c \in k$.

Demostració. Farem la part (a) però les altres parts es fan de manera similar. Per tant suposarem que $\overline{\omega}$ no ramifica.

Si seguim amb les notacions de la proposició 6.3.2, $\widetilde{\mathfrak{C}}$ està definida en un obert afí per $z^2 = \overline{Q}(v)$, amb $\deg \overline{Q} = 6$ i $\overline{Q}(v)$ té arrels simples i dobles. Segons la remarca 6.3.1

$$a_0' = \alpha^6\beta^{-2}a_0 \in R_L, \quad J_{12}' = \alpha^{36}\beta^{-24}J_{12} \in R_L$$

Per tant, aïllant α i β respectivament

$$\alpha^{36} = a_0^{-12}J_{12}R_L^*, \quad \beta^{12} = a_0^{-12}J_{12}R_L^*$$

Com que $a_0, J_{12} \in K$

$$\nu_L(\alpha^{36}) = 36\nu_L(\alpha) = \nu_L(a_0^{-12}J_{12}) = \nu(a_0^{-12}J_{12})[L : K] \quad \nu_L(\alpha) \in \mathbb{Z}$$

$$\nu_L(\beta^{12}) = 12\nu_L(\beta) = \nu_L(a_0^{-12}J_{12}) = \nu(a_0^{-12}J_{12})[L : K] \quad \nu_L(\beta) \in \mathbb{Z}$$

llavors tenim que $n|[L : K]$. Sigui $t_n \in L$ tal que $t_n^n = t$, llavors $\alpha t_n^r \in R_L^*$, $\beta t_n^q \in R_L^*$. Com en el cas anterior, τ

actua sobre $f^{-1}(\mathfrak{Z} - \Gamma) = \mathrm{Spec}(R_L[z,v]/z^2 - Q(v))$ de la forma

$$\tau(z) = \tau(\beta y) = \tau(\beta)y = \tau(\beta)\beta^{-1}z$$

$$\tau(v) = \tau(\alpha x + \gamma) = \tau(\alpha)x + \tau(\gamma) = \tau(\alpha)\alpha^{-1}(v - \gamma) + \tau(\gamma)$$

Aleshores sabent que τ actua sobre t_n multiplicant pel factor e_n, i τ no actua sobre les reduccions de R_L^* perquè estem treballant amb anells estrictament henselians, tenim

$$\overline{\tau}(z) = e_n^q z, \quad \overline{\tau}(v) = e_n^r v + c,\ c \in k$$

Per tant, de igual manera que hem fet en la secció anterior, arribem a $n = [L : K]$. □

6.3.3 Suposem que $\widetilde{\mathfrak{C}}/\langle\sigma\rangle$ no és irreductible

Durant tota aquesta secció suposarem que $\mathrm{car}(k) \neq 3$. El cas especial $\mathrm{car}(k) = 3$ es tractat en el capítol 6 de l'article [14]. Com hem vist en els capítols 5 i 4, el esquema $\widetilde{\mathfrak{Z}}$ correspon a dos rectes projectives que es tallen transversalment en un punt. I tal com hem vist en el corol·lari 3.2 del mateix capítol, els possibles divisors del cardinal de $\mathrm{Aut}(\widetilde{\mathfrak{C}})$ (i per tant de $[L : K]$) són 2 i 3. Per consegüent L/K és moderadament ramificat.

També sabem que el cas en el que estem correspon a tres tipus de reducció de $\widetilde{\mathfrak{C}}$:

- $\widetilde{\mathfrak{C}}$ es compon de dos corbes llises de gènere 1 que es tallen transversalment.
- $\widetilde{\mathfrak{C}}$ es compon de dos corbes que es tallen transversalment, una llisa de gènere 1 i l'altra racional amb un punt singular.

- $\widetilde{\mathfrak{C}}$ es compon de dos corbes racionals singulars que es tallen transversalment.

Per a nosaltres E_1 i E_2 seran les components irreductibles de $\widetilde{\mathfrak{C}}$, amb $\overline{\omega} \in f(E_1)$, definim

$$d_k := \begin{cases} \frac{1}{12}\nu(J_{10}J_2^{-5}) \text{ si } E_1 \text{ i } E_2 \text{ són llises} \\ \frac{1}{12}\nu(I_{12}J_2^{-6}) \text{ si } \widetilde{\mathfrak{C}} \text{ té una única component llisa} \\ \frac{1}{4}\nu(I_4J_2^{-2}) \text{ si } E_1 \text{ i } E_2 \text{ són singulars} \end{cases}$$

Pel tant, si fem una ullada al mateix capítol 5 teorema 2.2 remarca 2.3 l'espessor del punt P és $d = d_k[L : K]$. Aleshores pel Capítol 5 lema 2.4, l'espessor de $f(P)$ és $2d$.

Remarca 6.3.8. Com hem vist en el Capítol 4, $\mathfrak{Z}$ té un obert afí de la forma $U = \mathrm{Spec}(R_L[x, v]/(xv - \pi^2))$. I segons el Capítol 5, l'espessor del punt d'intersecció $E_1 \cap E_2$ és $2\nu_L(\pi)$.

Ara bé, Si volem traslladar el punt d'intersecció de les dues components al punt de l'infinit, primer fem el canvi

$$x \to s - t \quad v \to s + t$$

Per tant queda $U = \mathrm{Spec}(R_L[s, t]/(s^2 - t^2 - \pi^2))$. Si homogeneïtzem i deshomogeneïtzem obtenim l'altre obert afí $V = \mathrm{Spec}(R_L[s, z]/(s^2 - 1 - \pi^2 z))$, que correspon a dues rectes que es tallen en l'infinit.

Per tant, com que en l'antimatge del primer obert $f^{-1}(U)$ les components estaven definides per

$$y^2 = x^3 + ax^2 + x + b\pi^2 + \pi^2 v \quad z^2 = v^3 + bv^2 + v + a\pi^2 + \pi^2 x,$$

multiplicant les dos expressions, tindrem que en $f^{-1}(V)$, estarà definit per

$$y^2z^2 = w^2 = y^3x^3 - \pi^2 q(x, v, z) = (s^2 - 1)^3 + \pi^2 q(x, v, z).$$

En conclusió, si la nostra corba té el punt d'intersecció en l'infinit, després d'un canvi de variables, serà de la forma $w^2 = a_0 P_1(s) P_2(s)$ on $\overline{P_1}(s) = (s-1)^3$ i $\overline{P_2}(s) = (s+1)^3$.

Amb el mateix raonament, l'espessor del punt d'intersecció serà la meitat de la suma del mínim entre la diferència de les arrels de P_1 i P_2. Ja que, com que $\overline{P_1}(s) = (s-1)^3$, si λ_i^j són les arrels de P_j, $\lambda_i \equiv 1 (mod\ t_n)$,

$$m_j = \min\{\lambda_i^j - \lambda_k^j, \}$$

per tant $P_1(s)P_2(s) = (s-1)^3(s+1)^3 + t_n^{m_1} t_n^{m_2} q(s)$.

Proposició 6.3.9. *tenim les següents propietats següents*

(a) El punt $\overline{\omega}$ és no ramificat per $f \Leftrightarrow a_0^{-2} J_2^{-2} B_2^3, a_0^{-4} J_2^{-1} A_3^2$, $a_0^{-20} J_2^{-5} A_5^6 \in R$ i almenys una de les dues últimes expressions són invertibles en R.

(b) $f^{-1}(\overline{\omega})$ és regular $\Leftrightarrow a_0^{20} J_2^5 A_5^{-6} \in \wp, B_2^{10} J_2^{-5} A_5^{-2} \in R$.

(c) $f^{-1}(\overline{\omega})$ és singular $\Leftrightarrow a_0^2 J_2^2 B_2^{-3} \in \wp, B_2^{-10} J_2^5 A_5^2 \in \wp$.

(d) El punt $\overline{\omega}$ és singular $\Leftrightarrow a_0^{-2} J_2^{-2} B_2^3 \in R$ i $a_0^{-4} J_2^{-1} A_3^2$, $a_0^{-20} J_2^{-5} A_5^6 \in \wp$.

Demostració. pels casos (a),(b) i (c), sigui $\mathfrak{Z}'$ el model de $\mathfrak{Z}_\eta = \mathbb{P}^1_L$ obtingut en contraure la segona component $f(E_2)$ de $\widetilde{\mathfrak{Z}}$. Com $f(E_2) \cong \mathbb{P}^1_k$ i $f(E_1) \cdot f(E_2) = -1$ (són les úniques components i es tallen transversalment), pel criteri de Castelnuovo $\mathfrak{Z}'$ és el model minimal de $\mathbb{P}^1_L$, per tant $\mathfrak{Z}' = \mathbb{P}^1_{R_L}$.

Hem suposat que $\overline{\omega} \in f(E_1)$. Sigui S l'imatge de la secció induïda $\mathrm{Spec}(R_L) \to \mathfrak{Z}'$. Aleshores $\mathfrak{Z}' - S \cong \mathbb{A}^1_{R_L} = \mathrm{Spec}(R_L[v])$. Tenim

$$\mathfrak{C} \xrightarrow{2:1} \mathfrak{Z} \xrightarrow{\text{birracional}} \mathfrak{Z}'.$$

En anells indueix la inclusió

$$R_L[v] \subset L[v] \subset_{2:1} L(C).$$

La clausura entera de $R_L[v]$ en el cos de funcions $L(C)$ serà

$$R_L[z,v]/(z^2 - Q(v)) \text{ on } Q(v) \in R_L[v].$$

Correspon a un model birracional a $\mathfrak{C}$, però no isomorf. Tenim que $\widetilde{\mathfrak{C}'} : z^2 = \overline{Q}(v) \in k[v]$, en l'obert afí $\mathfrak{Z}' - S$. Si totes les arrels de $\overline{Q}$ tinguessin com a molt multiplicitat 2, pels exercicis 3.4 i 3.29 del capítol 10 del llibre [17], tindríem que $z^2 = \overline{Q}(v)$ és estable sobre k. I per tant que $\mathfrak{C}'$ seria el model estable de C. Per unicitat $\mathfrak{C} \cong \mathfrak{C}'$ i per tant $\mathfrak{Z}' \cong \mathfrak{C}'/\langle\sigma\rangle \cong \mathfrak{C}/\langle\sigma\rangle \cong \mathfrak{Z}$. Però això ja hem vist que no pot ser. Per tant, després d'un canvi de variables $\overline{Q}(v) = v^3\overline{H}(v)$. A més raonant amb el gènere aritmètic veiem que $\deg(H) > 0$ i $v \not| \overline{H}(v)$. A més com que $\overline{\omega}$ no és singular $\overline{H}$ no és un cub.

Per tant $\overline{\omega}$ ramifica si $\deg(\overline{H}) = 3$, $f^{-1}(\overline{\omega})$ és un punt regular si $\deg(\overline{H}) = 2$ i $f^{-1}(\overline{\omega})$ és un punt singular si $\deg(\overline{H}) = 1$.

Com que $\overline{Q}(v) = \overline{a_0}v^6 + \overline{a_1}v^5 + \overline{a_2}v^4 + \overline{a_3}v^3 \Rightarrow \overline{a_4}, \overline{a_5}, \overline{a_6} = 0$, les propietats de $\overline{H}$ es tradueixen:

$$v \not| \overline{H}(v) \Rightarrow \overline{a_3} \neq 0 \Rightarrow \overline{J_2} \neq 0$$

$$\text{Si } \overline{a_0} \neq 0 \ \overline{H}(v) \text{ no és un cub} \Rightarrow \overline{A_3 A_5} \neq 0$$

Aleshores si el punt $\overline{\omega}$ és no ramificat $\Rightarrow$ els invariants afins absoluts $a_0^{-2}J_2^{-2}B_2^3, a_0^{-4}J_2^{-1}A_3^2, a_0^{-20}J_2^{-5}A_5^6 \in R$, i almenys una de les dues últimes expressions són invertibles en R. Recíprocament, suposem que $a_0 \in \wp$. Si $a_0^{-2}J_2^{-2}B_2^3 \in R$, per l'expressió de B_2 arribem a, $\overline{a_2} = 0$. Fent el mateix

argument amb $a_0^{-20}J_2^{-5}A_5^6$, obtenim $\overline{a_1}=0$. Però això és absurd ja que hem dit que $\deg(H)>0$.

Si $f^{-1}(\overline{\omega})$ és regular $\Rightarrow \overline{a_0}=0, \overline{a_1}\neq 0 \Rightarrow \overline{a_0}=0, \overline{A_5}\neq 0$ $\Rightarrow a_0^{20}J_2^5A_5^{-6}\in \wp, B_2^{10}J_2^{-5}A_5^{-2}\in R$. Recíprocament, com que $a_0^{20}J_2^5A_5^{-6}\in\wp$, $\overline{a_0}=0$. Suposem $\overline{a_1}=0\Rightarrow \overline{A_5}=0$. Com que $B_2^{10}J_2^{-5}A_5^{-2}\in R$, $\overline{B_2}=0$. Per tant, $\overline{a_2}=0$, absurd per la mateixa raó que abans. Per tant $\overline{a_1}\neq 0$.

Si $f^{-1}(\overline{\omega})$ és singular $\Rightarrow \overline{a_0}=0, \overline{a_1}=0, \overline{a_2}\neq 0 \Rightarrow$ $\overline{a_0}=0, \overline{A_5}=0, \overline{B_2}\neq 0 \Rightarrow a_0^2J_2^2B_2^{-3}\in\wp, B_2^{-10}J_2^5A_5^2\in\wp$. Recíprocament, com que $a_0^2J_2^2B_2^{-3}\in\wp$, $\overline{a_0}=0$. I com que $B_2^{-10}J_2^5A_5^2\in\wp$, $\overline{A_5}=0\Rightarrow\overline{a_1}=0$.

Per últim, si $\overline{\omega}$ és singular, hi ha un canvi de variables $x=\alpha v+\gamma$ $y=\beta z$, amb $\alpha,\beta,\gamma\in L$, que dóna una equació $z=\delta H(v)$, on $\delta\in L$ i $H\in R_L[v]$ mònic. A més es compleix que $\overline{H}(v)=(v^2-1)^3$. Aleshores, per càlculs directes $a_0^{-2}J_2^{-2}B_2^3\in R$ i $a_0^{-4}J_2^{-1}A_3^2, a_0^{-20}J_2^{-5}A_5^6\in\wp$. Recíprocament, si $\overline{\omega}$ no fos singular, com que $a_0^{-2}J_2^{-2}B_2^3\in R$ i $a_0^{-4}J_2^{-1}A_3^2, a_0^{-20}J_2^{-5}A_5^6\in\wp$, tindríem que $\overline{H}$ és un cub, cosa que no pot passar. □

Proposició 6.3.10. *Tot element de* $\mathrm{Gal}(L/K)$ *deixa* E_i *invariant si i només si* $2|\nu(J_2)$.

Demostració. Si $\mathrm{Gal}(L:K)$ tingués un element d'ordre imparell ha de deixar cada E_i invariant. Com que $\mathrm{Gal}(L:K)$ és cíclic, $\mathrm{Gal}(L:K)$ deixa cada E_i invariant. Per altra banda, si $\mathrm{Gal}(L:K)$ té un element d'ordre imparell, $\mathrm{Aut}(\widetilde{\mathfrak{C}})=\mathrm{Aut}(E_1)\times\mathrm{Aut}(E_2)$ té un element d'ordre imparell. Com que deixa fix E_i, cada $\mathrm{Aut}(E_i)$ té un element de ordre imparell. Per tant cada E_i és una corba el·líptica regular amb invariant j zero. Això dicta una única classe

d'isomorfisme per a C amb $2|\nu(J_2)$.

Podem suposar que $[L:K]$ és una potència de 2. Suposem que E_1 és invariant per tot element de $\mathrm{Gal}(L/K)$. Si E_1 és llisa, com que hi ha un nombre parell de punts on f ramifica en E_1, i el punt de intersecció de E_1 y E_2 és invariant per $\mathrm{Gal}(L/K)$. Hi ha un punt, regular de E_1, que ramifica y és invariant per $\mathrm{Gal}(L/K)$. Si E_1 és singular, el punt singular és un punt doble. Per tant, continua havent-hi un punt ramificat regular que ha de ser invariant per $\mathrm{Gal}(L/K)$, perquè és l'únic regular en $\widetilde{\mathfrak{C}}$ que ramifica.

En qualsevol dels casos, tenim un punt regular $\overline{x_0}$, on f ramifica invariant per $\mathrm{Gal}(L/K)$. Per ser regular, i R henselià, aquest és una especialització d'un punt $x_0 \in \mathfrak{C}_\eta$ racional sobre K. Després d'un automorfisme $PGL_2(K)$ de $\mathbb{P}^1_K$, podem suposar que $f(x_0) = \omega$.

Pel lema anterior, sabem que en aquest cas ($\overline{\omega}$ ramifica i $f^{-1}(\overline{\omega})$ regular), $B_2^{10} J_2^{-5} A_5^{-2} \in R$. Com que existeix un canvi afí on $J_2, A_5 \in R^*$. aleshores $10|\nu(J_2^{-5} A_5^{-2})$, per tant $2|\nu(J_2)$.

Si els E_i no fossin invariants per $\mathrm{Gal}(L/K)$, l'únic punt invariant per $\mathrm{Gal}(L/K)$ seria el punt d'intersecció dels E_i. Per tant aquest hauria de ser $\overline{\omega}$. Amb les notacions de la prova anterior, tenim un canvi afí $x = \alpha v + \gamma$ $y = \beta z$, on la fibra especial és $z^2 = \overline{a_0}(v^2-1)^3$. $\mathrm{Gal}(L/K)$ passa de E_1 a E_2, aleshores l'acció de Galois a de ser $\tau(v) = -v$. Llavors $\alpha\tau(\alpha)^{-1} \in -1 + \wp$. Segons la notació de les proves dels apartats anteriors, $\alpha = t_n^r \alpha' \Rightarrow \tau(\alpha) = e_n^r \alpha + \wp$, per tant $r = \frac{n}{2}$.

Si $z^2 = \overline{a_0}(v^2-1)^3$ tenim $a_0^2 J_2^{-1} \in R_L^*$. Per tant segons la remarca 6.3.1, $\alpha^6 a_0^2 J_2^{-1} \in R_L^*$. Com que $\nu_L(a_0) = 0$,

$6\nu_L(\alpha) - \nu_L(J_2) = 0 = 6\frac{n}{2} - n\nu(J_2)$, aleshores, $2 \not| \nu(J_2)$. $\square$

Un invariant numèric. Sigui $H(u) = b_0u^3 + b_1u^2 + b_2u + b_3 \in K[u]$ un polinomi separable de grau 3. Tenim els invariants classics: $c_4(H) = 16(b_1^2 - 3b_0b_2)$ i $\mathrm{disc}(H)$ el discriminant de H. Definim

$$\varrho(H) = \min\left\{\frac{1}{2}\nu(c_4(H)), \frac{1}{6}\nu(\mathrm{disc}(H))\right\} \in \mathbb{Q}$$

Sigui ν_K, l'única valoració de K^{alg} que prolonga ν. Llavors un simple càlcul (sabem que $\mathrm{disc}(H) = \prod_{i>j}(\lambda_i - \lambda_j)^2$ on λ_i són les arrels de H) ens diu

$$\varrho(H) = \nu(b_0) + \min\left\{\nu_K(\lambda_i - \lambda_j)\right\}$$

Lema 6.3.11. *Si* $\mathrm{car}(k) \neq 2, 3$*, aleshores la corba el·líptica* $z^2 = H(u)$ *té reducció estable si i només si* $\varrho(H) \in 2\mathbb{Z}$.

Demostració. Primerament, sabem que en una corba el·líptica l'invariant j és $j(H) = \frac{c_4(H)^3}{\mathrm{disc}(H)}$. Per altra banda, també sabem que un canvi de variable de la corba el·líptica afecta als invariants de la següent forma

$$c_4' = a^4c_4 \quad \mathrm{disc}(H') = a^{12}\mathrm{disc}(H).$$

Per tant, $\varrho(H') = \varrho(H) + 2\nu(a)$.

(a) Si $\nu(j) = 3\nu(c_4) - \nu(\mathrm{disc}(H)) \geq 0$, per una part $\varrho(H) = \frac{1}{6}\nu(\mathrm{disc}(H))$. Per l'altra, la corba té reducció estable en K si i només si té bona reducció (ja que bona reducció estable implica potencialment bona reducció). Aleshores amb l'equació minimal $\nu(\mathrm{disc}(H')) = 0$. I per consegüent $\varrho(H) = \frac{1}{6}\nu(\mathrm{disc}(H')) + 2\nu(u) \in 2\mathbb{Z}$.

(b) Si $\nu(j) < 0$, per una part $\varrho(H) = \frac{1}{2}\nu(c_4(H))$. Per l'altra, la corba té reducció estable en K si i només si té reducció nodal (ja que bona reducció estable implica potencialment reducció multiplicativa). Aleshores amb l'equació minimal $\nu(c_4(H')) = 0$. I per consegüent $\varrho(H) = \frac{1}{2}\nu(c_4(H')) + 2\nu(u) \in 2\mathbb{Z}$.

□

Considerem el polinomi $P(x) = a_0x^6 + \cdots + a_6$. Si $a_0 \neq 0$, posem

$$r_K = \frac{1}{2}\nu(a_0) + \min\left\{\frac{1}{4}d_K, \frac{1}{8}\nu(A_2^{-3}A_3^2), \frac{1}{12}\nu(A_2^{-5}(A_3A_2 - 3A_5)^2)\right\} \in \mathbb{Q} \tag{6.3.2}$$

Lema 6.3.12. *Suposem que $\overline{\omega}$ és singular i $2|\nu(J_2)$. Aleshores tenim les següents propietats.*

(α) C admet una equació $w^2 = a_0P_0(u)$, amb $P_0(u) \in R[u]$ mònic i $\overline{P}(u) = (u^2-1)^3$.

(β) Si $P_0(u) = P_1(u)P_2(u)$ és la descomposició de $P_0(u)$ en $R[u]$ (sabem que existeix pel lema de Hensel per a polinomis), amb $P_1(u)$ mònic, i $\overline{P_1}(u) = (u-1)^3$. Llavors

$$\varrho(a_0P_1) + \varrho(a_0P_2) = 2\nu(a_0) + 2d_K,$$

i

$$\min\{\varrho(a_0P_1), \varrho(a_0P_2)\} = 2r_K$$

Demostració. (α) Partim de l'equació $y^2 = P(x)$. De manera similar als anteriors resultats, tenim $a_0^{-4}A_2^3J_2^{-1} \in R^*$. Ara be, com que $2|\nu(J_2) \Rightarrow 2|\nu(A_2)$. Aleshores A_2 és un quadrat. Per consegüent existeix $a \in K$ tal que $a^2 = -A_2/(36a_0^2)$. Fem el canvi de variables $u = a^{-1}(x + a_1/(6a_0))$,

$w = a^{-3}y$, i $P_0(u) = a_0^{-1}a^{-6}P(au - a_1/(6a_0))$. D'aquesta manera ens assegurem que P_0 té coeficient $b_1 = 0$, $P_0(u) = u^6 + b_2u^4 + b_3u^3 + b_4u^2 + b_5u + b_6 \in K[u]$. I l'equació resulta

$$w^2 = a_0P_0(u).$$

Com que $b_1 = 0$, és fàcil calcular $12b_2 = A_2(P_0) = a_0^{-2}a^{-2}A_2 = 36$, segons la remarca 6.3.1. On $b_2 = -3, A_2(P_0)J_2(P_0) \in R^*$. Pel la proposició 6.3.9(d), tenim que $b_3, b_5 \in \wp$. El fet de que $J_{10}(P_0), I_{12}(P_0) \in \wp$ implica que $\overline{P_0}$ té una arrel triple (està clar ja que estem en els casos V, VI i VII). Per consegüent $\overline{P_0}(u) = (u^2 - 1)^3$.

(β) La primera igualtat és immediata a partir de la remarca 6.3.8. Per la segona escrivim

$$P_0(u) = ((u-b)^2+b_{11}(u-b)+b_{12})((u+b)^2+b_{21}(u+b)+b_{22}),$$

amb $b, b_{ij} \in K$, llavors per la definició

$$\varrho(P_i) = \min\left\{\frac{1}{2}\nu(b_{i1}), \frac{1}{6}\nu(4b_{i1}^3 + 27b_{i2}^2)\right\}$$

la segona identitat surt a partir de la avaluació de r_k a partir de $P_0(u)$. □

L'acció de $\mathrm{Gal}(L/K)$ **sobre** $\widetilde{\mathfrak{C}}$**.** Siguin E_1 i E_2 les components irreductibles de $\widetilde{\mathfrak{C}}$. Abans de tot, hem de precisar la naturalesa de les seues components relativa a ω. Si tenim que $\overline{\omega}$ és regular, aleshores suposarem que $E_1 \supset f^{-1}(\overline{\omega})$. Si suposem que $\overline{\omega}$ és singular i $2|\nu(J_2)$, siguin P_1 i P_2 els polinomis del lema anterior. Els zeros de P_1 indueixen zeros punts en $\mathfrak{C}_\eta$. Si $\varrho(P_1) < \varrho(P_2)$, aleshores E_1 serà la component que conté les especialitzacions d'aquests punts. Si $\varrho(P_1) = \varrho(P_2)$ o $2 \not| \nu(J_2)$, l'elecció de E_1 és indiferent.

Escrivim les equacions de E_1 i E_2

$$\begin{cases} E_1: & z_1^2 = v_1^3 + \alpha_{11}v_1^2 + \alpha_{12}v_1 + \alpha_{13} \\ E_2: & z_2^2 = v_2^3 + \alpha_{21}v_2^2 + \alpha_{22}v_2 + \alpha_{23} \end{cases}$$

on la funció racional v_i sobre E_i tenint els pols al punt d'intersecció $E_1 \cap E_2$. Com en els apartats anteriors τ és el generador de $\mathrm{Gal}(L/K)$, tal que $\tau(t_m) = e_m t_m$, per tot divisor m de $[L:K]$, $\overline{\tau}$ la seua imatge canònica en $\mathrm{Aut}_k(\widetilde{\mathfrak{C}})$.

Teorema 6.3.13. *Suposem $2|\nu(J_2)$. Siguin n i r els enters definits com es mostra*

(a) Si $\overline{\omega}$ és no ramificada, n és el minim comú denominador de d_K i $\nu(a_0J_2)/6$, $r = n\nu(a_0J_2)/6$.

(b) Si $\overline{\omega}$ és regular i $f^{-1}(\overline{\omega})$ és un punt regular, n és el minim denominador de d_K i $\nu(A_5^2J_2)/8$, $r = n\nu(A_5^2J_2)/8$.

(c) Si $\overline{\omega}$ és regular i $f^{-1}(\overline{\omega})$ és un punt singular, n és el minim denominador de d_K i $\nu(B_2)/4$, $r = n\nu(B_2)/4$.

(d) Si $\overline{\omega}$ és singular, n és el minim denominador de d_K i r_K, $r = nr_K$.

Aleshores $[L:K] = n$. A més, si $d = nd_K$, τ actua sobre $\widetilde{\mathfrak{C}}$ de la següent forma

$$\begin{cases} \overline{\tau}(z_1) = e_n^{-3r}z_1, & \overline{\tau}(v_1) = e_n^{-2r}v_1 \\ \overline{\tau}(z_2) = e_n^{-3(d-r)}z_2, & \overline{\tau}(v_2) = e_n^{-2(d-r)}v_2 \end{cases}$$

Demostració. Primer farem el cas de $\overline{\omega}$ regular. Suposem que $f^{-1}(\overline{\omega})$ és un punt singular (els casos (a) i (b) es fan de manera similar). Siga $n' = [L:K]$, $d' = d_K n' \in \mathbb{N}$

l'espessor del punt $E_1 \cap E_2$ en $\mathfrak{C}$. Llavors existeix un canvi $x = \alpha v + \gamma, y = \beta z$, amb $\alpha, \beta, \gamma \in L$, tal que

$$z^2 = Q(v) \in R_L[v] \text{ amb } \overline{Q}(v) = v^2(v+1) \in k[v] \quad (6.3.3)$$

per ser $f^{-1}(\overline{\omega})$ singular.

Per tant tenim que el punt d'intersecció $E_1 \cap E_2$ estarà en l'altre punt singular $v = 0$. Sabem per la remarca 6.3.8, que l'altra component E_2 compleix $x_2 v = \pi^2$, $d_K = \nu(\pi)$ (el punt $E_1 \cap E_2$ estarà en $x_2 = 0$). I si la corba estava definida per $z^2 = Q(v)$, la corba amb la variable x_2 estarà definida per

$$y_2^2 = \pi^{-6} x^6 Q(\frac{\pi^2}{x_2}) = P(x_2).$$

Ara bé, com hem dit al principi, ens interessa que la funció v_2 tingui un pol en $E_1 \cap E_2$ en comptes d'un zero. Per tant fem el canvi hiperel·líptic

$$P_1(v_2) = v_2^6 P(\frac{1}{v_2}) = \pi^6 Q(\pi^2 v_2).$$

Per tant fent el canvi

$$v = t_{n'}^{2d'} v_2, z = t_{n'}^{3d'} z_2, \quad (6.3.4)$$

obtenim l'equació d'E_2: $z_2^2 = H(v_2) \in R_L[v_2]$ amb

$$\overline{H}(v_2) = v_2^3 + \alpha_{22} v_2 + \alpha_{23} \in k[v_2], \quad \alpha_{22} \text{ ó } \alpha_{23} \neq 0$$

de 6.3.3 resulta (segons la remarca 6.3.1)

$$\alpha^6 \beta^{-4} J_2 = J_2(Q) \in R_L^* \quad \alpha^8 \beta^{-4} B_2 = B_2(Q) \in R_L^*$$

Aïllant α, $2\nu_L(\alpha) - \nu_L(J_2) + \nu_L(B_2) = 2\nu_L(\alpha) - n'\nu(J_2) + 4n'\frac{r}{n} = 0 \Rightarrow \alpha \in t_n^{-2r} K R_L^*$ ja que per hipòtesi $2|\nu(J_2)$ (per

tant un element amb valoració a L $n'\nu(J_2)/2$ és de K). Amb un raonament similar $\beta \in t_n^{-3r} K R_L^*$. Com que $n'd_K \in \mathbb{N}$, tenim que $t_n \in L$. Un cop tenim com és la valoració de α i β, tal i com hem fet en els apartats anteriors tenim que $\overline{\tau}(v) = e_n^{2r} v + \mu$ amb $\mu \in k$, i $\overline{\tau}(z) = e_n^{3r} z$. Com que $\overline{\tau}$ deixa invariant $E_1 \cap E_2$ corresponent a $v = 0$, tenim $\mu = 0$. Com que volem que v_1 tingui un pol en $E_1 \cap E_2$, fem $v_1 = v^{-1}$ i $z_1 = v^{-3} z$, per tant la corba serà $z_1^2 = v_1^2(v_1 + 1)$ i

$$\overline{\tau}(v_1) = e_n^{-2r} v_1, \quad \overline{\tau}(z_1) = e_n^{-3r} z_1.$$

Per altra banda, sabem que la component E_2 està definida per l'equació $z_2 = \overline{H}(v_2)$ 6.3.4 d'abans. Com que $v = t_{n'}^{2d'} v_2, z = t_{n'}^{3d'} z_2$, tenim

$$\overline{\tau}(v_2) = e_{n'}^{-2d'} e_n^{2r} v_2 = e_{n'}^{(n'/n)(-2nd_K)} e_n^{2r} v_2 = e_n^{-2(r-d)} v_2,$$
$$\overline{\tau}(z_2) = e_{n'}^{-3d'} e_n^{3r} z_2 = e_{n'}^{(n'/n)(-3nd_K)} e_n^{3r} z_2 = e_n^{-3(r-d)} z_2.$$

Per consegüent, com que totes les transformacions tenen el factor e_n^t per algun t, es compleix $\overline{\tau}^n = 1$. Per consegüent $[L : K] = n' = n$.

Suposem ara que $\overline{\omega}$ és singular. Continuarem amb les notacions del lema 6.3.12. Primerament sabem que $n|[L : K]$. Ja que, per una part $[L : K]d_K = d \in \mathbb{N}$. Per l'altra, com que les corbes E_1 i E_2 són estables a L i estan definides per $z_i^2 = a_0 P_i(u)$, pel lema 6.3.11, $\varrho_L(a_0 P_i) \in 2\mathbb{Z}$. Per tant, per 6.3.12, $2r_L = \min\{\varrho_L(a_0 P_1), \varrho_L(a_0 P_2)\} \in 2\mathbb{Z}$, i $r_L = [L : K] r_K \in \mathbb{Z}$. Suposem, per exemple, que $\varrho(a_0 P_1) \leq \varrho(a_0 P_2)$. Aleshores $\varrho(a_0 P_1) = 2r/n$ segons el lema 6.3.12. Escrivim $P_1(u) = (u - b)^3 + \pi Q(u - b) \in R[u]$ on $\pi \in \wp$ i $b \equiv 1 (\mod \wp)$. Com hem vist en la remarca 6.3.8, $u - b$ és la funció que té un zero en el punt $E_1 \cap E_2$. Per fer que tingui

un pol, hem de fer com abans un canvi $u - b = \pi'^2 v_1$, de manera que ens surti una corba el·líptica estable. Tenim $w^2 = a_0((u-b)^3+\pi Q(u-b))P_2(u)$, fent el canvi $u-b = \pi'^2 v_1$ i obtenim

$$w^2 = a_0(\pi'^6 v_1^3 + \pi Q(\pi'^2 v_1))P_2(b + \pi'^2).$$

Ara be, $P_2(u) = (u + b)^3 + \pi Q'(u + b)$, per tant $P_2(b) \equiv 2b^3 \equiv 8(\mod \wp)$ i per tant invertible, per tant existeix $c \in R^*$ tal que $c^2 = P_2(b)$. Llavors

$$w^2 = a_0(\pi'^6 v_1^3 + \pi Q(\pi'^2 v_1))b^2(1 + \varepsilon(v_1)).$$

on $\varepsilon(v_1) \in \wp_L[v_1]$. Si $w = bw'$ obtenim

$$w'^2 = a_0(\pi'^6 v_1^3 + \pi Q(\pi'^2 v_1))(1 + \varepsilon(v_1)).$$

Per consegüent, l'únic que hem de fer és realitzar un canvi de la forma $w' = \pi'^3 z_1$, i obtindre $z_1^2 = a_0(v_1^3+\pi\pi'^{-6}Q(\pi'^2 v_1))$ una corba el·líptica amb reducció estable. Però això correspon a transformar la corba el·líptica $w'^2 = a_0 P_1(u)$ en una corba amb reducció estable, mitjançant el canvi $u - b = \pi'^2 a_0^{-1} v_1$ i $w' = \pi'^3 a_0^{-1} z_1'$, $z_1'^2 = Q_1(v_1)$. Reducció estable implica $\varrho_L(Q_1) = 0$. Com hem vist en el lema 6.3.11, aquest canvi transforma ϱ_L de la forma, $0 = \varrho_L(Q_1) = -2\nu_L(\pi') + \varrho_L(a_0 P_1) = -2\nu_L(\pi') + n' r_K$. Llavors $\pi' = t_n^{2r}$ i els canvis queden $u = b + a_0^{-1} t_n^{2r} v_1, w = c a_0^{-1} t_n^{3r} z_1$ i aleshores $z_1 = Q_1(v_1)(1 + \varepsilon(v_1))$, amb $Q_1(v_1) \in R_L$, $\overline{Q_1}(v_1) = v_1^3 + \alpha_{12} v_1 + \alpha_{13} \in k[v_1]$, i

$$\varepsilon(v_1) \in \wp_L[v_1].$$

L'equació $z_1^2 = \overline{Q_1}(v_1)$ defineix E_1 i es compleix que v_1 té els seus pols a $E_1 \cap E_2$. A més, $\overline{\tau}(v_1) = e_n^{-2r} v_1$ i $\overline{\tau}(z_1) = e_n^{-3r} z_1$.

Obtenim els resultats corresponents a E_2 reemplaçant r per $d-r$, ja que $\varrho(a_0P_2) = \nu(a_0) + (d_K - \varrho(a_0P_1)/2)$. Això implica en particular que $\overline{\tau}^n = 1$, d'on $[L:K] = n$. □

Corol·lari 6.3.14. *Suposem que* $2 \not| \nu(J_2)$. *Tenim que* $d_K + \nu(a_0) = 2r_K$. *Si* m *és el minim denominador de* d_K, *i* $r = md_K$. *Aleshores* $[L:K] = 2m$, *i*

$$\overline{\tau}^2(v_i) = e_m^{-2r} v_i, \quad \overline{\tau}^2(z_i) = e_m^{-3r} z_i.$$

Demostració. Siga $K' = K[t_2] = K[J_2^{1/2}] \subset L$. considerem la nostra corba definida en K'. Com que, pel lema 6.3.10, $\overline{\tau}$ permuta E_1 i E_2, τ permuta P_1 i P_2. Per tant $\varrho(a_0P_1) = \varrho(a_0P_2)$, i $\varrho_{K'}(a_0P_1) = \varrho_{K'}(a_0P_2)$. Aplicant el lema 6.3.12 a K', on $2|\nu_{K'}(J_2)$, obtenim $d_{K'} + \nu_{K'}(a_0) = 2r_{K'}$. Multiplicant per $[K:K'] = 2$ obtenim la primera igualtat $d_K + \nu_K(a_0) = 2r_K$.

Si $r_{K'} = r/m$, $d_{K'} = 2r/m - \nu_{K'}(a_0) = 2(r - \nu_K(a_0))/m$. Si apliquem el teorema anterior a $C_{K'}$ on $2|\nu_{K'}(J_2)$ obtenim que, $[L:K'] = m$ i

$$\begin{cases} \overline{\tau^2}(z_1) = e_n^{-3r} z_1, & \overline{\tau^2}(v_1) = e_n^{-2r} v_1 \\ \overline{\tau^2}(z_2) = e_n^{-3(d-r)} z_2 = e_n^{-3r} z_2, & \overline{\tau^2}(v_2) = e_n^{-2(d-r)} v_2 = e_n^{-2r} v_2 \end{cases}$$

τ^2 és el generador de $\mathrm{Gal}(L/K')$ i $[L:K'][K':K] = 2m$. □

6.4 Taules de models minimals

Per acabar només queda utilitzar la maquinaria desenvolupada per Viehweg [36] per trobar el model minimal a través del model estable. Tots els inputs necessaris; tipus de model estable, espessor de les singularitats, grau de l'extensió $L : K$, acció de $\mathrm{Gal}(L/K)$ sobre $\widetilde{\mathfrak{C}}$, la naturalesa de $\overline{\omega}$; ja els hem trobat en funció dels invariants afins i projectius de l'equació hiperel·líptica6.1.1, en les anteriors seccions d'aquesta exposició o ens els capítols anteriors 4, 5. Les taules són pel cas moderadament ramificat, pel cas de ramificació salvatge hi ha un algoritme alternatiu i ens adrecem a [14].

Ara mostrarem les taules, corresponents a cada tipus de model estable, on es mostra el tipus de model minimal, que denotarem $\mathfrak{X}$, en funció de $n = [L : K]$, r, q i d dels anteriors teoremes.

Cas $\widetilde{\mathfrak{C}}$ llisa.

n	$\overline{r} \in \mathbb{Z}/n\mathbb{Z}$	$\overline{q} \in \mathbb{Z}/n\mathbb{Z}$	$\mathfrak{X}$	Φ
1			$[I_{0-0-0}]$	0
2	0		$[I^*_{0-0-0}]$	$(2)^4$
	1		$[II]$	0
3			$[III]$	$(3)^2$
4			$[VI]$	$(2)^2$
5	1		$[IX-3]$	(5)
	2		$[IX-1]$	
	3		$[IX-4]$	
	4		$[IX-2]$	
6	1	0	$[V]$	(3)
	5	3		
	1	3	$[V^*]$	
	5	0		
	2 ó 4		$[IV]$	0
8		1 ó 3	$[VII^*]$	(2)
		5 ó 7	$[VII]$	
10	2		$[VIII-1]$	0
	4		$[VIII-3]$	
	6		$[VIII-2]$	
	8		$[VIII-4]$	

Cas $\widetilde{\mathfrak{C}}$ irreductible amb un únic punt doble ordinari.

Siga d l'espessor d'aquest punt.

n	$\overline{r} \in \mathbb{Z}/n\mathbb{Z}$	$\overline{q} \in \mathbb{Z}/n\mathbb{Z}$	$\mathfrak{X}$	Φ
1			$[I_{d-0-0}]$	(d)
2	0		$[I^*_{d/2-0-0}]$	$(2)^2 \times H_{d/2}$
	1	0	$[II^*_{d/2-0}]$	0
	1	1	$[II_{d/2-0}]$	$(2d)$
3	1		$[IV - II_{(d-2)/3}]$	(d)
	2		$[IV - II_{(d-2)/3}]$	
4	1	1	$[III - II_{(d-2)/4}]$	(d/2)
	1	3	$[III^* - II^*_{(d-2)/4}]$	(8)
	3	1	$[III - II^*_{(d-2)/4}]$	
	3	3	$[III^* - II_{(d-2)/4}]$	(d/2)
6	2		$[II^* - II^*_{(d-4)/6}]$	$H_{(d+2)/6}$
	4		$[II - II^*_{(d-2)/6}]$	$H_{(d+4)/6}$

Cas $\widetilde{\mathfrak{C}}$ irreductible amb un dos punts dobles ordinaris.

Siguin d_i els espessors dels seus punts singulars. Si $n = 4$, o bé si $n = 2$, $r = 1$ i $f^{-1}(\overline{\omega}) \subset (\widetilde{\mathfrak{C}})_{\text{reg}}$, tenim que $d_1 = d_2$.

n	$\overline{r} \in \mathbb{Z}/n\mathbb{Z}$	$f^{-1}(\overline{\omega})$	$\mathfrak{X}$	Φ
1			$[I_{d_1-d_2-0}]$	$(d_1) \times (d_2)$
2	0		$[I^*_{d_1/2-d_2/2-0}]$	$H_{d_1/2} \times H_{d_2/2}$
	1	$\subset (\widetilde{\mathfrak{C}})_{\text{reg}}$	$[2I_{d_1} - 0]$	(d_1)
	1	singular	$[II_{d_1/2-d_2/2}]$	$(d_1) \times (2)$ si $8 \mid (d_1 d_2 - 4)$
				$(2d_1)$ si no
4			$[III_{d_1/2}]$	$H_{d_1/2}$

Cas $\widetilde{\mathfrak{C}}$ és la unió de dues rectes projectives que es tallen transversalment en tres punts. Siguin d_i els espessors dels seus punts singulars. Si $n = 3$ ó 6, tenim $d_1 = d_2 = d_3$. Si $n = 2$ i $r = 1$, dos dels d_i són iguals. Denotem e_1 aquest valor i e_2 el valor de la tercera espessor. Denotem $g = d_1d_2 + d_1d_3 + d_3d_2$ i $h = \gcd(d_1, d_2, d_3)$.

n	$\overline{r} \in \mathbb{Z}/n\mathbb{Z}$	$\overline{q} \in \mathbb{Z}/n\mathbb{Z}$	$\mathfrak{X}$	Φ
1			$[I_{d_1-d_2-d_3}]$	$(h) \times (h^{-1}g)$
2	0		$[I^*_{d_1/2-d_2/2-d_3/2}]$	$H_{g/4} \times H_{\gcd(2,h/2)}$
	1	0	$[II^*_{e_1/2-e_2}]$	(e_2)
	1	1	$[II_{e_1/2-e_2}]$	$(2e_1 + e_2)$
3			$[III_{d_1}]$	$(3)^2$ si $3\|d_1$
				(9) si no
6			$[III^*_{d_1/2}]$	0

Cas $\widetilde{\mathfrak{C}}$ és la unió de dues corbes el·líptiques i $2|\nu(J_2)$. Siga d l'espessor del punt d'intersecció.

n	$\overline{r} \in \mathbb{Z}/n\mathbb{Z}$	$\overline{d} \in \mathbb{Z}/n\mathbb{Z}$	$\mathfrak{X}$	Φ
1			$[I_0 - I_0 - d]$	0
2	0		$[I_0^* - I_0^* - (d-2)/2]$	$(2)^4$
	1		$[I_0 - I_0^* - (d-1)/2]$	$(2)^2$
3	0		$[IV - IV^* - (d-3)/3]$	$(3)^2$
	1	0 ó 1	$[I_0 - IV - (d-1)/3]$	(3)
		2	$[IV^* - IV^* - (d-4)/3]$	$(3)^2$
	2	0 ó 2	$[I_0 - IV^* - (d-2)/3]$	(3)
		1	$[IV - IV - (d-2)/3]$	$(3)^2$
4	0		$[III - III^* - (d-4)/4]$	$(2)^2$
	1	0 ó 1	$[I_0 - III - (d-1)/4]$	(2)
		2 ó 3	$[I_0^* - III^* - (d-5)/4]$	$(2)^3$
	2	1	$[III - III - (d-2)/4]$	$(2)^2$
		3	$[III^* - III^* - (d-6)/4]$	$(2)^2$
	3	0 ó 3	$[I_0 - III^* - (d-3)/4]$	(2)
		1 ó 2	$[I_0^* - III - (d-3)/4]$	$(2)^3$
6	0		$[II - II^* - (d-6)/6]$	0
	1	0 ó 1	$[I_0 - II - (d-1)/6]$	0
		2 ó 5	$[II^* - IV - (d-7)/6]$	(3)
		3 ó 4	$[I_0^* - IV^* - (d-7)/6]$	$(2)^2 \times (3)$
	2	1	$[II - II - (d-2)/6]$	0
		3 ó 5	$[I_0^* - II^* - (d-8)/6]$	$(2)^2$
	3	1 ó 2	$[II - IV - (d-3)/6]$	(3)
		4 ó 5	$[II^* - IV^* - (d-9)/6]$	
	4	1 ó 3	$[I_0^* - II - (d-4)/6]$	$(2)^2$
		5	$[II^* - II^* - (d-10)/6]$	0
	5	0 ó 5	$[I_0 - II^* - (d-5)/6]$	0
		1 ó 4	$[II - IV^* - (d-5)/6]$	(3)
		3 ó 2	$[I_0^* - IV - (d-5)/6]$	$(2)^2 \times (3)$
12	1	3 ó 10	$[II^* - III - (d-13)/12]$	(2)
		4 ó 9	$[IV - III^* - (d-13)/12]$	(6)
	5	2 ó 3	$[II - III - (d-5)/12]$	(2)
		8 ó 9	$[IV^* - III^* - (d-17)/12]$	(6)
	7	3 ó 4	$[IV - III - (d-7)/12]$	(6)
		9 ó 10	$[II^* - III^* - (d-19)/12]$	(2)
	11	3 ó 8	$[IV^* - III - (d-11)/12]$	(6)
		2 ó 9	$[II - III^* - (d-11)/12]$	(2)

Cas $\widetilde{\mathfrak{C}}$ és la unió de dues corbes el·líptiques i $2 \not| \nu(J_2)$. Els enters m i r són els definits en el corol·lari 6.3.14. Per tant, segons aquest $n = 2m$ i $d = 2r$, d l'espessor del punt d'intersecció.

n	$\overline{r} \in \mathbb{Z}/n\mathbb{Z}$	$\mathfrak{X}$	Φ
2		$[2I_0 - (r-1)]$	0
4		$[2I_0 - (r-1)/2]$	$(2)^2$
6	1	$[2IV - (r-1)/3]$	(3)
	2	$[2IV^* - (r-2)/2]$	
8	1	$[2III - (r-1)/4]$	(2)
	3	$[2III^* - (r-3)/4]$	
12	1	$[2II - (r-1)/6]$	0
	5	$[2II^* - (r-5)/6]$	

Cas $\widetilde{\mathfrak{C}}$ és la unió de dues corbes racionals que es tallen en un únic punt. d és el espessor del punt d'intersecció, d_1, d_2 els espessors dels punts singulars de les corbes racionals. Si $n = 2$, $2|\nu(J_2)$ i d imparell, aleshores e_1 i e_2 són els enters que verifiquen $\{e_1, e_2\} = \{d_1, d_2\}$. Si $2 \not| \nu(J_2)$, tenim $d_1 = d_2$.

n	$\nu(J_2)$	$\overline{d} \in \mathbb{Z}/n\mathbb{Z}$	$\mathfrak{X}$	Φ
1			$[I_{d_1} - I_{d_2} - d]$	$(d_1) \times (d_2)$
2	$\in 2\mathbb{Z}$	0	$[I^*_{d_1/2} - I^*_{d_2/2} - (d-2)/2]$	$H_{d_1/2} \times H_{d_2/2}$
		1	$[I_{e_1/2} - I^*_{e_2/2} - (d-1)/2]$	$(e_1/2) \times H_{e_2/2}$
	$\notin 2\mathbb{Z}$		$[2I_{d_1} - d/2]$	(d_1)
4	$\notin 2\mathbb{Z}$		$[2I^*_{d_1} - (d-2)/2]$	$H_{d_1/2}$

Cas $\widetilde{\mathfrak{C}}$ la unió d'una corba el·líptica i una corba racional.

n	$\overline{d} \in \mathbb{Z}/n\mathbb{Z}$	$\overline{r} \in \mathbb{Z}/n\mathbb{Z}$	$\mathfrak{X}$	Φ
1			$[I_{d_1} - I_0 - d]$	(q)
2	0		$[I_0^* - I_{d_1}^* - (d-2)/2]$	$(2)^2 \times H_q$
	1		veure (4.4)	
3	1		$[IV - I_{d_1} - (d-1)/3]$	$(3) \times (q)$
	2		$[IV^* - I_{d_1} - (d-2)/3]$	
4	1	0 ó 1	$[III - I_{d_1} - (d-1)/4]$	$(2) \times (q)$
		2 ó 3	$[III^* - I_{d_1}^* - (d-5)/4]$	$(2) \times H_q$
	3	0 ó 3	$[III^* - I_{d_1} - (d-3)/4]$	$(2) \times (q)$
		1 ó 2	$[III - I_{d_1}^* - (d-3)/4]$	$(2) \times H_q$
6	1	0 ó 1	$[II - I_{d_1} - (d-1)/6]$	$(3) \times H_q$
		3 ó 4	$[IV^* - I_{d_1}^* - (d-7)/6]$	$(3) \times H_q$
	2		$[II^* - I_{d_1}^* - (d-8)/6]$	H_q
	4		$[II^* - I_{d_1}^* - (d-4)/4]$	
	5	0 ó 5	$[II^* - I_{d_1} - (d-5)/6]$	(q)
		3 ó 2	$[IV - I_{d_1}^* - (d-5)/6]$	$(3) \times H_q$

Capítol 7

El conductor de una curva de género 2 y las imágenes de las representaciones de Galois asociadas a su variedad Jacobiana

Sara Arias de Reyna[1]

7.1 Introducción

Sea A una variedad abeliana definida sobre un cuerpo de números K. Fijemos un número primo l. Podemos considerar el conjunto de los puntos de l-torsión de A,

$$A[l] = \{P \in A(\overline{K}) : \underbrace{P + \cdots + P}_{l \text{ veces}} = O\}.$$

Este conjunto es claramente un subgrupo del grupo de los puntos $\overline{K}$-definidos de A; de hecho, es isomorfo al pro-

[1]Dep. Àlgebra i Geometria, Universitat de Barcelona. E-mail: ariasdereyna@ub.edu

ducto de $2d$ copias de $\mathbb{Z}/l\mathbb{Z}$, donde d es la dimensión de la variedad A. El grupo de Galois absoluto de K actúa de forma natural sobre este grupo, dando lugar a una representación

$$\overline{\rho}_l : \mathrm{Gal}(\overline{K}|K) \to \mathrm{Aut}(A[l]) \simeq \mathrm{GL}_{2d}(\mathbb{F}_l).$$

Debido al criterio de Néron-Ogg-Shafarevich, esta representación es no ramificada en los primos de buena reducción de A diferentes de l. De forma más precisa, se puede definir un número, el conductor de A, que refleja el comportamiento de la representación de Galois l-ádica asociada al módulo de Tate de A sobre los grupos de inercia en los distintos primos (lo veremos en la sección 7.2).

Un problema interesante es el estudio de las imágenes de estas representaciones. Concretamente, se plantea la cuestión de investigar si estas representaciones tienen imágenes grandes.

Cuando la variedad abeliana A está principalmente polarizada, el pairing de Weil da lugar a una forma simpléctica no degenerada sobre $A[l]$, y las imágenes de los elementos de $\mathrm{Gal}(\overline{K}|K)$ se comportan bien respecto de esta forma simpléctica. Se deduce así que la imagen de $\overline{\rho}_l$ está contenida en el grupo general simpléctico $\mathrm{GSp}_{2d}(\mathbb{F}_l)$.

En [30], J-P. Serre estudia las imágenes de las representaciones de Galois asociadas a una variedad abeliana A definida sobre un cuerpo de números K, principalmente polarizada, y tal que $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. En particular, prueba el siguiente resultado:

Teorema 7.1.1 (Serre). *Sea K un cuerpo de números, y A/K una superficie abeliana principalmente polarizada tal que* $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. *Entonces, para todo número primo l salvo para una cantidad finita, se verifica que*

$$\mathrm{Im}\overline{\rho}_l = \mathrm{GSp}_4(\mathbb{F}_l).$$

Ante este resultado, surge el problema de determinar, dada una superficie concreta A/K y un número primo l, si para este primo la imagen de $\overline{\rho}_l$ coincide con $\mathrm{GSp}_4(\mathbb{F}_l)$. En este capítulo vamos a describir un método, debido a L. Dieulefait [8], que, dada una superficie abeliana A sobre $\mathbb{Q}$, principalmente polarizada, proporciona un conjunto finito de números primos, de forma que cualquier primo l fuera de este conjunto satisface la igualdad $\mathrm{Im}\overline{\rho}_l = \mathrm{GSp}_4(\mathbb{F}_l)$. Para aplicar este método, es necesario conocer una cota del conductor de A.

Dedicaremos la primera sección a definir el conductor de una variedad abeliana. Cuando C es una curva lisa, geométricamente conexa y de género $g \geq 1$, podemos definir su conductor a partir del conductor de su variedad Jacobiana $J(C)$.

En la siguiente sección veremos cómo el conductor de una curva C de género 2 se relaciona con su discriminante minimal $\Delta_{\min}(C)$, lo cual permitirá aplicar los resultados expuestos en los capítulos anteriores para obtener información sobre el conductor.

Finalmente, en la última sección haremos algunos comentarios sobre el método de L. Dieulefait. Daremos, a grandes rasgos, una visión general del método, y luego mostraremos un ejemplo concreto. Tomaremos una curva de

género 2 definida sobre $\mathbb{Q}$ y veremos cómo el método nos permite afirmar en este caso que, para todo primo $l > 3$ y distinto de 587, la imagen de la representación $\overline{\rho}_l$ asociada a los puntos de l-torsión de la variedad Jacobiana de esta curva coincide con el grupo general simpléctico $\mathrm{GSp}_4(\mathbb{F}_l)$.

7.2 El conductor de una curva y de una variedad abeliana

Sea p un número primo, y K una extensión finita del cuerpo $\mathbb{Q}_p$ de los números p-ádicos. Denotaremos por v a la normalización de la extensión a K de la valoración p-ádica, R_v a su anillo de enteros y k a su cuerpo residual.

Consideremos una variedad abeliana A de dimensión d definida sobre K. En esta sección vamos a definir un número f, que denominaremos el exponente del conductor de A. Esta definición se realizará a través de la representación de Galois asociada al módulo de Tate de A.

Sea l un número primo distinto de p. Para cada número natural n, denotemos por $A[l^n]$ al conjunto de los puntos de l^n-torsión definidos sobre una clausura algebraica $\overline{K}$ de K.

El módulo de Tate de A es el $\mathbb{Z}_l$-módulo

$$T_l(A) = \varprojlim_n A[l^n].$$

La acción del grupo de Galois $\mathrm{Gal}(\overline{K}|K)$ sobre los puntos de torsión de A induce una acción sobre $T_l(A)$. Si consideramos el $\mathbb{Q}_l$-espacio vectorial $V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, obtenemos una representación

$$\rho_l : \mathrm{Gal}(\overline{K}|K) \to \mathrm{GL}(V_l(A)) \simeq \mathrm{GL}_{2d}(\mathbb{Q}_l).$$

Esta representación es continua, si consideramos la topología de Krull sobre $\mathrm{Gal}(\overline{K}|K)$ y la topología inducida por $V_l(A)$ sobre $\mathrm{GL}(V_l(A))$.

Queremos definir un invariante que de alguna forma mida cómo es la acción del grupo de inercia sobre $V_l(A)$. Re-

cordemos que el grupo de inercia se define como

$$I(\overline{K}|K) = \{\sigma \in \mathrm{Gal}(\overline{K}|K) \text{ tales que } v(\sigma(x) - x) > 0 \text{ para todo } x \in R_v\}.$$

Denotemos por I al grupo de inercia, y por $V_l(A)^I$ al conjunto de los elementos de $V_l(A)$ que quedan invariantes por la acción de I, es decir,

$$V_l(A)^I = \{v \in V_l(A) : \rho_l(\sigma)(v) = v \text{ para todo } \sigma \in I\}.$$

Una forma de medir el tamaño de $\rho_l(I)$ es considerar la dimensión de $V_l(A)^I$ como $\mathbb{Q}_l$-espacio vectorial.

Definición 7.2.1. Se define el *exponente del conductor moderado* de A como

$$\varepsilon(A/K) = \dim V_l(A) - \dim V_l(A)^I.$$

Observación 7.2.2.

- $\varepsilon(A/K)$ no depende del primo $l \neq p$ escogido.
- Cuando ρ_l es no ramificada, es decir, cuando $\rho_l(I)$ es trivial, $\varepsilon(A/K) = 0$.

Consideremos ahora una extensión de Galois finita, digamos $L|K$. Denotemos por w a la normalización de la única extensión de la valoración de $\mathbb{Q}_p$ a L, y por $R_w \subset L$ al anillo de los enteros de w. Podemos definir una sucesión decreciente de subgrupos del grupo de inercia de $L|K$, del modo siguiente:

Definición 7.2.3. Para cada $i \in \mathbb{N}$, se define el *i-ésimo grupo de ramificación superior* de la extensión $L|K$ como

$$G_i = \{\sigma \in \mathrm{Gal}(L|K) \text{ tales que } w(\sigma(x)-x) \geq i+1 \text{ para todo } x \in R_w\}.$$

Observación 7.2.4. La definición anterior nos proporciona una filtración del grupo de inercia I de $L|K$,

$$I = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_i \supset \cdots$$

Supongamos ahora que

$$\overline{\rho}_l : \mathrm{Gal}(L|K) \to \mathrm{GL}(V)$$

es una representación de Galois, donde V es un $\mathbb{F}_l$-espacio vectorial de dimensión finita. Para cada $i \geq 1$, denotemos por V_i al subconjunto de V formado por los elementos que quedan fijos por la acción de G_i. Podemos entonces definir el siguiente número, que mide la acción del grupo de Galois de $L|K$ sobre los grupos de ramificación superior.

Definición 7.2.5. Se define el *exponente del conductor de Swan* de $\overline{\rho}_l$ como

$$\mathrm{sw}(\overline{\rho}_l) = \sum_{i \geq 1} \frac{g_i}{g_0} \dim_{\mathbb{F}_l}(V/V_i),$$

donde g_i denota el cardinal del i-ésimo grupo de ramificación superior.

Observación 7.2.6.

- Esta definición no depende del primo $l \neq p$ escogido.
- El exponente del conductor de Swan es un número entero mayor o igual que 0 (ver [26], § I).

Volvamos de nuevo a considerar una variedad abeliana A/K, y un primo l distinto de p. El grupo de Galois $\mathrm{Gal}(\overline{K}|K)$ actúa sobre los puntos de l-torsión de A, dando lugar a una representación

$$\overline{\rho}_l : \mathrm{Gal}(\overline{K}|K) \to \mathrm{GL}(A[l]) \simeq \mathrm{GL}_{2d}(\mathbb{F}_l).$$

Naturalmente, la extensión $\overline{K}|K$ es infinita, así que no podemos aplicar directamente la definición del exponente del conductor de Swan. Sin embargo, el cuerpo fijo de $\overline{K}$ por el núcleo de $\overline{\rho}_l$ es una extensión de Galois finita de K, generada por las coordenadas de los puntos de l-torsión, que denotaremos $K(A[l])$.

Luego la representación $\overline{\rho}_l$ da lugar a una representación inyectiva (que seguimos denotando igual)

$$\overline{\rho}_l : \mathrm{Gal}(K(A[l])|K) \to \mathrm{GL}(A[l]) \simeq \mathrm{GL}_{2d}(\mathbb{F}_l).$$

Definición 7.2.7. Sea K una extensión finita de $\mathbb{Q}_p$, y sea A una variedad abeliana definida sobre K. Se define el *exponente del conductor* de A como

$$f(A/K) = \varepsilon(A/K) + \mathrm{sw}(\overline{\rho}_l),$$

donde l es un primo distinto de p.

Observación 7.2.8. El exponente del conductor de A es un número entero mayor o igual que cero y no depende del primo $l \neq p$ escogido, ya que cada uno de los sumandos que lo componen satisface estas propiedades.

De este modo hemos definido, para cada variedad abeliana A/K, un número, $f(A/K)$, a través de la acción del grupo de Galois absoluto de K sobre el grupo de los puntos de A.

Observación 7.2.9. Aunque la medida de la ramificación salvaje $\mathrm{sw}(\overline{\rho}_l)$ se ha definido a partir de la representación asociada a los puntos de l-torsión, también podría haberse definido directamente a partir de la representación l-ádica asociada al módulo de Tate. Véase [29], § 2.1.

Supongamos ahora que tenemos una curva lisa, geométricamente conexa, de género $g \geq 1$, digamos C, definida sobre K. Podemos asociar a C una representación de $\mathrm{Gal}(\overline{K}|K)$ a través de los grupos de cohomología l-ádica. En efecto, para cada primo $l \neq p$, el grupo de Galois absoluto de K actúa sobre el $\mathbb{Q}_l$-espacio vectorial de dimensión finita $\mathrm{H}^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Q}_l)$, lo cual nos proporciona una representación continua

$$\rho_l : \mathrm{Gal}(\overline{K}|K) \to \mathrm{Aut}(\mathrm{H}^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Q}_l)).$$

De forma parecida a lo que acabamos de ver, se puede asociar a esta representación un exponente del conductor, que será por definición el exponente del conductor de C/K. No entraremos ahora en los detalles (ver [29], § 2.1). Observemos, no obstante, que el exponente del conductor así obtenido coincide con el exponente conductor de la variedad Jacobiana de C, considerada como variedad abeliana, ya que $\mathrm{H}^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Q}_l) \simeq V_l(J(C))$ como $\mathrm{Gal}(\overline{K}|K)$-módulos (ver [15], § 1.1).

Observación 7.2.10. Sea A una variedad abeliana definida sobre $\mathbb{Q}$. Para cada primo p hemos definido el exponente del conductor de A en p (considerando A como una variedad abeliana definida sobre $\mathbb{Q}_p$). Se define el *conductor* de A como el producto

$$f(A/\mathbb{Q}) = \prod_{p \text{ primo}} p^{f(A/\mathbb{Q}_p)}.$$

Observemos que, para todos los primos salvo para un número finito, $f(A/\mathbb{Q}_p) = 0$, y por tanto el producto anterior es un producto finito.

7.3 El conductor de una curva de género 2 y el discriminante minimal

En esta sección vamos a enunciar un teorema de Liu (ver [15], Teorema 1) que relaciona el exponente del conductor de una curva de género 2 con su discriminante minimal y otros datos de la curva.

Como en la sección anterior, denotamos por K a una extensión finita de $\mathbb{Q}_p$, v a la normalización de la extensión a K de la valoración p-ádica, R_v al anillo de los enteros de v y k al cuerpo residual de K.

Consideremos una curva C definida sobre K, lisa y proyectiva, geométricamente conexa, de género 2.

Vamos a definir una noción de discriminante minimal, $\Delta_{\min}(C)$, a partir del haz dualizante del modelo minimal regular de C. En general, $\Delta_{\min}(C)$ será diferente de $\Delta_0(C)$ (ver la sección 5 del Capítulo 5).

Recordemos que C es una curva hiperelíptica, y por tanto admite una ecuación entera (ver la Definición 5.2 del capítulo 5). Con más generalidad, aquí consideraremos ecuaciones hiperelípticas de la forma

$$y^2 + Q(x)y = P(x), \tag{7.3.1}$$

donde permitimos que $P(x)$ y $Q(x)$ tengan coeficientes en K. El discriminante minimal $\Delta_{\min}(C)$ se definirá como el discriminante asociado a una cierta ecuación de esta forma.

Dada una ecuación (7.3.1), podemos considerar las dos formas diferenciales siguientes:

$$\omega_1 = \frac{\mathrm{d}x}{2y + Q(x)}, \quad \omega_2 = \frac{x\mathrm{d}x}{2y + Q(x)}.$$

Estas dos formas diferenciales son holomorfas en C, y forman una base de $H^0(C, \Omega^1_{C/K})$ sobre K.

Sea $\mathfrak{C}_{\min}$ el modelo minimal regular de C (ver la Sección 3 del Capítulo 2), y $\omega_{\mathfrak{C}_{\min}/\mathrm{Spec}R_v}$ el haz dualizante (ver [17], Definición 4.18, Capítulo 6). La restricción a C da lugar a una aplicación inyectiva

$$H^0(\mathfrak{C}_{\min}, \omega_{\mathfrak{C}_{\min}/\mathrm{Spec}R_v}) \hookrightarrow H^0(C, \Omega^1_{C/K}).$$

De esta forma, podemos ver $H^0(\mathfrak{C}_{\min}, \omega_{\mathfrak{C}_{\min}/\mathrm{Spec}R_v})$ como un R_v-submódulo de $H^0(C, \Omega^1_{C/K})$.

Definición 7.3.1. Una *ecuación minimal* de C es una ecuación hiperelíptica (7.3.1) tal que el conjunto de las formas diferenciales asociadas $\{\omega_1, \omega_2\}$ es una base del R_v-módulo
$H^0(\mathfrak{C}_{\min}, \omega_{\mathfrak{C}_{\min}/\mathrm{Spec}R_v})$. El *discriminante minimal* $\Delta_{\min}(C)$ es el discriminante de una ecuación minimal de C.

Observación 7.3.2.

- La definición de discriminante minimal es independiente de la ecuación minimal escogida, salvo producto por unidades de R_v.
- Una ecuación minimal no tiene por qué tener coeficientes en R_v. Sin embargo, sí es cierto que la valoración del discriminante minimal es mayor o igual que 0 (ver [15], Nota 3).

Observación 7.3.3. En cualquier caso, si Δ es el discriminante asociado a una ecuación hiperelíptica entera para C, entonces $v(\Delta) \geq v(\Delta_{\min})$, de forma que la valoración del discriminante minimal, según lo acabamos de definir, es siempre menor o igual que la valoración del discriminante minimal $\Delta_0(C)$ según la Definición 5.2 del Capítulo

5. Claramente, si C admite una ecuación minimal entera, estas dos nociones de discriminante coinciden.

Observación 7.3.4. Cuando el anillo R_v es estrictamente henseliano, se puede expresar de forma muy precisa la relación entre $\Delta_{\min}(C)$ y $\Delta_0(C)$ (ver el Teorema 2 de [15]). En particular, cuando la fibra especial del modelo canónico es íntegra (y según el Lema 3.4 del Capítulo 5, esto ocurre en los casos I, II, III, IV del Teorema 3.2 del Capítulo 5), las dos nociones de discriminante minimal coinciden.

Consideremos ahora el henselianizado estricto R_v^{sh} de R_v (ver la sección 2 del Capítulo 5), que es también un anillo de valoración discreta, y sea K^{sh} su cuerpo de fracciones. Consideremos la curva $C' = C \times_K K^{\mathrm{sh}}$, y sea $\mathfrak{C}'_{\min}$ el modelo minimal regular de C'.

Vamos a definir un esquema $\mathfrak{Z}$ sobre $\mathrm{Spec} R_v^{\mathrm{sh}}$ a partir de $\mathfrak{C}'_{\min}$. Estaremos interesados en el número de componentes irreducibles de la fibra especial de su desingularización minimal.

Denotemos por $\Gamma_1, \ldots, \Gamma_n$ a las componentes conexas de la fibra especial $\mathfrak{C}'_{\min,\mathfrak{p}}$. Para cada subconjunto E de $\{\Gamma_1, \ldots, \Gamma_n\}$, existe un morfismo de contracción

$$\pi : \mathfrak{C}'_{\min} \to Y,$$

es decir, un morfismo propio con fibras conexas de $\mathfrak{C}'_{\min}$ en un esquema normal proyectivo Y sobre $\mathrm{Spec} R_v^{\mathrm{sh}}$ tal que $\pi(E)$ es un conjunto finito de puntos cerrados y el morfismo inducido entre $\mathfrak{C}'_{\min} - E$ y $Y - \pi(E)$ es un isomorfismo.

En particular, consideremos el conjunto E de las componentes conexas Γ_i que verifican las dos condiciones siguientes:

- $p_a(\Gamma_i) = 0$
- $\Gamma_i^2 = -2$

y sea $\pi : \mathfrak{C}'_{\min} \to \mathfrak{C}'_{\text{can}}$ el morfismo de contracción correspondiente (ver la Definición 4.3 del Capítulo 2).

Como C' es una curva de género 2, es hiperelíptica, así que podemos considerar la involución hiperelíptica σ. Esta involución se extiende a un automorfismo de $\mathfrak{C}'_{\min}$. Más aún, σ deja invariante el conjunto E, y por tanto da lugar a un automorfismo de $\mathfrak{C}'_{\text{can}}$. Definimos $\mathfrak{Z}$ como el cociente $\mathfrak{C}'_{\text{can}}/\langle\sigma\rangle$ (ver también la sección 3 del Capítulo 5).

Consideremos ahora la desingularización minimal $\widetilde{\mathfrak{Z}} \to \mathfrak{Z}$, y supongamos que la fibra especial $\widetilde{\mathfrak{Z}}_{\mathfrak{p}}$ tiene d componentes conexas. Estamos ya en condiciones de enunciar el teorema.

Teorema 7.3.5. *Sea C una curva definida sobre una extensión finita K de $\mathbb{Q}_p$, lisa y proyectiva, geométricamente conexa, de género 2. Entonces, con las notaciones introducidas en esta sección, tenemos que el exponente del conductor f de C/K se expresa como*

$$f(C/K) = v(\Delta_{\min}(C)) - \frac{d-1}{2} - n + 1.$$

Observación 7.3.6. Cuando $p \neq 2$, el número d está completamente determinado en función del tipo geométrico de $\mathfrak{C}'_{\min}$ (ver las proposiciones 7 y 8 de [15]). Es decir, es suficiente calcular el tipo numérico de C' (en otras palabras, la fibra especial $\mathfrak{C}'_{\min,\mathfrak{p}}$, ver la sección 3 del capítulo 6), y el número de componentes irreducibles de la reducción estable $\widetilde{\mathfrak{C}'}$ (ver el Capítulo 4, Teorema 3.1).

7.4 Imágenes de representaciones de Galois de Jacobianas de curvas de género 2

Sea A una superficie abeliana definida sobre $\mathbb{Q}$, principalmente polarizada, y tomemos un primo l de buena reducción. La pregunta que nos planteamos es la siguiente:

¿Coincide la imagen de $\overline{\rho}_l$ con $\mathrm{GSp}_4(\mathbb{F}_l)$?

En [8], L. Dieulefait propone un método que responde a esta pregunta para todos los primos l de buena reducción salvo para un conjunto finito. En esta sección vamos a exponer algunas de las ideas que intervienen en este método y veremos un ejemplo concreto.

Consideremos un primo p distinto de l, donde A tenga buena reducción. Como la proyección natural

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$$

es sobreyectiva, existe un elemento $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ que se aplica en el elemento de Frobenius de $\mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$. Este elemento Frob_p es único salvo multiplicación por elementos del grupo de inercia $I_p = I(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$. Ahora bien, como A tiene buena reducción en p, el criterio de Néron-Ogg-Shafarevich afirma que la imagen por $\overline{\rho}_l$ de I_p es trivial (ver [31], Teorema 1). Por tanto, el elemento $\overline{\rho}_l(\mathrm{Frob}_p)$ de $\mathrm{Im}\overline{\rho}_l$ está bien definido independientemente de la elección de Frob_p.

Ahora bien, $\overline{\rho}_l(\mathrm{Frob}_p)$ es un elemento de $\mathrm{GSp}_4(\mathbb{F}_l)$, así que podemos considerar su polinomio característico, que

será de la forma

$$\mathrm{Pol}_p(x) = x^4 - a_p x^3 + b_p x^2 - p a_p x + p^2,$$

para ciertos $a_p, b_p \in \mathbb{Q}$.

Cuando A es la variedad Jacobiana asociada a una curva C de género 2 definida sobre $\mathbb{Q}$, podemos determinar a_p y b_p a partir de la curva reducida $\widetilde{C}$ en p, del modo siguiente:

$$\begin{cases} a_p = p + 1 - N_1 \\ b_p = (N_1^2 + N_2)/2 + p - N_1 - pN_1, \end{cases} \tag{7.4.2}$$

donde

$$N_1 = \mathrm{card}(\widetilde{C}(\mathbb{F}_p))$$
$$N_2 = \mathrm{card}(\widetilde{C}(\mathbb{F}_{p^2}))$$

(ver [27], § 5).

La observación clave para responder a nuestra pregunta es que, si la imagen de $\overline{\rho}_l$ no fuera igual al grupo simpléctico $\mathrm{GSp}_4(\mathbb{F}_l)$, entonces los números a_p y b_p tendrían que satisfacer unas relaciones muy particulares.

En efecto, si la inclusión $\mathrm{Im}\overline{\rho}_l \subset \mathrm{GSp}_4(\mathbb{F}_l)$ es estricta, entonces $\mathrm{Im}\overline{\rho}_l$ debe estar contenida en un subgrupo maximal propio de $\mathrm{GSp}_4(\mathbb{F}_l)$. Esto da lugar a distinguir una serie de casos, según los distintos subgrupos maximales de $\mathrm{GSp}_4(\mathbb{F}_l)$. En cada uno de los casos, Dieulefait encuentra condiciones necesarias que debe satisfacer el par (a_p, b_p). Así pues, si para cada uno de los casos somos capaces de mostrar un primo p de buena reducción, distinto de l, de forma que el par (a_p, b_p) no verifique las condiciones requeridas, podremos asegurar que $\mathrm{Im}\overline{\rho}_l = \mathrm{GSp}_4(\mathbb{F}_l)$.

En primer lugar, se puede distinguir si la imagen de $\overline{\rho}_l$ es reducible o irreducible sobre $\overline{\mathbb{F}}_l$. Si es reducible, puede ocurrir que en la semisimplificación aparezca un bloque de dimensión 1, o que aparezcan dos bloques de dimensión 2. Este último caso, a su vez, se puede separar en dos, según cómo se agrupen las raíces del polinomio característico de $\overline{\rho}_l(\mathrm{Frob}_p)$ dentro de los bloques, para los primos p de buena reducción de A.

Para estudiar el caso en que la imagen de $\overline{\rho}_l$ es irreducible, podemos utilizar la clasificación de Mitchell (ver la sección 2.1 de [8]) de los grupos maximales propios de $\mathrm{PSp}_4(\mathbb{F}_l)$, y distinguir en qué tipo de grupo está contenida la imagen de $\overline{\rho}_l$. Una vez que se aplican estos resultados a la situación que estamos considerando, obtenemos el siguiente esquema:

$$\begin{cases} \text{Caso reducible} \begin{cases} \text{(1) Bloque 1-dimensional} \\ \text{Bloques 2-dimensionales} \begin{cases} \text{(2) relacionados} \\ \text{(3) no relacionados} \end{cases} \end{cases} \\ \text{Caso irreducible} \begin{cases} \text{(4) Estabilizador de una congruencia elíptica o hiperbólica, o de una cuádrica} \\ \text{(5) Casos excepcionales} \end{cases} \end{cases}$$

Por tanto, hay que considerar cada uno de los cinco casos que se indican arriba.

De forma genérica, el planteamiento es el siguiente: supongamos que $\mathrm{Im}(\overline{\rho}_l)$ se encuentra en uno de los casos (1), (2) o (4). Entonces se deduce la existencia de un cierto carácter

$$\varepsilon : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \overline{\mathbb{F}}_l^*$$

En el primer caso, este carácter se obtiene a partir de aquel que da lugar al bloque 1-dimensional; en el segundo caso, aparece relacionado con el determinante de los bloques 2-dimensionales, y en el cuarto caso el carácter viene dado por la forma del subgrupo de $\mathrm{GSp}_4(\mathbb{F}_l)$ que contiene a la imagen de $\overline{\rho}_l$ (necesitamos suponer que l es un primo mayor que 3).

La idea ahora es observar que la ramificación de ε está limitada en función de la ramificación de $\overline{\rho}_l$. Y sobre la ramificación de $\overline{\rho}_l$ tenemos mucha información.

Más concretamente, si denotamos por N al producto de los primos de mala reducción de A, $\overline{\rho}_l$ es no ramificada fuera de $l \cdot N$. Además, debido a unos resultados de Raynaud, la restricción de $\overline{\rho}_l$ al grupo de inercia en l sólo puede ser de una forma muy concreta (ver la sección 2.2 de [8]), lo cual controla la ramificación de $\overline{\rho}_l$ en l. En cuanto a la ramificación en los primos de mala reducción de la superficie A, podemos controlarla a través del conductor de A. Es en este punto donde será esencial conocer cuánto vale este conductor, o al menos poder acotarlo.

Reuniendo toda esta información, podemos concluir que el carácter ε debe pertenecer a un conjunto finito de caracteres. Evaluando cada uno de estos caracteres en un primo p de buena reducción, obtenemos condiciones que tendrían que satisfacer los coeficientes a_p y b_p del polinomio característico de la imagen del elemento de Frobenius en p cuando ε coincide con estos caracteres.

En el caso (3), Dieulefait hace uso de la conjetura de Serre. Concretamente, deduce que cada uno de los bloques 2-dimensionales que aparecen en la semisimplificación de

$\overline{\rho}_l$ tiene que proceder de una forma modular parabólica de peso 2 y carácter trivial; además, el producto de los niveles de las dos formas modulares obtenidas tiene que dividir al conductor de A. Por tanto, se puede hallar un conjunto finito de formas modulares de tal forma que los bloques deben estar asociados a alguna de ellas. Tomando ahora un primo p de buena reducción, y teniendo en cuenta que el polinomio característico de la imagen de Frob_p por $\overline{\rho}_l$ debe coincidir con el producto de los polinomios característicos en p de dos de las formas modulares obtenidas, se deducen condiciones sobre los coeficientes a_p y b_p.

Notemos que este paso depende de la conjetura de Serre para niveles que dividan al conductor de A.

Finalmente, el caso (5) se corresponde con grupos que tienen orden pequeño. Por tanto, es suficiente encontrar elementos en el grupo de Galois cuya imagen tenga orden grande. Cuando l sea suficientemente grande, la imagen de la inercia en l nos proporciona estos elementos. Para los primos l pequeños, podemos proceder del siguiente modo: tomando un primo p de buena reducción, se pueden encontrar condiciones sobre los coeficientes a_p y b_p que garanticen que la imagen de Frob_p tiene orden suficientemente grande.

En el resto de la sección vamos a presentar un ejemplo, y veremos algún caso con detalle.

Consideremos la curva C de género 2 dada por la ecuación hiperelíptica

$$y^2 = x^6 + 2x^4 - 2x^3 - 3x^2 + 2x + 1$$

(ver [35]). Utilizando los resultados de Liu (según hemos visto en la sección 7.3), se puede calcular la parte prima

con 2 del conductor de C, que es el primo 587.

Por otra parte, la curva C se puede expresar también mediante la ecuación hiperelíptica

$$y^2 + (x^3 + x + 1) \cdot y = -x^3 - x^2$$

El discriminante de esta ecuación es -587, por tanto C tiene buena reducción en 2. Así pues, el conductor de C es

$$c = 587.$$

Queremos probar que, para todo primo $l > 3$ y distinto de 587, la imagen de $\overline{\rho}_l$ coincide con $\mathrm{GSp}_4(\mathbb{F}_l)$. Tenemos entonces que mostrar que no se puede dar ninguno de los casos (1), (2), (3), (4) y (5).

Vamos a explicar con detalle por qué no puede tenerse el caso (1), para mostrar el tipo de razonamientos que se utilizan. Supongamos pues que la imagen de $\overline{\rho}_l$ es reducible sobre $\overline{\mathbb{F}}_l$, de forma que en la semisimplificación aparece un bloque 1-dimensional. Este bloque viene dado por un carácter

$$\mu_l : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \overline{\mathbb{F}}_l^*.$$

Debido a la forma que tiene la restricción de $\overline{\rho}_l$ al grupo de inercia en l, obtenemos que μ_l es de la forma

$$\mu_l = \varepsilon \cdot \chi_l^i,$$

donde χ_l es el carácter ciclotómico en l, y el índice i es igual a 0 ó 1. Además, el conductor del carácter ε al cuadrado debe dividir al conductor de la superficie abeliana, es decir, a 587. La única posibilidad, por tanto, es que el conductor sea 1. Es decir, ε es un carácter del grupo de Galois

$\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ no ramificado en ningún primo, así que tiene que ser la identidad. Por tanto

$$\mu_l = \chi_l^i.$$

Consideremos un primo p de buena reducción. Entonces $\mu_l(\mathrm{Frob}_p)$ es una raíz del polinomio característico

$$\mathrm{Pol}_p(x) = x^4 - a_p x^3 + b_p x^2 - p a_p x + p^2$$

con coeficientes en $\mathbb{F}_l$. Sustituyendo $\mu(\mathrm{Frob}_p) = \chi_l^i(\mathrm{Frob}_p) = 1$ ó p según $i = 0$ ó 1, obtenemos la congruencia

$$b_p - a_p(p+1) + p^2 + 1 \equiv 0 \pmod{l}.$$

Consideremos el primo $p = 3$. Con las fórmulas (7.4.2), calculamos $a_p = -4$, $b_p = 9$, y por tanto concluimos que

$$b_p - a_p(p+1) + p^2 + 1 = 35 \equiv 0 \pmod{l}.$$

Así pues, o bien $l = 3$, o bien l divide a 35, es decir, sólo tenemos tres posibles valores para l. Pero si consideramos ahora el primo $p = 19$, tenemos que

$$b_p - a_p(p+1) + p^2 + 1 = 533 = 13 \cdot 41 \equiv 0 \pmod{l},$$

luego $l = 19, 13$ ó 41. Hemos llegado a una contradicción. Por tanto, para todo $l \geq 3$, concluimos que la imagen de $\overline{\rho}_l$ no es reducible con un bloque de dimensión 1.

En los otros casos se procede de forma semejante. Por ejemplo, podemos asegurar que no estamos en el caso (2) cuando l es un primo impar, utilizando los primos 3 y 5 y los valores de a_3, b_3, a_5 y b_5. Para comprobar que no se puede dar el caso (3) no es necesario efectuar ningún cálculo, ya

que tendrían que existir dos formas parabólicas de peso 2, carácter trivial y niveles N_1 y N_2 verificando $N_1 \cdot N_2 | 587$, y por tanto uno de los dos números N_1 o N_2 tendría que ser igual a 1. Pero el espacio $\mathrm{S}_2(1)$ de las formas parabólicas de peso 2, carácter trivial y nivel 1 es nulo.

En el caso (4), habría que encontrar un primo p distinto de l de buena reducción, verificando que -587 no sea un cuadrado en $\mathbb{F}_p$, y tal que $a_p \not\equiv 0 \pmod{l}$. El primo $p = 5$ satisface estas condiciones, para todo $l \neq 5$ impar. Para descartar el caso $l = 5$ elegimos otro primo p diferente que también verifique estas condiciones, por ejemplo el primo $p = 11$.

Finalmente, el caso (5) también se descarta calculando los coeficientes a_p, b_p para varios primos p de buena reducción.

La conclusión que obtenemos, por tanto, es la siguiente:

Proposición 7.4.1. *Sea C la curva de género 2 dada por la ecuación hiperelíptica*

$$y^2 = x^6 + 2x^4 - 2x^3 - 3x^2 + 2x + 1.$$

Entonces, para todo primo $l > 3$, $l \neq 587$, la representación $\overline{\rho}_l$ asociada a los puntos de l-torsión de la jacobiana de C satisface

$$\mathrm{Im}(\overline{\rho}_l) = \mathrm{GSp}_4(\mathbb{F}_l).$$

Apèndix A

Equacions de Thue: Models regulars i fites uniformes.

Xavier Xarles[1]

Aquestes notes són les transparencies de la meva xerrada del dia 1 de Febrer de 2007 al Seminari de Teoria de Nombres a la Facultat de Nàutica de la UPC. Estan basades en l'article de Lorenzini i Tucker [20].

A.1 Equacions de Thue

$F(X,Y) \in \mathbb{Z}[X,Y]$ homogénea, de grau $n \geq 3$, i tal que $F(x,1)$ no té arrels repetides.

Una equació de Thue és una equació de la forma, per $h \in \mathbb{Z}$,

$$F(X,Y) = h.$$

Teorema (Thue 1909)

[1]Dep. Matemàtiques, Univ. Autònoma de Barcelona. E-mail: xarles@mat.uab.cat

Les equacions de Thue tenen un nombre finit de solucions $(x, y) \in \mathbb{Z}^2$.

A.1.1 Observació

Una equació de Thue (tal com l'he definit) ens determina una corba (plana) no singular $X_{F,h}$, de gènere

$$g(X_F) = \frac{(n-1)(n-2)}{2}.$$

Teorema(Faltings 1982)

Les equacions de Thue amb $n \geq 4$ tenen un nombre finit de solucions racionals ($(x, y) \in \mathbb{Q}^2$).

A.1.2 Conjectura Solucions primitives

Conjectura(Erdös, Steward, Tijdeman)

Per a tota $n \geq 3$, existeix una constant $C(n)$ que només depèn de n tal que

$$\sharp\{(x, y) \in \mathbb{Z}^2 \mid F(x, y) = h \text{ i } (x, y) = 1 \} \leq C(n)$$

per a tota equació de Thue $F(X, Y) = h$ de grau n.

A.1.3 Conjectura solucions racionals

Conjectura(Caporaso, Harris, Mazur)

Per a tota $n \geq 4$, existeix una constant $C(n)$ que només depèn de n tal que

$$\sharp\{(x,y) \in \mathbb{Q}^2 \mid F(x,y) = h \} \leq C(n)$$

per a tota equació de Thue $F(X,Y) = h$ de grau n.

A.1.4 Resultats Coneguts

Notació

$$N(F,h) = \sharp\{(x,y) \in \mathbb{Z}^2 \mid F(x,y) = h \text{ i } (x,y) = 1 \}$$

Teorema(Bombieri-Schmidt 1987)

Suposem $F(x,1)$ irreductible. Existeix una constant B_1 (que podem prendre igual a 215 si n és gran), tal que

$$N(F,h) \leq B_1 n^{\omega(h)+1}$$

on $\omega(h)$ és el nombre de factors primers de h.

Denotem per $r(X_{F,h})$ el rank del grup de punts racionals de la Jacobiana de $X_{F,h}$.

Teorema(Silverman 1983)

Existeix una constant (inefectiva) $h(F)$ tal que per tota $h > h(F)$ lliure de potències enèsimes,

$$N(F,h) \leq n^{2n^2}(8n^3)^{r(X_{F,h})}$$

Teorema(Lorenzini-Tucker)

Si $r(X_{F,h}) < g(X_F) = \frac{(n-1)(n-2)}{2}$, aleshores

$$N(F,h) \leq 2n^3 - 2n - 3.$$

(Per certs casos especials obtenen una fita del ordre $O(n^2)$).

Observació La fita que s'obté del resultat del Silverman és exponencial en n.

A.2 Mètode de Chabauty-Coleman

Idea a retenir Si $r(X) < g(X)$, i $p > 2g$, aleshores

$$\sharp X(\mathbb{Q}) \leq \sharp \overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + 2g(X) - 2$$

on $\overline{\mathcal{X}}$ és la reducció mòdul p de qualsevol model regular $\mathfrak{X}$ de X sobre $\mathbb{Z}_p$, i ns indica els punts no singulars.

Generalització Val pels cossos de nombres K amb completació en un primer no ramificada sobre $\mathbb{Q}_p$.

A.2.1 Comentaris

$$\sharp X(\mathbb{Q}) \leq \sharp \overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + 2g(X) - 2$$

- Coleman va provar això només per bona reducció.
- La fita donada pot ser molt gran si la reducció és molt dolenta

- Necessitem una millora per estudiar els punts que ens interessen (no tots els punts racionals)

A.2.2 Notacions

$X/\mathbb{Q}$ corba de gènere $g \geq 2$.

$\mathfrak{X}$ un model regular sobre $\mathbb{Z}_p$

$\overline{\mathcal{X}}$ la fibra especial de $\mathfrak{X}$ a $\mathbb{F}_p$

$red_p : X(\mathbb{Q}_p) \to \overline{\mathcal{X}}_{ns}(\mathbb{F}_p)$ el morfisme reducció.

Exercici: La imatge sempre cau dins els punts no singulars

A.2.3 Chabauty-Coleman General

Prenem $X/\mathbb{Q}$ corba de gènere $g \geq 2$. Suposem $r(X) < g$

Sigui $d < p$ tal que $p^d > 2g + 1 - d$. (Prendrem d=2)

Sigui $U \subseteq \overline{\mathcal{X}}_{ns}(\mathbb{F}_p)$ un subconjunt qualsevol.

Aleshores

$$\sharp red_p^{-1}(U) \cap X(\mathbb{Q}) \leq \sharp U + \left(\frac{p-1}{p-d}\right)(2g-2)$$

A.2.4 Idea

Considerem un nombre primer p tal que $n < p < 2n$.

Aleshores $p^2 > 2g(X_{F,h}) - 1$.

Trobem U a la reducció en p d'un model regular de $X_{F,h}$ que contingui totes les imatges de punts primitius sobre $\mathbb{Z}$.

Fitem superiorment el nombre de punts de U en funció de n i p i apliquem el teorema anterior.

Substituïm p per $2n$. I ja està!

A.2.5 Notacions

$F(X, Y)$ polinomi homogeni amb coefficients a $\mathbb{Z}$ de grau $n > 3$ sense arrels repetides a $\overline{\mathbb{Q}}$.

$d(F) \in \mathbb{Z}$ discriminant de $F(x, 1)$.

$h \in \mathbb{Z}$ enter lliure de potències enèsimes (si en té podem fer un canvi de variables per treure-la)

Suposem que $X := X_{F,h}$ té $r(X) < g(X)$.

p un nombre primer $n < p < 2n$.

A.3 Casos a estudiar

1. $p \nmid d(F)$ i $p \nmid h$ (Cas bona reducció).

2. $p \mid d(F)$ i $p \nmid h$ (Cas mala reducció).

3. $p \nmid d(F)$ i $p \mid h$ (Cas bona reducció potencial)

4. $p \mid d(F)$ i $p \mid h$ (Cas molt mala reducció)

A.3.1 1. $p \nmid d(F)$ i $p \nmid h$

Prenem el model $\mathfrak{X}$ de X sobre $\mathbb{Z}_p$ donat per $F(X,Y) = hZ^n$.

Aquest model redueix a una corba no singular. El model és llis, i per tant regular.

Chabauty-Coleman: $\sharp X(\mathbb{Q}) \leq \sharp \overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + \left(\frac{p-1}{p-2}\right)(2g-2)$.

Tenim $\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) \leq (n-1)(p+1)+1$.

$p \leq 2n-1 \Rightarrow (2g-2)\left(\frac{p-1}{p-2}\right) \leq 2g+n-5$.

Obtenim finalment que $\sharp X(\mathbb{Q}) \leq 3n^2-4n-2$.

A.3.2 2. $p \mid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{C}$ de X sobre $\mathbb{Z}_p$ donat per $F(X,Y) = hZ^n$.

Aquest model no és regular! Ara bé, la part afí U de la reducció $\overline{\mathcal{C}}$ corresponent a $F(X,Y) = h$ és llisa.

Tota solució primitiva $(a,b) \in \mathbb{Z}^2$ de $F(X,Y) = h$ cau a dins de U al reduir.

Prenem $\varphi : \mathfrak{X} \to \mathcal{C}$ model regular obtingut resolen $\mathcal{C}$. Aleshores $\overline{\varphi}^{-1}(U) \cong U$.

Per tant $N(F,h) \leq (2g-2)(p-1)/(p-2) + \sharp U \leq (2g-2)(p-1)/(p-2) + np \leq 3n^2-3n-3$.

A.3.3 3. $p \nmid d(F)$ i $p \mid h$

Prenem $K = \mathbb{Q}_p(\sqrt[n]{h})$. Aleshores

$$X \otimes_{\mathbb{Q}_p} K \cong X_{F,1}$$

que té bona reducció pel cas 1.

Idea: Prenem model $\mathcal{Y}$ sobre $\mathcal{O}_K$ llis, i fem quocient per l'acció de $Gal(K/\mathbb{Q}_p)$. Resolem el model obtingut.

Problema: $K/\mathbb{Q}_p$ no és cíclica, ni tant sols Galois.

Idea: Prenem $L = \mathbb{Q}_p^{nr}(\sqrt[n]{h})/\mathbb{Q}_p^{nr}$ que és Galois, cíclica, moderadament ramificada.

A.4 Construcció quocient: Cas llis

Tenim $\mathcal{Y}$ llis sobre $\mathcal{O}_L$, el model anterior:

$$\mathcal{Y} := Proj(\mathcal{O}_L[X,Y,Z]/(F(X,Y) - Z^n)$$

L'acció de $G := Gal(L/\mathbb{Q}_p^{nr}) = \langle\sigma\rangle$ sobre X_L dóna acció sobre $\mathcal{Y}$:

$$\sigma(X) = X \ , \ \sigma(Y) = Y \ , \ \sigma(Z) = \xi_m Z$$

ξ_m arrel primitiva enèsima de 1, $m := n/ord_p(h)$, $L = \mathbb{Q}_p^{nr}(\xi_m)$.

El morfisme $q : \mathcal{Y} \to \mathcal{Y}/G$ redueix al morfisme $\bar{q} : \overline{\mathcal{Y}} \to \overline{\mathcal{Y}}/G$.

A.4.1 Estudi del quocient

El quocient $\mathcal{Y}/G$ és un esquema sobre $\mathbb{Z}_p^{nr}$, normal, els seus punts singulars estan a la fibra especial i són "singularitats quocient".

Els punts singulars són els punts ramificats de $\bar{q} : \overline{\mathcal{Y}} \to \overline{\mathcal{Y}}/G$.

O sigui els punts $q(P)$ amb $P = [x : y : 0]$, i n'hi ha n.
A més $q^{-1}(P)$ només conté el punt tancat P.

A.4.2 Desingularització de quocient

Prenem $\nu : \mathfrak{X}' \to \mathcal{Y}/G$ la desingularització sobre $\mathbb{Z}_p^{nr}$.

Donat $P \in (\overline{\mathcal{Y}}/G)_{sing}$, $\nu^{-1}(P)$ és una cadena de corbes llises i racionals, amb una sola E_1 intersecant $\overline{\mathcal{X}}' \setminus \nu^{-1}(P)$ i la última component E_P de multiplicitat 1 (=número de punts tancats de $q^{-1}(P)$).

A.4.3 3. $p \nmid d(F)$ i $p \mid h$ (Cont.)

Un punt $[x : y : z]$ de $X(\mathbb{Q})$ ens dóna un punt $[x : y : \sqrt[n]{h}z]$ de $\mathcal{Y}$.

Que correspon a un del n punts $[x : y : 0]$ de $\overline{\mathcal{Y}}$, singular a $\overline{\mathcal{Y}}/G$.

Per tant, al reduir a través de $\mathfrak{X}'$ un punt en una de les n components llises i racionals de $\overline{\mathcal{X}}'$ de multiplicitat 1.

Que necessàriament ha de ser una de les $\leq n$ components llises i racional de $\overline{\mathcal{X}}$ de multiplicitat 1.

A.4.4 3. $p \nmid d(F)$ i $p \mid h$ (Final)

Prenem $U \subseteq \overline{\mathcal{X}}$ la unió d'aquestes components racionals.

Aleshores $red^{-1}(U) \cap X(\mathbb{Q}) = X(\mathbb{Q})$.

Chabauty-Coleman: $\sharp X(\mathbb{Q}) \leq \sharp U + \left(\frac{p-1}{p-2}\right)(2g-2) \leq np + 2g + n - 5$

$$\sharp X(\mathbb{Q}) \leq 3n^2 - 3n - 3$$

A.5 4. $p \mid d(F)$ i $p \mid h$

No té pot. bona reducció. Prenem un model enter $\mathcal{Y}$ de X sobre L, cos de descomposició de $F(x,1)$ sobre $\mathbb{Q}_p^{nr}$.

$p > n \Rightarrow L/\mathbb{Q}_p^{nr}$ moderada.

Per a cada arrel α de $F(x,1)$, es construeixen oberts llisos U_α de $\mathcal{Y}$ sobre $\mathcal{O}_L$.

Aquests oberts tenen acció de $G := Gal(L/\mathbb{Q}_p^{nr})$ natural.

Considerem $Z_P = U_P/G$ i s'estudia la reducció de la seva desingularització.

Es prova que tot punt primitiu P de X està en un U_α

A.6 Construcció quocient: Cas general

$\mathcal{U}$ sub-esquema obert i llis de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on G actua. Prenem $q : \mathcal{U} \to \mathcal{Z} := \mathcal{U}/G$, $\mathcal{Z}$ esquema sobre $\mathbb{Z}_p^{nr}$.

Existeix un esquema regular $\mathfrak{X}$ sobre $\mathbb{Z}_p^{nr}$ i un morfisme birracional $\nu : \mathfrak{X} \to \mathcal{Z}$ induint iso entre $\mathfrak{X}_{ns}$ i $\mathcal{Z}_{ns}$.

Per a tot punt $z \in \mathcal{Z}_{sing}$, $\nu^{-1}(z)$ és una cadena $\{E_1, \ldots, E_z\}$ connexa de corves racionals i llises.

U llis, per tant la cadena sols interseca el resta de la fibra $\overline{\mathcal{X}}$ en un punt a E_1.

El conjunt de punts singulars és igual als punts de ramificació de q. E_z té multiplicitat $= \sharp q^{-1}(z)$.

A.6.1 Oberts adequats

Per a cada arrel α de $F(x, 1)$, construïm $\mathcal{V}_\alpha$ obert de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on

$$\mathcal{Y} := Proj(\mathcal{O}_L[X, Y, Z]/(F(X, Y) - hZ^n).$$

$$\mathcal{V}_\alpha := Spec(\mathcal{O}_L[z', y](F_\alpha(z', y) - h/\pi^{u_\alpha}))$$

on π uniformitzant de L.

Fent $z_0 = x - \alpha y$, obtenim $F_0(z_0, y)$ de $F(x, y)$.

$z' := z_0/\pi^t$, on t és cert enter.

$F_\alpha(z_\alpha, y) = F_0(z_0, y)\pi^{-u_\alpha}$ amb u_α un cert enter.

Proposició $\mathcal{V}_\alpha$ és un esquema llis, obert de $\mathcal{Y}$. Igualment per

$$\mathcal{U}_\alpha := \bigcap_{\tau \in G} \tau(\mathcal{V}_\alpha)$$

que a més és invariant per $G := Gal(L/\mathbb{Q}_p^{nr})$.

Per a tot P solució primitiva de $F(X,Y)=h$, existeix un α tal que $P \in U_\alpha$.

Concretament, $P=(a,b)$, aleshores $P \in \mathcal{U}_\alpha$ si i només si

$$t := v(a-\alpha b) = \max_{\beta}(a-\beta b)$$

on β es mou dins les arrels de $F(x,1)=0$.

A.6.2 4. $p \mid d(F)$ i $p \mid h$ (cont)

Fem el mateix raonament que el cas 3, però pels $\mathcal{U}_\alpha$.

$$\mathcal{U}_\alpha \to \mathcal{Z}_\alpha \leftarrow \mathfrak{X}_\alpha$$

Si $\mathfrak{X}$ model regular sobre $\mathbb{Z}_p$, tenim $\mathfrak{X}_\alpha \to \mathfrak{X} \otimes \mathbb{Z}_p^{nr}$.

Fet clau: Com a molt np punts de la imatge de $\mathcal{Z}_\alpha$ a $\overline{\mathcal{X}}$ poden ser reducció de punts primitius.

A.6.3 4. $p \mid d(F)$ i $p \mid h$ (Final)

En resum:
Si U és la unió de les imatges de $\mathcal{U}_\alpha$ a $\overline{\mathcal{X}}$, aleshores

Chabauty-Coleman:

$$N(F,h) \leq \sharp U + \left(\frac{p-1}{p-2}\right)(2g-2) \leq n^2p + 2g + n - 5.$$

Per tant

$$N(F,h) \leq 2n^3 - 2n - 3$$

A.7 Resum definitiu

Tenim en el cas general que si

$$r(X_{F,h}) < g(X_F) = \frac{(n-1)(n-2)}{2},$$

aleshores

$$N(F,h) \leq 2n^3 - 2n - 3.$$

Si $\exists p \nmid d(F)$ tal que $n < p < 2n$, aleshores

$$\sharp X_{F,h}(\mathbb{Q}) \leq 3n^2 - 3n - 3.$$

Si $\exists p \nmid h$ tal que $n < p < 2n$, aleshores

$$N(F,h) \leq 3n^2 - 3n - 3.$$

Bibliografia

[1] M. Artin, G. Winters, Degenerate fibres and stable reduction of curves, *Topology* **10** (1971), 373-383.

[2] M.F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley 1969.

[3] O. Bolza, Darstellung der rationalen ganzen Invarianten der Binúrform sechsten Grades durch die Nullwerthe der zugehrigen θ-Functionen, *Math. Ann.* **30** (1887), 478-495.

[4] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Springer Verlag 1990.

[5] A. Clebsch, *Theorie der Binären Algebraischen Formen*, Verlag von B.G. Teubner, Leipzig, 1872.

[6] P. Deligne, D. Mumford, The irreducibility of the space of curves of given genus, *Publ. Math. Inst. Hautes Étud. Sci.* **36** (1969), 75-110.

[7] M. Deschamps, Réduction semi-stable, Séminaire sur les pinceaux de courbes aux moins deux, *Astérisque* **86** (1981), 1-34.

[8] L. Dieulefait, Explicit determination of the images of the Galois representations attached to abelian surfaces

with $\mathrm{End}(A) = \mathbb{Z}$, *Experiment. Math.* **11** (2002), 503-512.

[9] J. Dixmier, On the projective Invariants of Quartic Plane Curves, *Adv. Math.* **64** (1987), 279-304.

[10] R. Hartshorne, *Algebraic Geometry*, Grad. Texts Math. **52**, Springer Verlag, 1977.

[11] J. I. Igusa, Arithmetic variety of moduli for genus two, *Ann. Math.* **72** (1960), 612-649.

[12] K. Kodaira, On compact analytic surfaces II, *Ann. Math.* **78** (1963), 563-626.

[13] Q. Liu, Courbes stables de genre 2 et leur schéma de modules, *Math. Ann.* **295**, (1993) 201-222.

[14] Q. Liu, Modèles minimaux des courbes de genre deux, *J. reine angew. Math.* **453**, (1994) 137-164.

[15] Q. Liu, Conducteur et discriminant minimal de courbes de genre 2, *Comp. Math.* **94**, (1994) 51-79.

[16] Q. Liu, Modèles entiers des courbes hiperelliptiques sur un corps de valuation discrète, *Trans. Amer. Math. Soc.* **348:11**, (1996) 4577-4610.

[17] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, 2002.

[18] D. Lorenzini, Dual graphs of degenerating curves, *Math. Ann.* **287** (1990), 135-150.

[19] D. Lorenzini, Groups of components of Néron models of Jacobians, *Comp. Math.* **73** (1990), 145-160.

[20] D. Lorenzini, T. J. Tucker, Thue equations and the method of Chabauty-Coleman. *Invent. Math.* **148** (2002), no. 1, 47–77.

[21] J-F. Mestre, Construction de courbes de genre 2 à partir de leurs modules, *Effective methods in algebraic geometry (Castiglioncello, 1990)*, Progr. Math. **94** (1991), 313-334.

[22] J. Müller, C. Ritzenthaler, On the ring of invariants of ordinary quartic curves in characteristic 2, *J. Algebra* **303** (2006), 530-542.

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

[24] Y. Namikawa, K. Ueno, The complete classification of fibers of curves of genus two, *Manuscripta Math.* **9** (1973), 143-186.

[25] A. P. Ogg, On pencils of curves of genus two, *Topology* **5** (1966), 355-362

[26] A. P. Ogg, Elliptic curves and wild ramification, *Amer. J. Math.* **89:1** (1967), 1-21.

[27] B. Poonen, Computational aspects of curves of genus at least 2, *Lect. Notes Comput. Sci.* **1122** (1996), 283-306.

[28] T. Ohno, Invariant subring of ternary quartic I - Generators and Relations-. *Preprint.*

[29] J-P. Serre, Facteurs locaux des fonctions zêta des variétés algébriques, *Séminaire DPP* **19**, 1969-1970.

[30] J-P. Serre, Ouvres **4**, Springer-Verlag (2000), 1-55.

[31] J-P. Serre, J. Tate, Good reduction of abelian varieties, *Ann. Math.* **88** (1968), 492-517.

[32] T. Shioda, On the graded ring of binary octavics. *Amer. J. Math.* **89** (1967), 1022-1046.

[33] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts Math. **106**, Springer Verlag, 1986.

[34] J. H. Silverman, *Advanced topics in the Arithmetic of Elliptic curves*, Grad. Texts Math. **151**, Springer Verlag, 1994.

[35] M. Stoll, Genus 2 curves with small odd discriminant, http://www.faculty.iu-bremen.de/stoll/data/

[36] E. Viehweg, Invarianten der degenerierten Fasern in lokalen Familien von Kurven, *J. Reine Angew. Math.* **293** (1977), 284-308.