

Una introducció a la teoria d'Arakelov*

JOSÉ I. BURGOS GIL

1 Introducció

Una de les millors qualitats de la Matemàtica és la seva capacitat de prendre una idea apareguda en un camp determinat, abstroure-la i aplicar-la a un altre camp completament diferent. Aquesta capacitat és molt més interessant i profitosa quan el camp on apareix la idea i aquell on s'aplica són completament diferents, i quan el tipus de intuïció que hom obté de l'un i de l'altre són complementaris. La teoria d'Arakelov és un exemple d'aquest fenomen, ja que pren idees de la geometria projectiva, els orígens de la qual es remunten als estudis de perspectiva dels pintors renaixentistes, i les aplica, en el marc de la teoria de nombres, a l'estudi de les solucions enteres de sistemes d'equacions polinòmiques.

De fet, la teoria d'Arakelov pot ser entesa com un diccionari que permet traduir enunciats de geometria algebraica projectiva en enunciats que relacionen la teoria de nombres i l'anàlisi complexa. Aquesta traducció no és trivial: la identificació de conceptes anàlegs en l'un i l'altre camp no és evident. A més, els enunciats obtinguts mitjançant analogia no són certs a priori, sinó que necessiten una demostració que, en molts casos, és més complexa que la demostració del resultat original. L'enunciat proposat fins i tot pot revelar-se fals. En resulta que la teoria d'Arakelov és, fonamentalment, una font d'analogies que permeten guiar la investigació, i no un mètode automàtic per obtenir nous teoremes.

Tot i que la idea subjacent en la teoria d'Arakelov és senzilla i d'una gran bellesa conceptual, no és menys cert que pertany a un àmbit d'una gran complexitat tècnica. L'objectiu d'aquesta nota és donar una imatge general

* Conferència pronunciada a la Tercera Trobada Matemàtica de la Societat Catalana de Matemàtiques, que va tenir lloc a la Universitat de València el març de 2000.

d'aquesta teoria, accessible a un públic com més ampli millor. És per aquest motiu pel qual s'intentaran obviar els detalls tècnics i s'insistirà en les idees generals.

En una introducció d'aquest tipus, és inevitable donar una versió parcial i esbiaixada de la teoria d'Arakelov. Molts aspectes, sigui per la seva complexitat, o simplement per falta d'espai, no hi tenen cabuda. Per exemple, poca cosa direm sobre la teoria d'altures, que és un dels aspectes fonamentals d'aquesta teoria.

El lector podrà comprovar que el punt de vista des del qual s'han redactat aquestes notes és el de la geometria. S'ha posat més èmfasi en l'estètica de les idees i en el fet que la geometria permet donar un llenguatge comú a dues àrees en principi disjunts, que no a les aplicacions concretes.

2 Teoria d'intersecció

La idea bàsica que es vol traslladar des de la geometria algebraica a la teoria de nombres és el concepte de compleció projectiva d'una varietat. Vegem primer, en un exemple senzill, en què consisteix la compleció projectiva i quina és la seva utilitat.

En línies generals, podem dir que la geometria algebraica estudia les solucions de sistemes d'equacions polinòmiques. El conjunt de solucions d'un sistema d'aquest tipus es denomina varietat algebraica. La teoria d'intersecció estudia la posició relativa d'aquestes varietats. Un problema clàssic de la teoria d'intersecció és el de comptar els punts de tall de dues corbes planes. Ens plantegem, concretament, el problema següent:

1 PROBLEMA *Trobar un teorema, com més precís millor, sobre el nombre de punts de tall de dues corbes planes reals.*

El primer exemple que estudiarem serà el de la posició relativa de dues rectes diferents. De seguida veiem que hi ha dues possibilitats:

- a) Dues rectes transversals. En aquest cas, les dues rectes es tallen en un punt.
- b) Dues rectes paral·leles. En aquest cas, les rectes no es tallen.

Així doncs, el millor resultat general que, en aquest moment, podem enunciar és el següent:

*el nombre de punts de tall de dues rectes
diferents és menor o igual que u.*

El següent exemple que podem estudiar és el de dues corbes algebraiques diferents del pla \mathbb{R}^2 . Cada una és el conjunt de solucions d'una equació polinòmica en dues variables. Suposarem que aquestes corbes no tenen components comuns, ja que en cas contrari tindrien infinits punts en comú.

Siguin d_1 i d_2 els graus d'aquestes equacions. Com en l'exemple de les rectes, si comptem els punts de tall entre les dues corbes, podem escriure el resultat general següent:

$$\text{nombre de punts de tall de dues corbes afins reals de graus } d_1 \text{ i } d_2 \leq d_1 d_2. \quad (1)$$

Es pot provar que aquest és el millor resultat a què es pot arribar. En efecte, hi ha exemples de corbes de graus d_1 i d_2 sense cap punt de tall.

Un cas particular del problema de comptar punts d'intersecció de dues corbes és el de comptar les arrels d'un polinomi. En aquest cas, una de les corbes és la recta $y = 0$, que té grau u , i l'altra corba es la gràfica de la funció polinòmica. Obtenim, en principi, el mateix tipus de resultat:

el nombre d'arrels d'un polinomi és menor o igual que el grau del polinomi.

El nombre d'arrels del polinomi pot disminuir per dos fenòmens diferents. D'una banda, les arrels poden ser nombres complexos i no nombres reals. De l'altra, el polinomi pot tenir arrels repetides. En aquest cas, a cada arrel se li pot assignar un pes, anomenat multiplicitat, que és el nombre de vegades que es repeteix l'arrel.

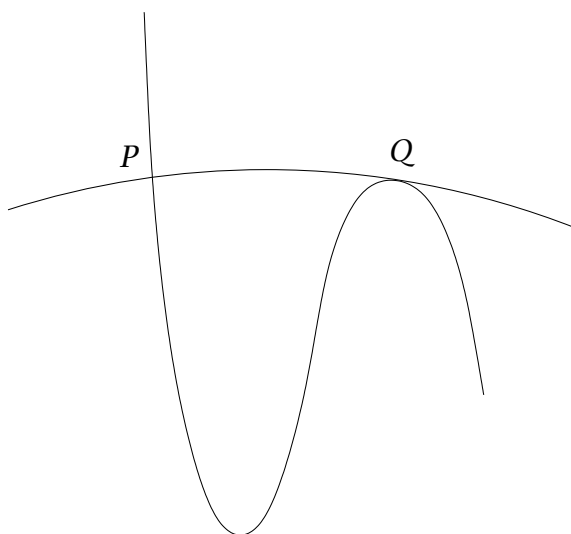


FIGURA 1: P punt simple, Q punt de multiplicitat major que 1.

Si tenim en compte aquests dos fenòmens, obtenim un resultat molt més precís:

el nombre d'arrels complexes d'un polinomi, comptada cadascuna amb la seva multiplicitat, és exactament igual al grau del polinomi.

A la vista d'aquest exemple, podem pensar que el nombre de punts de tall entre dues corbes de graus d_1 i d_2 és igual al producte $d_1 d_2$, però que determinats fenòmens ens oculten alguns punts de tall. Com abans, existeixen punts de tall amb coordenades complexes, i, també, a cada punt de tall entre dues corbes se li pot assignar una multiplicitat, que generalitza el concepte de multiplicitat d'una arrel, i que reflecteix l'ordre de contacte entre les corbes (vegeu la figura 1). Això ens porta a modificar el problema original, plantejant-lo de la manera següent:

2 PROBLEMA *Trobar un teorema, com més precís millor, sobre el nombre de punts de tall de dues corbes planes complexes, comptats cadascun amb la seva multiplicitat.*

Plantejat d'aquesta forma, trobem molts més punts d'intersecció entre les corbes. Es més, si escollim dues corbes qualssevol a l'atzar, de graus d_1 i d_2 , trobem que el nombre de punts d'intersecció és efectivament $d_1 d_2$. Tot i això, com en el cas real, existeixen exemples de corbes de qualsevol grau sense cap punt d'intersecció. De manera que, de nou, el millor resultat que podem enunciar és:

$$\text{nombre de punts de tall, comptats amb multiplicitat, de dues corbes afins complexes de graus } d_1 \text{ i } d_2 \leq d_1 d_2. \quad (2)$$

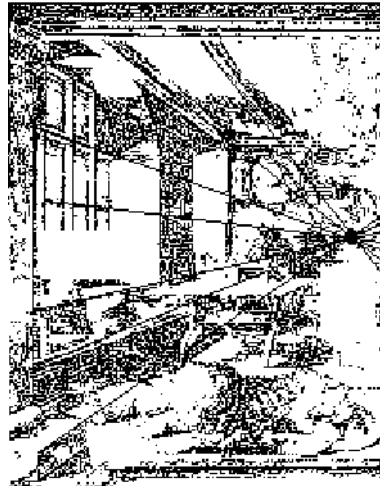


FIGURA 2: San Jeroni a la seva cella (Dürer).

Per comprendre què succeeix en els casos on el nombre de punts de tall és menor que no esperàvem, tornarem a considerar el problema de les rectes paral·leles. Visualment, dues rectes paral·leles semblen unir-se en un punt (vegeu la figura 2). Aquest punt, que en pintura es denomina punt de fuga, l'anomenarem punt de l'infinit. Això suggereix que, en lloc de considerar el pla complex, hem d'estudiar un conjunt més gran, el pla projectiu. Aquest conjunt, format per tots els punts del pla complex i per tots els possibles punts de l'infinit, el denotarem per \mathbb{P}^2 .

Encara que el pla projectiu sembli més complicat que el pla afí, és molt útil perquè posseeix molt bones propietats. Per exemple, de la mateixa definició es dedueix que en el pla projectiu no hi ha dos tipus de parells de rectes, transversals o paral·leles. En efecte, dues rectes diferents es tallen sempre en un únic punt. És més, el problema de comptar els punts de tall de dues corbes en el pla projectiu té una resposta molt satisfactòria:

1 TEOREMA (BÉZOUT) *Siguin C_1 i C_2 dues corbes diferents del pla projectiu complex, sense components comuns i de graus d_1 i d_2 . El nombre de punts d'intersecció, comptats amb la seva multiplicitat, és sempre $d_1 d_2$.*

Aquest és un exemple clar de la potència de la completió projectiva. El pla projectiu té propietats noves, més precises que no pas les del pla afí. Però allò realment interessant és que l'existència i les propietats del pla projectiu ens permeten entendre millor les propietats del pla afí. Per il·lustrar aquesta idea considerarem el teorema de Bézout des d'un punt de vista diferent. Si dues corbes tenen un punt de l'infinit en comú direm que tenen una direcció asimptòtica comuna (hem utilitzat els punts de l'infinit per definir direcció asimptòtica, però aquesta pot definir-se en termes purament afins). A les direccions asimptòtiques comunes també se'ls assigna una multiplicitat. El teorema de Bézout pot escriure's de la manera següent:

$$\begin{array}{l} \text{nombre de} \\ \text{punts de tall} \end{array} + \begin{array}{l} \text{nombre de direccions} \\ \text{asimptòtiques comunes} \end{array} = d_1 d_2. \quad (3)$$

El teorema de Bézout implica, doncs, que dues quantitats, el nombre de punts de tall i el nombre de direccions asimptòtiques comunes, estan relacionades.

La conclusió que extraïem d'aquesta discussió és la següent. El pla projectiu està format per dues parts, el pla afí i el conjunt de punts de l'infinit. Les propietats globals del pla projectiu poden entendre's com relacions entre aquestes dues parts. Aquest és, precisament, el punt de vista que conforma la Teoria d'Arakelov.

3 Funcions racionals

Veurem en aquesta secció un nou exemple, molt relacionat amb l'anterior, relatiu a les diferències en el comportament de varietats afins i varietats projectives. Sigui $X = \mathbb{A}_{\mathbb{C}}^1$ la recta afí complexa. Per completar aquesta recta n'hi

ha prou amb afegir un punt. La línia projectiva complexa pot descriure's com

$$Y = \mathbb{P}_{\mathbb{C}}^1 = \mathbb{A}_{\mathbb{C}}^1 \cup \{\infty\}.$$

Sigui f una funció racional en X . Això és, f és un quocient de dos polinomis:

$$f(z) = \frac{a_0 z^n + a_1 z^{n-1} + \dots + a_n}{b_0 z^m + b_1 z^{m-1} + \dots + b_m},$$

que suposarem sense arrels comunes. Els zeros de la funció són les arrels del numerador i els pols de la funció són les arrels del denominador. L'ordre de la funció f en un punt p es un número enter que es denota $\text{ord}_p(f)$. Si p és un zero de f llavors $\text{ord}_p(f)$ és positiu i igual a la multiplicitat de p en tant que arrel del numerador de f . Si p és un pol de f , $\text{ord}_p(f)$ és negatiu i el seu valor absolut és igual a la multiplicitat de p en tant que arrel del denominador de f . Si p no és ni un zero ni un pol, llavors $\text{ord}_p(f) = 0$. Clarament podem construir funcions amb un nombre arbitrari de zeros i de pols. De fet, la quantitat

$$\sum_{p \in \mathbb{C}} \text{ord}_p(f)$$

és igual a la diferència entre el grau del numerador i el grau del denominador. Anomenarem d a aquesta última quantitat:

$$d = n - m.$$

Estudiem ara el cas projectiu. La funció f la podem considerar com una funció racional en $Y = \mathbb{P}_{\mathbb{C}}^1$. Per estudiar el comportament de f en el punt ∞ utilitzem el canvi de variables $u = 1/z$, que envia el punt de l'infinit a l'origen de coordenades. Aplicant aquest canvi de variables, la funció f queda

$$f(u) = u^{-d} \frac{a_0 + \dots + a_n u^n}{b_0 + \dots + b_m u^m},$$

que té un pol, un zero o un valor no nul a l'origen depenent de si d és positiu, negatiu o zero. En conseqüència, podem posar

$$\text{ord}_{\infty}(f) = -d.$$

Així doncs, si tenim en compte tots els punts de \mathbb{P}^1 , obtenim la fórmula

$$\sum_{p \in \mathbb{P}^1} \text{ord}_p(f) = 0. \quad (4)$$

De nou, una quantitat que en el cas afí podria prendre qualsevol valor té, en el cas projectiu, un valor constant.

L'equació (4) pot generalitzar-se a una corba qualsevol. Sigui X una corba complexa llisa afí. Podem completar X afegint un conjunt finit de punts a

l'infinit. Sigui Y la corba projectiva obtinguda. El resultat no és tan immediat com en el cas de $\mathbb{P}_{\mathbb{C}}^1$, però el teorema dels Residus de Cauchy ens permet afirmar que, per una funció racional qualsevol f en Y , també es verifica

$$\sum_{p \in Y} \text{ord}_p(f) = 0. \quad (5)$$

Aquesta equació pot escriure's en forma multiplicativa. Per fer-ho escollim un real positiu r , i per cada punt p definim la norma associada

$$\|f\|_p = r^{-\text{ord}_p(f)}. \quad (6)$$

La versió multiplicativa de l'equació (5) es denomina fórmula del producte:

$$\prod_{p \in Y} \|f\|_p = 1. \quad (7)$$

4 L'analogia entre cossos de nombres i cossos de funcions

Tot i que la Teoria d'Arakelov pròpiament dita comença amb les superfícies aritmètiques, és a dir, en dimensió dos, pot considerar-se que el cas de dimensió u d'aquesta teoria és l'analogia entre un cos de nombres i el cos de funcions d'una corba algebraica. Vegem en què consisteix aquesta analogia.

Els punts de la recta afí complexa $\mathbb{A}_{\mathbb{C}}^1$ estan en bijecció amb els ideals primers de l'anell de polinomis $\mathbb{C}[z]$. Al punt a li correspon l'ideal $(x - a)$. El cos de funcions racionals de $\mathbb{A}_{\mathbb{C}}^1$ és $\mathbb{C}(z)$, és a dir, el cos de fraccions de $\mathbb{C}[z]$. Tal com hem comentat a la secció anterior, a cada punt $p \in \mathbb{A}_{\mathbb{C}}^1$ li correspon una valoració: ord_p i una norma: $\|\cdot\|_p$. Hem vist que al punt de l'infinit li correspon també una valoració i una norma. El fet que $\mathbb{P}_{\mathbb{C}}^1 = \mathbb{A}_{\mathbb{C}}^1 \cup \{\infty\}$ sigui una corba completa (projectiva) es reflecteix en la fórmula del producte (7).

De la mateixa manera, els ideals primers de l'anell \mathbb{Z} són els punts d'una varietat algebraica anomenada $\text{Spec}(\mathbb{Z})$. El cos de funcions d'aquesta varietat és \mathbb{Q} , que és el cos de fraccions de \mathbb{Z} . A cada nombre primer p li correspon una valoració de \mathbb{Q} , que denotarem ord_p , definida per

$$\text{ord}_p(q) = d,$$

si q es pot escriure com $q = p^d a/b$, amb a i b no divisibles per p . Cadascuna d'aquestes valoracions ens permet definir una norma:

$$\|q\|_p = p^{-\text{ord}_p q}.$$

Aquesta norma es denomina norma p -àdica. Volem completar $\text{Spec}(\mathbb{Z})$ de manera anàloga a com hem completat \mathbb{A}^1 . Observem que, a més de les normes p -àdiques, el cos \mathbb{Q} admet una altra norma: el valor absolut habitual. Aquesta norma la denotarem $\|\cdot\|_{\infty}$. És conseqüència directa de la definició de les diferents normes que es compleix la fórmula del producte

$$\|q\|_{\infty} \times \prod_{p \in \text{Spec}(\mathbb{Z})} \|q\|_p = 1. \quad (8)$$

Aquesta fórmula suggereix la possibilitat que la varietat afí $\text{Spec}(\mathbb{Z})$ pugui completar-se afegint un únic punt a l'infinit, que correspondria al valor absolut habitual.

Una diferència important entre les varietats $\mathbb{A}_{\mathbb{C}}^1$ i $\text{Spec}(\mathbb{Z})$ és que, en la primera, tots els punts són indistingibles. Per aquesta raó, en passar de la valoració a la norma, s'escull com a base un mateix nombre real positiu r . En canvi, els punts de $\text{Spec}(\mathbb{Z})$ són tots diferents. Per exemple, el cos residual del punt p és $\mathbb{Z}/p\mathbb{Z}$, que té exactament p elements. Per això, per cada valoració s'ha utilitzat una base diferent, que coincideix amb el nombre d'elements del cos residual. Aquesta diferència de comportament entre el cas geomètric (\mathbb{A}^1) i el cas aritmètic $\text{Spec}(\mathbb{Z})$ és encara més acusada al punt de l'infinit. En el cas geomètric, el punt que s'afegia tenia les mateixes propietats que la resta de punts. De fet, \mathbb{P}^1 és una varietat homogènia. En canvi, en el cas aritmètic, el punt que s'afegeix és de naturalesa completament diferent.

La versió additiva de la fórmula del producte s'obté prenent el logaritme de la igualtat (8), i és

$$\log \|q\|_{\infty} + \sum_{p \in \text{Spec}(\mathbb{Z})} -\log(\#(\mathbb{Z}/p\mathbb{Z})) \text{ord}_p(q) = 0. \quad (9)$$

Sigui E un cos de nombres i \mathfrak{o} el seu anell d'enters. És a dir, E és una extensió algebraica finita de \mathbb{Q} , i \mathfrak{o} el conjunt d'elements d' E que són solució d'una equació polinòmica, amb tots els coeficients enters i amb el coeficient del terme de major grau igual a u . Els ideals primers de \mathfrak{o} formen la varietat algebraica $\text{Spec}(\mathfrak{o})$. L'analogia entre $\text{Spec}(\mathbb{Z})$ i $\mathbb{A}_{\mathbb{C}}^1$ s'estén a una analogia entre les varietats $\text{Spec}(\mathfrak{o})$ i les corbes afins complexes.

Vegem com podem completar la varietat $\text{Spec}(\mathfrak{o})$. Com abans, cada punt de $\text{Spec}(\mathfrak{o})$, \mathfrak{p} , dóna lloc a una valoració de E , que denotarem $\text{ord}_{\mathfrak{p}}$, i per tant a una norma

$$\|q\|_{\mathfrak{p}} = (\#(\mathfrak{o}/\mathfrak{p}))^{-\text{ord}_{\mathfrak{p}}(q)}. \quad (10)$$

Els punts de l'infinit vindran donats per normes anàlogues al valor absolut usual. Per cada immersió $\sigma: E \rightarrow \mathbb{C}$ podem construir una norma d'aquest tipus mitjançant

$$\|q\|_{\sigma} = \|\sigma(q)\|^e, \quad (11)$$

on $e = 1$, o $e = 2$, depenent, respectivament, de si la imatge de σ està, o no, continguda en \mathbb{R} . Observem que, si $\sigma(E) \not\subset \mathbb{R}$, llavors la immersió conjugada, $\bar{\sigma}$, tot i seguir essent diferent de la immersió σ , dóna lloc a la mateixa norma. Sigui Σ el conjunt de totes les normes que poden obtenir-se mitjançant aquest sistema. Aquestes normes es denominen normes arquimedianes. La fórmula del producte d'Artin assegura que

$$\prod_{\mathfrak{p} \in \text{Spec}(\mathfrak{o})} \|q\|_{\mathfrak{p}} + \prod_{v \in \Sigma} \|q\|_v = 1. \quad (12)$$

Podem dir, doncs, que la varietat afí $\text{Spec}(\mathfrak{o})$ es pot completar afegint un nombre finit de punts, que corresponen a les diferents normes arquimedianes d' E .

Utilitzant un petit truc tècnic, també podríem dir que $\text{Spec}(\mathfrak{v})$ es pot completar afegint les diferents immersions complexes de E .

5 Divisors de Cartier i divisors de Weil

En aquesta secció farem una breu introducció a la teoria de divisors. Introduïrem, en concret, els divisors de Cartier i de Weil, i enunciarem les principals propietats que els relacionen.

Començarem introduint els divisors de Cartier. Donada una varietat algebraica complexa X , un divisor de Cartier està determinat per un recobriment obert, $\mathcal{U} = \{U_\alpha\}_{\alpha \in \Lambda}$, i una col·lecció de funcions racionals invertibles $\{g_{\alpha\beta}\}$, on la funció $g_{\alpha\beta}$ està definida a l'obert $U_{\alpha\beta} = U_\alpha \cap U_\beta$. Aquestes funcions han de satisfer la condició

$$g_{\alpha\beta}g_{\beta\gamma} = g_{\alpha\gamma}.$$

A la definició d'un divisor de Cartier, la dada important són les funcions invertibles $g_{\alpha\beta}$. Més concretament, suposem que $\mathcal{V} = \{V_{\alpha'}\}_{\alpha' \in \Lambda'}$ és un recobriment més fi que el recobriment \mathcal{U} , i que $\tau: \Lambda' \rightarrow \Lambda$ és una funció tal que $V_{\alpha'} \subset U_{\tau(\alpha')}$. Si $f_{\alpha'\beta'} = g_{\tau(\alpha')\tau(\beta')}$, direm que les dades $(\mathcal{U}, g_{\alpha\beta})$ i $(\mathcal{V}, f_{\alpha'\beta'})$ defineixen el mateix divisor de Cartier. D'aquesta manera, passant a un recobriment més fi, sempre podem pensar que dos divisors de Cartier diferents estan definits sobre el mateix recobriment. Per això, en la notació freqüentment ometrem el recobriment obert.

El producte de dos divisors de Cartier ve donat pel producte de les funcions que els defineixen. En altres paraules, donats dos divisors de Cartier $\mathcal{L} = (f_{\alpha\beta})$ i $\mathcal{M} = (g_{\alpha\beta})$, el seu producte és el divisor de Cartier $\mathcal{L} \otimes \mathcal{M} = (f_{\alpha\beta}g_{\alpha\beta})$.

El concepte de divisor de Cartier està molt relacionat amb el concepte de fibrat de línia. Un fibrat de línia sobre X és una varietat \mathcal{L} provista d'un morfisme

$$\pi: \mathcal{L} \rightarrow X$$

que compleix les propietats següents:

1. Existeix un recobriment obert $\mathcal{U} = \{U_\alpha\}$, i per cada obert d'aquest recobriment U_α un isomorfisme d'espais fibrats

$$\phi_\alpha: \pi^{-1}(U_\alpha) \rightarrow U_\alpha \times \mathbb{C}.$$

Aquests isomorfismes es denominen cartes locals.

2. A la intersecció de dos oberts d'aquest recobriment, $U_{\alpha\beta} = U_\alpha \cap U_\beta$, els canvis de carta

$$U_{\alpha\beta} \times \mathbb{C} \xrightarrow{\phi_\beta^{-1}} \pi^{-1}(U_{\alpha\beta}) \xrightarrow{\phi_\alpha} U_{\alpha\beta} \times \mathbb{C}$$

són lineals en cada fibra i vénen donats per les funcions de transició

$$(x, v) \mapsto (x, g_{\alpha\beta}v).$$

El conjunt de dades format pel recobriment obert $\mathcal{U} = \{U_\alpha\}$ i les cartes locals $\{\phi_\alpha\}$ es denomina una trivialització local del fibrat de línia \mathcal{L} . Podem pensar que un fibrat de línia sobre X és una família d'espais vectorials de dimensió n parametritzada pels punts de X . Localment, el fibrat és trivial, és a dir, té estructura de producte. Tot i això, globalment no és un producte, i són les funcions de transició les que mesuren aquesta falta de trivialitat global. Són precisament les funcions de transició les que determinen un divisor de Cartier. Aquestes funcions de transició depenen de l'elecció d'una trivialització local i, per tant, un fibrat de línia pot donar lloc a diferents divisors de Cartier. Direm que dos divisors de Cartier són equivalents si es poden obtenir mitjançant diferents trivialitzacions locals d'un mateix fibrat de línia. Tècnicament, si $(f_{\alpha\beta})$ i $(g_{\alpha\beta})$ són dos divisors de Cartier definits en el mateix recobriment \mathcal{U} , direm que són equivalents si existeix una col·lecció de funcions $\{u_\alpha\}$, amb u_α regular i sense zeros en l'obert U_α , tal que

$$f_{\alpha\beta} = g_{\alpha\beta} \frac{u_\alpha}{u_\beta}. \quad (13)$$

Observem que les funcions u_α corresponen a canviar la trivialització local del fibrat de línia.

La relació d'equivalència entre divisors de Cartier és compatible amb el producte de divisors de Cartier i, per tant, el conjunt de classes d'equivalència té estructura de grup. Aquest grup es denomina el grup de Picard de X , i el denotarem $\text{Pic}(X)$. Observem que $\text{Pic}(X)$ també és el grup de classes d'isomorfisme de fibrats de línia. A més, el producte de divisors de Cartier correspon al producte tensorial de fibrats de línia (d'aquí la notació emprada).

Les seccions d'un fibrat de línia $\pi: \mathcal{L} \rightarrow X$ són funcions $\sigma: X \rightarrow \mathcal{L}$ tals que $\pi \circ \sigma = \text{Id}$. Aquestes seccions es poden entendre com funcions generalitzades, en les quals el conjunt d'arribada varia a cada punt. Exemples de seccions de fibrats de línia són els elements de volum i les formes modulars. En termes d'una trivialització local, una secció pot descriure's mitjançant una funció en cada obert, sempre que aquestes funcions compleixin unes certes condicions de compatibilitat. Això dóna lloc a la definició següent:

Una secció d'un divisor de Cartier $\mathcal{L} = (g_{\alpha\beta}, \mathcal{U} = \{U_\alpha\})$ és una col·lecció de funcions (σ_α) , amb σ_α definida a l'obert U_α , tals que, en $U_{\alpha\beta} = U_\alpha \cap U_\beta$, es compleix

$$\sigma_\alpha = g_{\alpha\beta} \sigma_\beta.$$

En general, s'entén que una secció no té pols, és a dir, que totes les funcions σ_α són regulars. Quan vulguem posar èmfasi en aquest fet parlarem de seccions regulars. En canvi, parlarem de seccions racionals si admitem la possibilitat que alguna funció σ_α tingui pols. Un fibrat de línia pot no tenir cap secció regular, però sempre té seccions racionals. A partir de la definició, és fàcil veure que, si σ i τ són dues seccions racionals d'un mateix fibrat de línia, llavors el quocient σ/τ és una funció racional. L'espai de seccions regulars de \mathcal{L} es denota $H^0(X, \mathcal{L})$ i la seva dimensió, $h^0(X, \mathcal{L})$.

Introduïrem ara els divisors de Weil. El grup de divisors de Weil d'una varietat algebraica X , que denotarem per $\text{Div}(X)$, és el grup abelià lliure generat per totes les subvarietats irreductibles de codimensió u . Si X és una corba complexa llisa, cosa que suposarem a partir d'ara, les varietats irreductibles de codimensió u són els punts. Per tant, un divisor de Weil d'una corba complexa X és una suma formal de punts

$$D = \sum_{p \in X} n_p p,$$

amb només un nombre finit de coeficients n_p no nuls. Així, podem definir el grau d'un divisor de Weil com

$$\text{deg}(D) = \sum_{p \in X} n_p.$$

Sigui f una funció racional. A la funció f li podem assignar un divisor de Weil comptant els seus zeros i els seus pols:

$$\text{div}(f) = \sum_{p \in X} \text{ord}_p(f) p.$$

El subgrup de $\text{Div}(X)$ generat pels divisors de la forma $\text{div}(f)$ es denomina el grup de divisors racionalment equivalents a zero, i es denota $\text{Rat}(X)$. El quocient és el grup de classes de divisors:

$$\text{Cl}(X) = \text{Div}(X) / \text{Rat}(X).$$

Sigui ara X una corba projectiva. La fórmula dels residus (5) és equivalent a

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

Per tant, tenim un invariant ben definit

$$\text{deg}: \text{Cl}(X) \rightarrow \mathbb{Z}.$$

Vegem la relació que hi ha entre divisors de Weil i divisors de Cartier. Sigui $\mathcal{L} = (f_{\alpha\beta})$ un divisor de Cartier i $\sigma = (\sigma_\alpha)$ una secció racional de \mathcal{L} . Observem que, atès que la funció $f_{\alpha\beta}$ no té zeros ni pols en l'obert $U_{\alpha\beta}$, per tot punt $p \in U_{\alpha\beta}$ tenim

$$\text{ord}_p(\sigma_\alpha) = \text{ord}_p(\sigma_\beta).$$

Té sentit, per tant, definir $\text{ord}_p(\sigma)$. Escrivim

$$\text{div}(\mathcal{L}, \sigma) = \sum_{p \in X} \text{ord}_p(\sigma) p.$$

Com que el quocient de dues seccions σ i σ' de \mathcal{L} és una funció racional, tenim

$$\text{div}(\mathcal{L}, \sigma) - \text{div}(\mathcal{L}, \sigma') \in \text{Rat}(X).$$

I, per tant, una aplicació

$$\text{div}: \text{Pic}(X) \longrightarrow \text{Cl}(X).$$

Aquesta aplicació pot definir-se per qualsevol varietat algebraica i compleix el següent

2 TEOREMA *Sigui X una varietat algebraica llisa. L'aplicació div és un isomorfisme de grups.*

En particular, si X és una corba projectiva, podem definir el grau d'un divisor de Cartier a partir del grau del divisor de Weil corresponent. És a dir, si σ és una secció racional, llavors

$$\text{deg}(\mathcal{L}) = \sum_{p \in X} \text{ord}_p(s).$$

6 El teorema de Riemann-Roch i el teorema de Minkowski

L'analogia entre cossos de nombres i cossos de funcions no passaria de ser una anècdota si es reduís a la fórmula del producte. Existeix, però, un notable parallelisme entre les dues teories. Per exemple, el teorema principal de la teoria de corbes projectives és el teorema de Riemann-Roch, mentre que un teorema fonamental en l'estudi de les unitats de l'anell d'enters d'un cos de nombres és el teorema de Minkowski. En aquesta secció veurem que, escollint adequadament el llenguatge, aquests dos teoremes són anàlegs. Aquesta analogia pot arribar a fer-se molt precisa, però nosaltres discutirem només el seu aspecte més superficial. Per veure una exposició completa d'aquesta analogia el lector pot consultar [27].

El teorema de Riemann-Roch permet decidir si un fibrat de línia té seccions regulars. La seva versió més simple és el teorema de Riemann-Roch asimptòtic.

3 TEOREMA (TEOREMA DE RIEMANN-ROCH ASIMPTÒTIC) *Sigui \mathcal{L} un fibrat de línia sobre una corba complexa projectiva i llisa. Si el grau de \mathcal{L} és suficientement gran, llavors existeixen seccions racionals. En altres paraules,*

$$\text{deg}(\mathcal{L}) \gg 0 \implies H^0(X, \mathcal{L}) \neq 0.$$

Recordem ara el teorema de Minkowski. Una ret Λ és un subgrup discret d'un espai vectorial real V que conté una base de V . Si l'espai vectorial V és euclidià, podem definir el covolum de la ret com el volum d'un recinte fonamental, o com el volum del quocient V/Λ . Si $\{v_1, \dots, v_n\}$ és una base de Λ , llavors

$$\text{CoVol}(\Lambda) = \text{Vol}(V/\Lambda) = \det(v_1, \dots, v_n),$$

on el determinant es calcula respecte a una base ortonormal de V .

El teorema de Minkowski és un criteri d'existència de punts de mida petita en una ret.

4 TEOREMA (TEOREMA DE MINKOWSKI) *Sigui $B \subset \mathbb{R}^N$ un subconjunt convex, compacte, amb simetria central, i sigui Λ una ret de \mathbb{R}^N . Si*

$$\text{Vol}(\mathbb{R}^N/\Lambda) \leq 2^{-N} \text{Vol}(B),$$

llavors existeix $s \in \Lambda \cap B$, $s \neq 0$.

El nostre objectiu és ara veure què tenen en comú tots dos resultats. Per aconseguir-ho, necessitem l'anàleg aritmètic de la teoria de fibrats de línia. Sigui E un cos de nombres i $\mathfrak{v} \subset E$ el seu anell d'enters. En aquest context, un fibrat de línia és un \mathfrak{v} -mòdul lliure de torsió de rang u , L . Les seccions regulars de L són els elements de L . Les seccions racionals de L són precisament els elements de $L_E = L \otimes_{\mathfrak{v}} E$, que és un E -espai vectorial de dimensió u i, per tant, un \mathbb{Q} -espai vectorial de dimensió $d = [E : \mathbb{Q}]$.

Vegem com «compactificar» L . Recordem que els punts de l'infinit de $X = \text{Spec}(\mathfrak{v})$ són les normes arquimedianes del cos E . Per cada norma arquimediàna v podem construir el cos complet E_v que pot ser \mathbb{R} o \mathbb{C} . Per definició, la fibra de L en el punt v serà el E_v -espai vectorial $L_v = L \otimes_{\mathfrak{v}} E_v$.

Hem de decidir ara quan una secció té un pol o un zero en el punt v . Més precisament, ens interessa definir l'ordre d'una secció en un punt de l'infinit. Aquí hem de treballar de nou per analogia. Recordem que, en el cas de les corbes complexes, a cada punt p li corresponia una valoració ord_p , i a partir d'aquesta valoració definíem una norma $\|\cdot\|_p$ donada per

$$\|\sigma\|_p = q^{-\text{ord}_p(\sigma)}.$$

Els zeros i els pols vénen caracteritzats, mitjançant la norma, per

$$\begin{aligned} \|\sigma\|_p < 1 &\iff \sigma \text{ té un zero en } p, \\ \|\sigma\|_p = 1 &\iff \sigma \text{ és invertible en } p, \\ \|\sigma\|_p > 1 &\iff \sigma \text{ té un pol en } p. \end{aligned}$$

En aquest cas procedirem al revés. Escollim una norma en cada espai vectorial L_v . Aquesta norma serà euclidiana si $E_v = \mathbb{R}$ i serà hermitica si $E_v = \mathbb{C}$. Un cop escollides les normes, direm que una secció σ té un zero o un pol en v depenent de si $\|\sigma\|_v$ és menor o major que u , respectivament. A partir de la norma podem definir la valoració

$$\text{ord}_v(\sigma) = -\log \|\sigma\|_v.$$

Observem que ara l'ordre ja no ha de ser un nombre enter, sinó que pot prendre valors reals. A més, el fet que una secció racional tingui un zero o un pol en un punt de l'infinit v depèn no només de L , sinó també de la norma $\|\cdot\|_v$. Això dóna lloc a la definició següent.

5 DEFINICIÓ Un fibrat de línia aritmètic és un parell $\bar{L} = (L, h)$, on L és un fibrat de línia sobre $\text{Spec}(\mathfrak{v})$ i $h = (h_v)$ és la dada d'una norma sobre cada un dels espais vectorials L_v .

Així, una compactificació de L és un fibrat de línia aritmètic $\bar{L} = (L, h)$. Si canviem la norma canviem la compactificació. Això es correspon perfectament amb el cas geomètric. Per exemple, el fibrat de línia trivial \mathcal{O} sobre $\mathbb{A}_{\mathbb{C}}^1$ es pot estendre a qualsevol dels fibrats $\mathcal{O}(n)$, $n \in \mathbb{Z}$, sobre $\mathbb{P}_{\mathbb{C}}^1$. Una manera d'escollir una extensió en concret és decidir quines seccions racionals tenen zeros o pols en el punt de l'infinit i quina és la seva multiplicitat. Aquesta és precisament la informació que està codificada en les normes h_v .

Ara podem definir l'espai de seccions globals regulars d'un fibrat aritmètic L . Aquest espai està format pel conjunt d'elements de L que no tenen pols en cap dels punts de l'infinit v . És a dir:

$$H^0(X, \bar{L}) = \{\sigma \in L \mid \|\sigma\|_v \leq 1, \forall v\}.$$

Continuant amb l'analogia amb el cas geomètric, podem definir el grau d'un fibrat de línia aritmètic \bar{L} . Per intuir la definició correcta de grau aritmètic es poden comparar les versions additives de la fórmula del producte en els casos geomètric i aritmètic (equacions (5) i (9)). Si escollim una secció $\sigma \in L$ llavors el grau aritmètic ve donat per

$$\begin{aligned} \widehat{\text{deg}}(\bar{L}) &= \sum_{\mathfrak{p} \in \text{Spec}(\mathfrak{v})} \log[L/\mathfrak{p}L : (\mathfrak{v}/\mathfrak{p}\mathfrak{v})\sigma] - \sum_v \log(\|\sigma\|_v) \\ &= \log[L : \mathfrak{v}\sigma] - \sum_v \log(\|\sigma\|_v). \end{aligned}$$

Precisament, la fórmula del producte d'Artin ens assegura que aquesta quantitat és independent de l'elecció de la secció σ . És a dir, la fórmula del producte d'Artin juga un paper completament anàleg al que jugava la fórmula dels residus en el cas geomètric.

Considerem l'espai vectorial real $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$. Tenim la descomposició

$$L_{\mathbb{R}} = \bigoplus_v L_v.$$

El conjunt de normes $h = \{h_v\}$ indueix, doncs, una mètrica euclidiana en $L_{\mathbb{R}}$. Denotarem aquesta mètrica també per h . A més L és una ret en $L_{\mathbb{R}}$. Sigui $V = \text{Vol}(L_{\mathbb{R}}/L)$. Es pot demostrar que

$$\widehat{\text{deg}}(\bar{L}) = -\log(V) + \frac{1}{2} \log |D_E|,$$

on D_E és el discriminant del cos E .

Podem aplicar el teorema de Minkowski a aquesta situació. Sigui B el conjunt de punts de $L_{\mathbb{R}}$ de mida petita. Això és

$$B = \{s \in L_{\mathbb{R}} \mid \|s\|_v \leq 1, \forall v\}.$$

Clarament, aquest conjunt B satisfà les hipòtesis del teorema de Minkowski. Si $\widehat{\deg}(\bar{L})$ augmenta, $\text{CoVol}(L)$ disminueix. En particular, si $\widehat{\deg}(\bar{L})$ és prou gran, podem aconseguir que

$$\text{CoVol} \leq 2^{-d} \text{Vol}(B)$$

i pel teorema de Minkowski existeix una secció $0 \neq \sigma \in L$ amb $\|\sigma\|_v \leq 1$ per tot v . En altres paraules, existeix un element $0 \neq \sigma \in H^0(X, \bar{L})$. Per tant, el teorema de Minkowski implica un resultat completament anàleg al teorema de Riemann-Roch.

6 TEOREMA (TEOREMA DE RIEMANN-ROCH ARITMÈTIC ASIMPTÒTIC)

$$\widehat{\deg}(\bar{L}) \gg 0 \implies H^0(X, \bar{L}) \neq \{0\}.$$

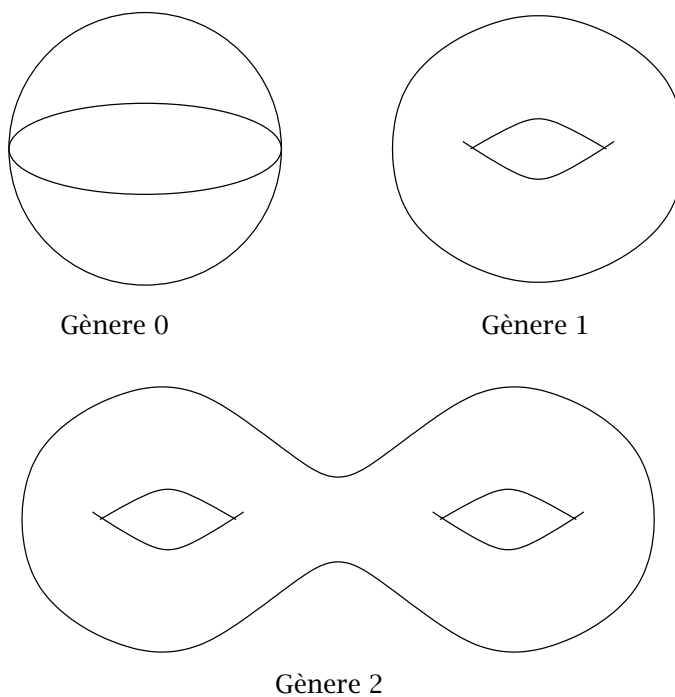


FIGURA 3: Corbes de gènere zero, u i dos.

7 La conjectura de Mordell

El gènere d'una corba complexa llisa i projectiva (vegeu la figura 3) és un invariant per homeomorfisme que caracteritza completament el tipus topològic

de la corba. El valor d'aquest invariant té moltes conseqüències. Per exemple, des d'un punt de vista analític, el gènere és igual a la dimensió de l'espai de les formes diferencials holomorfs sobre la corba.

D'acord amb les seves propietats, en una primera classificació de les corbes, podem dividir-les en tres categories. Gènere zero, gènere u i gènere major o igual que u . Aquesta classificació correspon al que coneixem com dimensió de Kodaira. Gènere zero es equivalent a dimensió de Kodaira negativa, gènere u a dimensió de Kodaira zero i gènere major o igual que u a dimensió de Kodaira u . Aquesta classificació es manifesta en tots els aspectes de la corba.

Des d'un punt de vista analític, tota corba és el quocient d'una varietat complexa simplement connexa per un grup discret d'automorfismes holomorfs. Per gènere zero aquesta varietat és l'esfera de Riemann, per gènere u és el pla complex i per gènere major que u és el semiplà de Poincaré.

Des del punt de vista de la geometria diferencial, tota corba admet una mètrica riemanniana amb curvatura constant. Les corbes de gènere zero tenen curvatura positiva, les de gènere u curvatura zero i les de gènere major que u , curvatura negativa.

Des del punt de vista de la geometria algebraica, en el cas de gènere zero, el fibrat canònic no té seccions, de manera que no existeix el morfisme canònic. En el cas de grau zero, la dimensió de la imatge del morfisme canònic és zero, mentre que per a gènere major o igual que u la imatge del morfisme canònic té dimensió u . Aquesta distinció dóna lloc a la dimensió de Kodaira que comentàvem prèviament.

La classificació mitjançant la dimensió de Kodaira es reflecteix també en el comportament aritmètic de les corbes. Suposem que tenim una corba definida sobre \mathbb{Q} , com per exemple el conjunt de punts del pla projectiu que són solució d'un polinomi amb coeficients racionals. Els punts amb coordenades en \mathbb{Q} s'anomenen punts racionals. En qualsevol dels tres casos pot no existir cap punt racional. És per aquest motiu que ens limitarem a estudiar el cas en què, almenys, hi ha un punt racional. En el cas de gènere zero, l'existència d'un punt racional implica que hi ha tota una família de punts parametrizats per $\mathbb{P}_{\mathbb{Q}}^1$. En el cas de gènere u , el conjunt de punts racionals té estructura de grup abelià. Un teorema demostrat per Mordell assegura que aquest grup abelià és finit generat. Així, el nombre de punts pot ser finit o infinit, depenent del rang del grup. Per últim, la conjectura de Mordell [25], demostrada per Faltings [10], cobreix el cas de gènere major que u :

7 TEOREMA (CONJECTURA DE MORDELL) *Si X és una corba projectiva llisa de gènere major que u , definida sobre \mathbb{Q} . El conjunt de punts racionals és finit.*

Per veure clarament quin és l'anàleg geomètric de la conjectura de Mordell, hem d'elaborar una mica més el concepte de punt racional. Per això, començarem observant que, eliminant els denominadors, podem construir un model X definit sobre \mathbb{Z} de la corba racional X . Aquest model no és únic, però l'elecció d'un model o altre no afectarà el resultat final. A més, podem suposar que X és un esquema regular.

De la mateixa manera que podem veure $\text{Spec}(\mathbb{Z})$ com una corba, el model \mathcal{X} és una superfície fibrada sobre $\text{Spec}(\mathbb{Z})$ (vegeu la figura 4):

$$\pi: \mathcal{X} \rightarrow \text{Spec}(\mathbb{Z}).$$

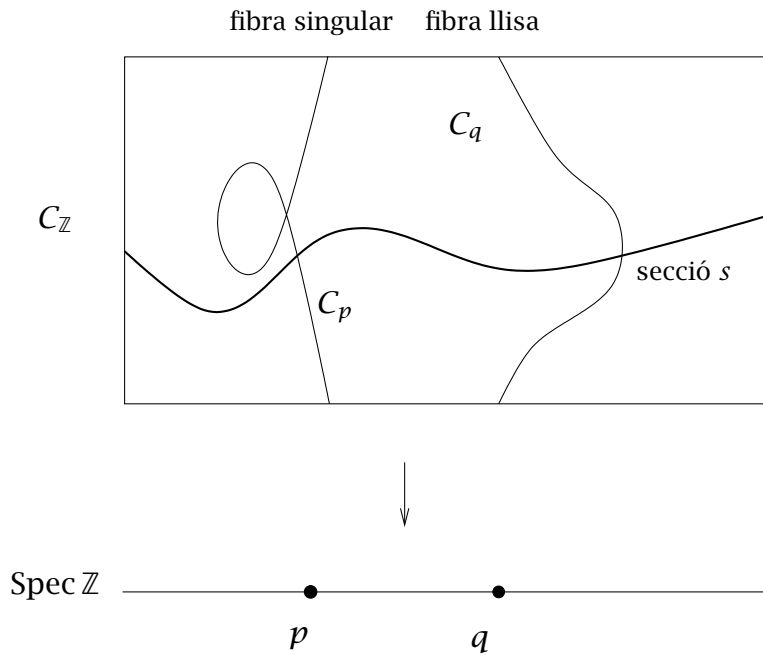


FIGURA 4: Superfície aritmètica.

Així com els punts $p \in \text{Spec}(\mathbb{Z})$ són els nombres primers, la fibra de \mathcal{X} sobre p , que denotarem \mathcal{X}_p , és la reducció mòdul p de \mathcal{X} . Llevat d'un nombre finit de casos, aquesta reducció serà una corba llisa. Ens referirem a \mathcal{X} com una superfície aritmètica.

Donat un punt amb coordenades projectives racionals, després d'eliminar denominadors, obtenim un punt amb coordenades enteres. Podem suposar fins i tot que el màxim comú denominador de les coordenades és u . D'aquesta forma, reduint mòdul p obtenim un punt en cada una de les fibres \mathcal{X}_p . És a dir, donar un punt racional és equivalent a donar una secció de la fibració π .

Ara queda clar a què podem anomenar conjectura de Mordell geomètrica:

8 TEOREMA (CONJECTURA DE MORDELL GEOMÈTRICA) *Sigui $\pi: \mathcal{X} \rightarrow C$ una superfície fibrada sobre una corba C . Suposem que la fibra genèrica és una corba*

llisa de gènere major o igual que dos i que la fibració no és isotrivial, és a dir que les fibres no són isomorfes entre si. Aleshores el nombre de seccions de la fibració és finit.

La versió geomètrica de la conjectura de Mordell va resultar ser més senzilla que la conjectura aritmètica original. Va ser demostrada per Manin l'any 1963 utilitzant la connexió de Gauss-Manin. El 1966 Grauert va donar una nova demostració de la conjectura de Mordell. Un cop demostrada la versió geomètrica de la conjectura, semblava natural intentar adaptar la seva demostració al cas aritmètic. Però en ambdues demostracions s'utilitza de manera essencial l'existència d'un cos base, el cos dels nombres complexos, \mathbb{C} , que té derivacions no trivials. Aquest és un ingredient del qual no es disposa en el cas aritmètic. De manera que, en principi, les dues demostracions no poden adaptar-se a aquest cas.

Posteriorment, Parshin [28] va elaborar una nova estratègia per a la demostració de la conjectura de Mordell relacionant-la amb la conjectura de Shafarevich. La conjectura de Shafarevich assegura que, amb les hipòtesis adequades, només existeix un nombre finit de classes d'isomorfisme de fibracions de corbes no isotrivials. Parshin va demostrar, a més, la conjectura de Shafarevich per famílies de corbes amb bona reducció en tots els punts, i va realitzar importants avenços en el cas general. Arakelov [5] va estendre els treballs de Parshin demostrant la conjectura de Shafarevich i donant una nova demostració de la conjectura de Mordell geomètrica.

En aquest punt, l'argument de la demostració de la conjectura de Mordell geomètrica encara utilitza l'existència de derivacions en el cos base i , per tant, no es pot adaptar al cas aritmètic. Tot i això, una bona part de la demostració es basa en la teoria d'intersecció sobre superfícies. Així, si aquesta estratègia havia de donar una demostració de la conjectura de Mordell aritmètica, un primer pas seria desenvolupar una teoria d'intersecció sobre superfícies aritmètiques. Aquesta teoria hauria de ser capaç de proporcionar invariants numèrics anàlegs al grau i per tant una superfície aritmètica hauria de tenir propietats anàlogues a les d'una varietat completa. Aquesta teoria d'intersecció en superfícies aritmètiques va ser introduïda per Arakelov [4], i és el punt de partida de la Teoria d'Arakelov.

Posteriorment, L. Szpiro va estendre els resultats de Parshin i Arakelov al cas de característica positiva. A més, amb el seu treball, va quedar clar quins eren els problemes que s'havien de resoldre per tal que aquesta estratègia conduís a una demostració de la conjectura de Mordell [30], [31]. Aquests problemes van ser finalment resolts per Faltings [10], que va publicar una demostració de la conjectura de Mordell l'any 1983.

8 Rudiments de la Teoria d'Arakelov

En aquesta secció donarem unes breus nocions de la Teoria d'Arakelov. Per simplificar, ens centrarem únicament en el cas de les superfícies aritmètiques

sobre $\text{Spec}(\mathbb{Z})$. Convé notar, per una part, que la teoria ha estat estesa a qualsevol dimensió per Gillet i Soulé i, per l'altra, que es poden considerar varietats aritmètiques sobre bases més generals, com l'anell d'enters d'un cos de nombres.

Un altre detall a tenir en compte és que, en la teoria original, Arakelov imposa certa condició d'harmonicitat. Però en no ser el producte exterior de dues formes diferencials harmòniques necessàriament harmònic, aquesta condició es va descartar a l'hora d'elaborar la generalització a dimensió superior. És per aquest motiu que en aquesta secció no en farem cap referència.

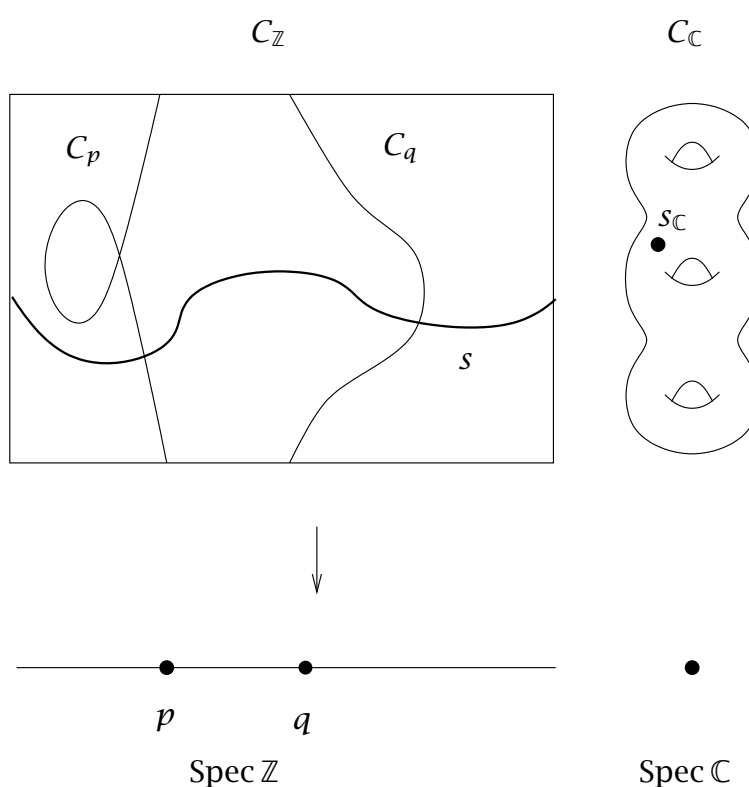


FIGURA 5: Superfície aritmètica compactificada.

Sigui $\mathcal{X} \rightarrow \text{Spec}(\mathbb{Z})$ un esquema regular, pla i projectiu sobre $\text{Spec}(\mathbb{Z})$, de dimensió relativa u . És a dir, \mathcal{X} és una superfície aritmètica. Com que $\text{Spec}(\mathbb{Z})$ no és una varietat projectiva, \mathcal{X} no es comporta globalment com una varietat projectiva. Per exemple, no podem construir un producte d'intersecció no trivial que sigui invariant per equivalència racional. El nostre primer objectiu serà compactificar \mathcal{X} .

Per a compactificar $\text{Spec}(\mathbb{Z})$ afegim un punt, que corresponia a la immersió $\mathbb{Z} \rightarrow \mathbb{R}$. En conseqüència, per a compactificar X , haurem d'afegir la fibra en aquest punt. Aquesta fibra serà la varietat real $X_{\mathbb{R}} = X \otimes_{\mathbb{Z}} \mathbb{R}$. Ara bé, la varietat real $X_{\mathbb{R}}$ està determinada pel parell $(X_{\mathbb{C}}, F)$, on $X_{\mathbb{C}}$ és la varietat complexa $X_{\mathbb{C}} = X_{\mathbb{R}} \otimes \mathbb{C}$ i F és la involució antilineal definida per conjugació complexa. Per simplificar la discussió, treballarem únicament amb la varietat $X_{\mathbb{C}}$. Però, per ser precisos, a tots els objectes que definim sobre $X_{\mathbb{C}}$ se'ls hauria d'imposar una condició de compatibilitat amb la conjugació complexa F .

La varietat aritmètica compactificada \overline{X} té l'aspecte de la figura 5. Tot objecte aritmètic ha d'estar necessàriament format per dos components. Una part definida sobre la varietat entera X , i una altra part sobre la varietat complexa $X_{\mathbb{C}}$. Observem que totes dues varietats són de naturalesa molt diferent; no tenen, per exemple, la mateixa dimensió. Els dos components d'un objecte aritmètic seran, en conseqüència, també molt diferents.

Una part important de la geometria algebraica que es vol imitar en la teoria d'Arakelov és la relació entre fibrats vectorials i cicles algebraics. Aquesta relació es realitza mitjançant l'ús de classes característiques. El seu aspecte més senzill és la relació entre divisors de Cartier (fibrats de línia o fibrats vectorials de rang u) i divisors de Weil (cicles algebraics de codimensió u), que ja vam discutir en el cas d'una varietat aritmètica de dimensió u . Generalitzarem ara aquesta discussió al cas de les superfícies aritmètiques.

Com en el cas de dimensió u , un fibrat de línia aritmètic és un parell (\mathcal{L}, h) on \mathcal{L} és un fibrat de línia sobre X i h és una mètrica hermitica sobre el fibrat de línia $L_{\mathbb{C}}$. (Més precisament, a la mètrica h se li ha d'imposar el fet de ser F -invariant). El grup de Picard aritmètic de X , $\widehat{\text{Pic}}(X)$, és el grup de classes d'isometria de fibrats de línia sobre X . És a dir, dos fibrats hermitics són equivalents si existeix un isomorfisme entre ells que conservi les mètriques.

Vegem ara què és un divisor de Weil aritmètic. El component sobre X és un divisor de Weil algebraic en el sentit usual, és a dir, una combinació lineal formal de subvarietats de codimensió u . El punt clau és escollir com és el component sobre $X_{\mathbb{C}}$. És lògic imposar que els components sobre X i sobre $X_{\mathbb{C}}$ estiguin relacionats. Un divisor de Weil D sobre X determina al seu torn un divisor $D_{\mathbb{C}}$ sobre $X_{\mathbb{C}}$. Aquest divisor és una combinació lineal de punts:

$$D_{\mathbb{C}} = \sum n_p p.$$

Però el component sobre $X_{\mathbb{C}}$ ha de ser un objecte de codimensió u en \overline{X} . Donat que $X_{\mathbb{C}}$ ja té codimensió u en \overline{X} , resulta que aquest objecte ha de tenir codimensió zero en $X_{\mathbb{C}}$. Donat que el divisor $D_{\mathbb{C}}$ té codimensió u en $X_{\mathbb{C}}$, el component sobre $X_{\mathbb{C}}$ no pot ser simplement el divisor $D_{\mathbb{C}}$, sinó un objecte relacionat amb ell, però que es comporti com si tingués codimensió zero en $X_{\mathbb{C}}$. Un exemple d'objectes de codimensió zero són les funcions. D'això en resulta que un possible candidat al component sobre $X_{\mathbb{C}}$ del divisor D sigui una funció que determini el divisor $D_{\mathbb{C}}$. Aquestes consideracions (i algunes altres, com el teorema 9) ens porten a definir un divisor aritmètic com

un parell $\hat{D} = (D, g_D)$, on D és un divisor de Weil sobre X i g_D una funció de Green per D_C , que definirem tot seguit.

Si C és una corba complexa llisa i $D = \sum n_p p$ és un divisor, llavors una funció de Green per D és una funció diferenciable sobre $C - D$, tal que en un entorn coordinat al voltant del punt $p \in C$ pot escriure's com

$$g_D(t) = f(t) - n_p \log(\|t\|^2), \quad (14)$$

amb f una funció diferenciable.

Vegem un exemple de funció de Green. Sigui f una funció racional i sigui $D = \text{div}(f)$ el seu divisor associat. Llavors $-\log(\|f\|^2)$ és una funció de Green per D .

Observem que, a partir del divisor aritmètic $\hat{D} = (D, g_D)$, podem construir una 2-forma diferencial

$$\omega(\hat{D}) = \frac{1}{2\pi i} \partial \bar{\partial} g_D.$$

A partir de l'equació (14), es pot veure que $\omega(\hat{D})$ s'estén a una 2-forma diferencial llisa sobre tota la corba X_C . Aquesta forma diferencial representa la mateixa classe de cohomologia que el divisor D_C .

Donat que la suma de dues funcions de Green per dos divisors és una funció de Green per la suma de divisors, es té que el conjunt dels divisors aritmètics $\widehat{\text{Div}}(\overline{X})$ té estructura de grup.

Designarem per $\widehat{\text{Rat}}(\overline{X})$ el subgrup de $\widehat{\text{Div}}(\overline{X})$ generat pels divisors de la forma $\widehat{\text{div}}(f) = (\text{div}(f), -\log(\|f\|^2))$, on f és una funció racional en \overline{X} . Aquests divisors es denominen divisors racionalment equivalents a zero. El grup de classes de divisors és el quocient

$$\widehat{\text{CH}}^1(\overline{X}) = \widehat{\text{Div}}(\overline{X}) / \widehat{\text{Rat}}(\overline{X}).$$

Sigui ara (\mathcal{L}, h) un fibrat de línia hermitic, i sigui s una secció de \mathcal{L} . Aleshores

$$\widehat{\text{div}}(s) = (\text{div}(s), -\log(h(s)))$$

és un divisor aritmètic. A més, si s' és una altra secció, el divisor $\widehat{\text{div}}(s') - \widehat{\text{div}}(s)$ és racionalment equivalent a zero. Per tant, obtenim una aplicació

$$\widehat{\text{div}}: \widehat{\text{Pic}}(\overline{X}) \rightarrow \widehat{\text{CH}}^1(\overline{X}).$$

El resultat següent demostra que l'elecció de la funció de Green com al component sobre X_C és adequada:

9 TEOREMA *L'aplicació $\widehat{\text{div}}$ és un isomorfisme de grups.*

El problema següent és construir un producte d'intersecció entre divisors aritmètics (l'anàleg a comptar punts d'intersecció entre corbes planes).

Siguin $\hat{D} = (D, g_D)$ i $\hat{E} = (E, g_E)$ dos divisors aritmètics. Suposarem que D i E no tenen components comuns. Volem definir un producte d'intersecció (\hat{D}, \hat{E}) . Aquest producte d'intersecció el podrem descompondre com

$$(\hat{D}, \hat{E}) = (\hat{D}, \hat{E})_{\text{fin}} + (\hat{D}, \hat{E})_{\infty}.$$

El component finit $(\hat{D}, \hat{E})_{\text{fin}}$ es construeix a partir de les multiplicitats d'intersecció, i la seva definició és purament algebromètrica.

El component a l'infinit es calcula a partir de les funcions de Green:

$$(\hat{D}, \hat{E})_{\infty} = g_D(E_{\infty}) + \frac{1}{2\pi i} \int_{X_{\infty}} g_E \partial \bar{\partial} g_D,$$

on, si $E_{\infty} = \sum n_p p$, llavors $g_D(E_{\infty}) = \sum n_p g_D(p)$. Observem que, en no tenir els divisors D i E components comuns, els dos termes de la dreta de la igualtat anterior estan ben definits. Observem també que aquesta fórmula no és arbitrària, sinó que ve imposada per les propietats que volem obtenir del producte d'intersecció. En particular, la propietat de simetria i el fet que, si $\hat{D} = \widehat{\text{div}} f$ o $\hat{E} = \widehat{\text{div}} f$, llavors $(\hat{D}, \hat{E}) = 0$. Aquesta última propietat és conseqüència de la fórmula del producte. A partir d'aquí es pot demostrar el resultat bàsic de la teoria d'Arakelov:

10 TEOREMA *Sigui \bar{X} una superfície aritmètica «compactificada», projectiva sobre $\text{Spec}(\mathbb{Z})$. El producte d'intersecció de cicles indueix un producte bilineal simètric no trivial*

$$\widehat{\text{CH}}^1(\bar{X}) \otimes \widehat{\text{CH}}^1(\bar{X}) \rightarrow \mathbb{R}.$$

En aquest punt disposem d'un llenguatge i unes eines per a les superfícies aritmètiques completament anàlegs al llenguatge i eines usals en les superfícies algebraiques. Les preguntes que, de manera natural, ens plantegem ara són les següents: fins a quin punt es pot desenvolupar aquesta analogia? És una analogia purament formal, o, com en el cas de les corbes, podem traduir els teoremes clàssics de la geometria algebraica de superfícies al cas aritmètic? La resposta és que l'analogia pot arribar a fer-se extremadament precisa, i que la gran majoria dels teoremes geomètrics tenen un anàleg aritmètic. Han estat demostrats, per exemple, l'anàleg del teorema de l'índex de Hodge per Néron, Faltings [11] i Hriljac [18], la fórmula d'adjunció, per Arakelov, i el teorema de Riemann-Roch, per Faltings [11].

9 Alguns progressos recents en teoria d'Arakelov

Acabarem aquesta nota fent un breu comentari sobre el desenvolupament de la teoria d'Arakelov en aquests darrers anys. Aquest comentari no és exhaustiu, i només pretén donar una visió de conjunt d'algunes de les línies actuals d'investigació.

Una primera línia de treball és la fonamentació i el desenvolupament dels conceptes bàsics de la teoria. En aquest apartat podem destacar la introducció, per H. Gillet i C. Soulé, dels anells de Chow aritmètics per varietats de dimensió superior, de la teoria K aritmètica i de les classes de Chern aritmètiques que relacionen tots dos conceptes, [14], [15]. També podem mencionar l'extensió a les varietats quasiprojectives per l'autor [9], la generalització a fibrats vectorials amb diferents tipus de mètriques degenerades per A. Moriwaki [26], V. Maillot [24] i U. Kühn [20] i l'estudi de les varietats singulars per W. Aitken [3].

Una altra línia de treball important és la demostració dels anàlegs aritmètics dels principals teoremes de la geometria algebraica. Un lloc central en aquest apartat l'ocupa el teorema de Riemann-Roch aritmètic per Gillet i Soulé [16] i Faltings [12]. Aquest resultat depèn, en gran mesura, dels treballs de J. M. Bismut sobre torsió analítica. Altres resultats importants són el teorema de Bézout aritmètic per Bost, Gillet i Soulé [7], la fórmula de Hilbert Samuel, obtinguda per Gillet i Soulé a partir del teorema de Riemann-Roch aritmètic i posteriorment per Abbes i Bouche [1], un teorema d'Adams-Riemann-Roch per Roessler [29], el teorema del punt fix de Lefschetz (Köhler i Roessler [19]) (una versió equivariant del teorema de Riemann-Roch), l'anàleg d'un altre teorema de Lefschetz sobre la relació entre el grup fonamental d'una varietat i el d'un divisor (Bost [6]), els anàlegs aritmètics de les conjectures estàndards per varietats abelianes (Künnemann [21]) i varietats que admeten una descomposició cel·lular (Künnemann i Maillot [22]) i un anàleg del criteri de Cayley-Bacharach (Gasbarri [13]).

Una tercera línia de treball són els càlculs explícits en teoria d'Arakelov. Un problema important és trobar cotes per a l'autointersecció del fibrat canònic d'una superfície aritmètica. L'interès d'aquest problema està en el fet que l'obtenció d'una cota general permetria demostrar una versió efectiva de la conjectura de Mordell. S'han trobat cotes per les superfícies aritmètiques obtingudes a partir de corbes de gènere dos per Bost, Mestre i Moret-Bailly [8] i per corbes modulars (Abbes, Ullmo [2]). També podem esmentar en aquest apartat la nova relació entre els diferents invariants analítics d'una superfície de Riemann obtinguda per J. Guàrdia [17]. En un altre camp diferent, s'han obtingut fórmules explícites pels números d'intersecció aritmètics en Grasmannianes (Maillot [23], Tamvakis [33]) i varietats de banderes (Tamvakis [32]).

Finalment, cal destacar els progressos en teoria d'altures i l'aproximació diofàntica realitzats per nombrosos autors com ara Batirev, Bombieri, Michell, Morivaki, Szpiro, Tschinkel, Ullmo, Zhang i d'altres.

Referències

- [1] ABBES, A.; BOUCHE T. «Théorème de Hilbert-Samuel arithmétique». *Ann. Inst. Fourier* [Grenoble], **45** (1995), 375–401.

- [2] ABBES, A.; ULLMO, E. «Auto-intersection du dualisant relatif des courbes modulaires $X_0(N)$ ». *J. Reine Angew. Math.*, **484** (1997), 1–70.
- [3] AITKEN, W. «An arithmetic Riemann-Roch theorem for singular arithmetic surfaces». *Mem. Amer. Math. Soc.*, vol. 120, (1996). American Mathematical Society.
- [4] ARAKELOV, S. «An intersection theory for divisors on an arithmetic surface». *Math. USSR Izv.*, **8** (1974), 1167–1180.
- [5] ARAKELOV, S. «Families of curves with fixed degeneracies». *Math. USSR Izv.*, **5** (1979), 1277–1302.
- [6] BOST, J.-B. «Potential theory and Lefschetz theorems for arithmetic surfaces». *Ann. Sci. École Norm. Sup.*, **32** (1999), 241–312.
- [7] BOST, J.-B.; GILLET, H.; SOULÉ C. «Heights of projective varieties and positive Green forms». *J. Amer. Math. Soc.*, **7** (1994), 903–1027.
- [8] BOST, J. B.; MESTRE, J. F.; MORET-BAILLY, L. «Sur le calcul explicite des classes de Chern des surfaces arithmétiques de genre 2». *Séminaire sur les Pinceaux de Courbes Elliptiques, Asterisque*, vol. 183, (1990), 69–105.
- [9] BURGOS, J. I. «Arithmetic Chow rings and Deligne-Beilinson cohomology». *Journal of Algebraic Geometry*, **6** (1997), 335–377.
- [10] FALTINGS, G. «Endlichkeitssätze für abelsche Varietäten über Zahlkörpern». *Invent. Math.*, **73** (1983), 349–366.
- [11] FALTINGS, G. «Calculus on arithmetic surfaces». *Ann. of Math.*, **119** (1984), 387–424.
- [12] FALTINGS, G. «Lectures on the arithmetic Riemann-Roch theorem». *Annals of Mathematics Studies*, vol. 127, (1992), [Princeton University Press].
- [13] GASBARRI, C. «Hermitian vector bundles of rank two and adjoint systems on arithmetic surfaces». *Topology*, **38** (1999), 1161–1174.
- [14] GILLET, H.; SOULÉ C. «Arithmetic intersection theory». *Publ. Math. IHES*, **72** (1990), 94–174.
- [15] GILLET, H.; SOULÉ C. «Characteristic classes for algebraic vector bundles with hermitian metric I, II». *Annals of Mathematics*, **131** (1990), 163–203, 205–238.
- [16] GILLET, H.; SOULÉ C. «An arithmetic Riemann-Roch theorem». *Invent. Math.*, **110** (1992), 473–543.
- [17] GUÀRDIA, J. «Analytic invariants in Arakelov theory for curves». *C. R. Acad. Sci. Paris*, **329** (1999), 41–46.
- [18] HRILJAC. «Heights and Arakelov’s intersection theory». *Amer. J. Math.*, **107** (1985), 33–38.
- [19] KÖHLER, K.; ROESSLER, D. «Un théorème du point fixe de Lefschetz en géométrie d’Arakelov». *C. R. Acad. Sci. Paris*, (1998), 719–722.
- [20] KÜHN, U. «Generalized arithmetic intersection numbers», to appear in *J. Crelle*.

- [21] KÜNNEMANN, K. «Arakelov chow groups of abelian schemes, arithmetic Fourier transform and analogues of the standard conjectures of Lefschetz type». *Math. Ann.*, **300** (1994), 365–392.
- [22] KÜNNEMANN, K.; MAILLOT, V. *Regulators in analysis, geometry and number theory*. Progr. Math., vol. 171, ch. Théorèmes de Lefschetz et de Hodge arithmétiques pour les variétés admettant une décomposition cellulaire. Birkhäuser Boston, 2000.
- [23] MAILLOT, V. «Un calcul de Shubert arithmétique». *Duke Math. J.*, **80** (1995), 195–221.
- [24] MAILLOT, V. «Géométrie d'Arakelov des variétés toriques et fibrés en droites intégrables». *Mém. Soc. Math. Fr.*, **80** (2000).
- [25] MORDELL, L. J. «On the rational solutions of the indeterminate equation of third and fourth degrees». *Proc. Cambridge Phil. Soc.*, **21** (1922), 179–192.
- [26] MORIWAKI, A. *Intersection pairing for arithmetic cycles with degenerate Green currents*. Alg-Geom preprints: math A:G/9803054.
- [27] NEUKIRCH, J. *Algebraic number theory*. Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer-Verlag, 1999.
- [28] PARSHIN, A. «Algebraic curves over function fields I». *Math. USSR Izv.*, **2** (1968), 1145–1170.
- [29] ROESSLER, D. «An Adams-Riemann-Roch theorem in Arakelov geometry». *Duke Math. J.*, **96** (1999), 61–126.
- [30] SZPIRO, L. «Sur le théorème de rigidité de Parshin et Arakelov». *Asterisque*, **64** (1974), 169–202.
- [31] SZPIRO, L. «Séminaire sur les pinceaux de courbes de genre au moins deux». *Asterisque*, **86** (1981).
- [32] TAMVAKIS, H. «Arithmetic intersection theory on flag varieties». *Math. Ann.*, **314** (1999), 207–223.
- [33] TAMVAKIS, H. «Schubert calculus on the arithmetic grassmannian». *Duke Math. J.*, **98** (1999), 421–443.

DEPARTAMENT D'ÀLGEBRA I GEOMETRIA
FACULTAT DE MATEMÀTIQUES
UNIVERSITAT DE BARCELONA
GRAN VIA DE LES CORTS CATALANES, 585
08007 BARCELONA
burgos@mat.ub.es