NOTES DEL SEMINARI

DIBUIXOS D'INFANTS

Barcelona *2005*

12

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

DIBUIXOS D'INFANTS

Edició a cura de

T. Crespo i X. Xarles

Amb contribucions de

T. Crespo B. Plans J. Roé X. Xarles

X. Xarles
Dep. de Matemàtiques
Edifici C
Univ. Autònoma de
Barcelona
08193 Bellaterra
Espanya

T. Crespo
Fac. de Matemàtiques
Univ. de Barcelona
Gran Via de les Corts
Catalanes, 585
08007 Barcelona
Espanya

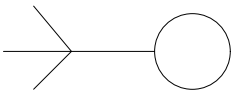
Classificació AMS
Primària: 11G30, 11G05, 14H25, 14H30, 14Q05
Secundària: 11G18, 14G35, 14G25, 13P10

Barcelona, 2004
Amb suport parcial de MCYT, BFM-2003-06092

ISBN: 84-934244-0-4

Índex

Introducció



Cela tient sûrement à la nature tellement familière, non technique, des objets considérés, dont tout dessin d'enfant griffonné sur un bout de papier donne un exemple parfaitement explicite.
Alexander Grothendieck.

Aquestes notes contenen les conferències sobre dibuixos d'infants presentades en la divuitena edició del Seminari de Teoria de Nombres (UB-UAB-UPC), celebrat de l'1 al 8 de Febrer de 2004 a Barcelona, a la Facultat de Nàutica de la Universitat Politècnica de Catalunya.

El programa general va ser elaborat per T. Crespo i X. Xarles i les sessions varen ser dutes a terme per diferents persones del seminari, gràcies a les quals tenim les notes que presentem aquí.

L'any 1978, el matemàtic rus G. V. Belyĭ va explicar en el congrés internacional de matemàtiques de Helsinki una demostració elemental d'un teorema aparentment innocent: *Una corba algebraica definida sobre* $\mathbb{C}$ *està definida sobre un cos de nombres si i només si té un morfisme a* $\mathbb{P}^1$ *ramificat només en tres punts* [3].

Mentrestant, Alexander Grothendieck, "retirat" de les matemàtiques actives a Montpeller, estava estudiant aquests tipus de recobriments de $\mathbb{P}^1$, assignant a cadascun d'ells un graf d'un cert tipus

dibuixat sobre la superfície de Riemann associada a la corba complexa. Així, quan va sentir parlar del Teorema de Belyĭ, s'adonà ràpidament que tenia una manera "elemental" de veure les corbes algebraiques sobre cossos de nombres.

L'any 1984, Grothendieck va escriure el seu famós "Esquisse d'un programme" [15] on descrivia la recerca que havia estat fent i el seu projecte pels següents anys. Allí parlava de com un objecte tan "senzill" com un dibuix d'un infant ens determinava una corba algebraica i un morfisme a $\mathbb{P}^1$ definits tots dos sobre un cos de nombres (i en particular ens determinava un cos de nombres). Ell considerava que un estudi detallat d'aquesta correspondència permetria una comprensió més profunda i senzilla dels cossos de nombres, de les corbes algebraiques, del grup de Galois absolut de $\mathbb{Q}$, etc.

L'objectiu d'aquest seminari va ser d'entendre la correspondència de Grothendieck entre "dibuixos d'infants" i corbes algebraiques sobre cossos de nombres, i veure fins a on és possible fer efectiva aquesta correspondència.

En el primer capítol es demostra el teorema de Belyĭ i el resultat famós d'Elkies provant que la conjectura ABC implica Mordell efectiu, o sigui que per a tota corba de gènere més gran que 1 hi ha un procediment efectiu per a trobar tots els seus punts racionals. En la segona xerrada s'introdueixen els dibuixos d'infants des de varis punts de vista i la correspondència entre dibuixos i morfismes de Belyĭ, es parla breument del cos de definició i del cos de moduli del dibuix, i finalment s'estudien breument alguns exemples bàsics de dibuixos: els dibuixos en gènere 0, els dibuixos associats a corbes el·líptiques, les corbes de Fermat i les corbes amb molts automorfismes. Els dos capítols següents es centren en els casos de gènere 0 i de gènere 1; la idea és veure resultats precisos sobre com passar explícitament del morfisme de Belyĭ al dibuix i viceversa, i també la relació entre el dibuix i altres invariants coneguts de la corba.

T. Crespo i X. Xarles

Bellaterra, 24 de Desembre de 2004.

Capítol 1

El Teorema de Belyi (dels tres punts)

Bernat Plans

Introducció

Aquest capítol està centrat en el resultat de G. V. Belyi [3, Thm. 4]:

1.0.1 Teorema. (de Belyi dels tres punts) *Per a una corba projectiva i llisa X sobre $\mathbb{C}$, són equivalents:*

(i) *X es pot definir sobre $\overline{\mathbb{Q}}$.*

(ii) *Existeix algun morfisme no constant $f : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ ramificat en, com a màxim, tres punts.*

En (ii), composant amb una transformació lineal fraccionària convenient, podem suposar que els punts de ramificació de f pertanyen, per exemple, a $\{0, 1, \infty\}$. Així, la implicació $(ii) \Rightarrow (i)$ (la "part òbvia"del Teorema de Belyi) és conseqüència del fet que, en les hipòtesis anteriors, f i X es poden definir sobre $\overline{\mathbb{Q}}$ si (i només si) la ramificació de f pertany a $\mathbb{P}^1(\overline{\mathbb{Q}})$. Donem una demostració d'aquest resultat a la Secció 1.2.

En la Secció 1.3 demostrem la implicació $(i) \Rightarrow (ii)$ (Teorema de Belyi pròpiament dit). Una conseqüència d'aquest resultat (reiteradament destacada en [15]) és que el grup de Galois absolut $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ s'injecta en el grup d'automorfismes externs del grup (profinit lliure amb dos generadors) $\pi_1^{alg}\left(\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash\{0,1,\infty\}\right)$. Idealment, això hauria de ser el punt de partida per a obtenir una presentació de $G_{\mathbb{Q}}$.

Finalment, la Secció 1.4 està dedicada a un exemple d'aplicació del Teorema de Belyi. Concretament, es tracta de veure un resultat d'Elkies que estableix: ABC efectiva $\Rightarrow$ Mordell efectiu.

1.1 Recobriments de $\mathbb{P}^1$

Aquest apartat és de caràcter preliminar. L'objectiu és, únicament, recordar alguns resultats clàssics (essencialment el Teorema d'existència de Riemann). En particular, hi ha poques definicions i cap demostració. Com a referència bàsica, hem seguit [9].

Podem pensar en $\mathbb{P}^1(\mathbb{C})$ com a espai topològic, com a superfície de Riemann o com el conjunt de punts definits sobre $\mathbb{C}$ de la varietat algebraica $\mathbb{P}^1_{\mathbb{C}}$. De la mateixa manera, podem parlar de recobriments *topològics* (d'oberts) de $\mathbb{P}^1(\mathbb{C})$, recobriments *analítics* de $\mathbb{P}^1(\mathbb{C})$ o recobriments *algebraics* de $\mathbb{P}^1_{\mathbb{C}}$. Concretament, si $S \subset \mathbb{P}^1(\mathbb{C})$ és un conjunt finit, ens interessen els:

(i) Recobriments topològics *finits* $f : U \to \mathbb{P}^1(\mathbb{C})\backslash S$ d'espais topològics *connexos*. És a dir, U és connex i f és una aplicació recobridora amb fibres finites.

(ii) Recobriments analítics $f : X \to \mathbb{P}^1(\mathbb{C})$ de superfícies de Riemann *compactes i connexes*, no ramificats fora de S. És a dir, X és una superfície de Riemann compacta i connexa i f és una aplicació holomorfa no constant. En aquest cas, f és necessàriament *finit*.

(iii) Recobriments algebraics $f : X \to \mathbb{P}^1_{\mathbb{C}}$ de corbes *projectives i llises* sobre $\mathbb{C}$, no ramificats fora de S. És a dir, X és una corba projectiva i llisa sobre $\mathbb{C}$ i f és un morfisme algebraic no constant. En aquest cas, f és necessàriament *finit*.

En tots tres casos, un *morfisme de recobriments* es defineix per la commutativitat del diagrama (triangular) evident.

Per a nosaltres, el fet essencial és que, en cert sentit, aquests tres conceptes són equivalents. Concretament, (una de les múltiples versions de) el **Teorema d'existència de Riemann** estableix:

1.1.1 Teorema. *Donat un conjunt finit* $S \subset \mathbb{P}^1(\mathbb{C})$*, les tres categories definides per (i), (ii) i (iii) són equivalents. En particular, es tenen bijeccions entre els respectius conjunts de classes d'equivalència de "recobriments de* $\mathbb{P}^1$*"(és a dir, classes d'isomorfisme en les respectives categories).*

1.1.2 Observació. Aquest resultat és bàsic a l'hora de veure l'equivalència entre diverses interpretacions dels *dibuixos d'infants* (veure capítol següent).

En el Teorema anterior, a més, l'equivalència enunciada es pot definir pels functors naturals "oblit"(i restricció) de (ii) a (i) i de (iii) a (i). La dificultat principal és demostrar que són plenament fidels i essencialment exhaustius i que, per tant, defineixen equivalències de categories. D'altra banda, és ben conegut que el functor "cos de funcions racionals"(resp. meromorfes) estableix una (anti)equivalència entre (iii) (resp. (ii)) i la categoria de:

(iv) Extensions *finites* $K/\mathbb{C}(T)$ de cossos, no ramificades fora de S. Aquí, els morfismes són els $\mathbb{C}(T)$-morfismes.

Això estableix una equivalència entre (ii) i (iii), compatible amb les equivalències ja esmentades.

Fixat un punt base $x_0 \in \mathbb{P}^1(\mathbb{C})\backslash S$, el grup fonamental topològic $\pi_1^{top}(\mathbb{P}^1(\mathbb{C})\backslash S, x_0)$ és isomorf al grup de transformacions recobridores del recobriment universal de $\mathbb{P}^1(\mathbb{C})\backslash S$. Així s'obté una bijecció entre classes d'equivalència de recobriments de (i) i classes de conjugació de subgrups d'índex finit de $\pi_1^{top}(\mathbb{P}^1(\mathbb{C})\backslash S, x_0)$. A més, es té

$$\pi_1^{top}(\mathbb{P}^1(\mathbb{C})\backslash S, x_0) \cong F_s,$$

on $s+1$ és el cardinal de S i F_s denota el grup lliure en s generadors.

D'altra banda, en una clausura algebraica fixada de $\mathbb{C}(T)$, podem considerar la màxima subextensió $\mathbb{C}(T)^S/\mathbb{C}(T)$ no ramificada fora de S i definir el grup fonamental algebraic de $\mathbb{P}^1_{\mathbb{C}}\backslash S$ com:

$$\pi_1^{alg}(\mathbb{P}^1_{\mathbb{C}}\backslash S) := \mathrm{Gal}\left(\mathbb{C}(T)^S/\mathbb{C}(T)\right).$$

1.1.3 Observació. En la Secció 1.3 també parlarem del grup fonamental algebriac de $\mathbb{P}^1_L\backslash S$, per a certs cossos $L \subset \mathbb{C}$. La definició és anàloga, entenent que el conjunt S ha d'estar definit sobre el cos L.

Les classes de conjugació de subgrups d'índex finit de $\pi_1^{alg}(\mathbb{P}^1_{\mathbb{C}}\backslash S)$ corresponen bijectivament a les classes d'isomorfisme d'extensions de (iv) i, per tant, a les classes d'equivalència en (i), (ii) i (iii). De fet, es té

$$\pi_1^{alg}(\mathbb{P}^1_{\mathbb{C}}\backslash S) \cong \widehat{F_s},$$

on $\widehat{F_s}$ denota la compleció profinita de F_s. És a dir, $\pi_1^{alg}(\mathbb{P}^1_{\mathbb{C}}\backslash S)$ és un grup profinit lliure en s generadors.

1.1.4 Observació. Donat un grup finit G i un natural s, només hi ha un nombre finit d'epimorfismes $F_s \to G$, per ser F_s finitament generat. Així, fixat un conjunt finit $S \subset \mathbb{P}^1(\mathbb{C})$ de cardinal $s+1$, només hi ha un nombre finit d'extensions de Galois finites de $\mathbb{C}(T)$ (en una clausura algebraica fixada) no ramificades fora de S i amb grup de Galois isomorf a G. Aquest és un dels fets clau en la demostració de la part òbvia del Teorema de Belyi que donem en la secció següent.

1.2 La "part òbvia"del Teorema de Belyi

L'objectiu d'aquesta secció és demostrar la implicació $(ii) \Rightarrow (i)$ del Teorema 1.0.1, que es coneix com la "part òbvia"del Teorema de Belyi. Es tracta d'una conseqüència directa del següent resultat, anterior a Belyi.

1.2.1 Teorema. *Sigui $f : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ un recobriment de corbes projectives i llises sobre $\mathbb{C}$. Si els punts de ramificació de f són $\overline{\mathbb{Q}}$-racionals, aleshores f i X es poden definir sobre $\overline{\mathbb{Q}}$.*

En [3], Belyi pràcticament es limita a dir que es tracta d'una conseqüència del criteri de Weil (i cita [31]). Detalls sobre aquesta afirmació i demostracions alternatives del Teorema 1.2.1 (i generalitzacions) es troben, per exemple, en [14, XIII, Cor. 2.12], [13, Lemma 1.2], [25, Thm. 6.3.3], [34], [20, Cap. I, Prop. 2.1], [9, § 12], [17], [18], ...

La prova que donem a continuació es troba, essencialment, en [30, Cap. 7]. Abans, però, és convenient recordar el següent fet elemental (veure també, per exemple, [30, Lemma 1.1]).

1.2.2 Lema. *El grau de qualsevol extensió finita de* $\overline{\mathbb{Q}}(T)$ *es conserva per extensió d'escalars de* $\overline{\mathbb{Q}}$ *a* $\mathbb{C}$ *o, equivalentment,* $\overline{\mathbb{Q}(T)}$ *i* $\mathbb{C}(T)$ *són linealment disjunts sobre* $\overline{\mathbb{Q}}(T)$.

Demostració: Que les dues afirmacions són equivalents és clar, per exemple, notant que els coeficients del polinomi irreductible sobre $\mathbb{C}(T)$ d'un element de $\overline{\mathbb{Q}(T)}$ pertanyen a $\overline{\mathbb{Q}(T)} \cap \mathbb{C}(T)$.

Sigui $\alpha \in \overline{\mathbb{Q}(T)} \cap \mathbb{C}(T)$. Expressem $\alpha = P(T)/Q(T)$, on $P(T)$ i $Q(T)$ són polinomis coprimers de $\mathbb{C}[T]$. Multiplicant α, si cal, per un element convenient de $\overline{\mathbb{Q}}(T)$, podem suposar que tant $P(T)$ com $Q(T)$ no tenen cap arrel a $\overline{\mathbb{Q}}$. Així, si $f(X) \in \overline{\mathbb{Q}}(T)[X]$ és el polinomi irreductible de α sobre $\overline{\mathbb{Q}}(T)$, aleshores els coeficients de $f(X)$ no tenen cap zero ni cap pol en el conjunt d'arrels de $Q(T)$ i $P(T)$. Com que $(Q(T))^{deg(f)}\, f(\alpha) = 0$, ara és clar que les arrels de $P(T)$ també ho han de ser del terme independent de $f(X)$ i que les arrels de $Q(T)$ ho han de ser de $P(T)$. En les nostres hipòtesis, només pot ser $\alpha \in \mathbb{C}$. Especialitzant tots els coeficients de $f(X)$ en qualsevol $T = t \in \overline{\mathbb{Q}}$ (que no sigui pol de cap d'ells) obtenim un polinomi $f_t(X) \in \overline{\mathbb{Q}}[X]$ que s'anul.la en α. És a dir, $\alpha \in \mathbb{C} \cap \overline{\mathbb{Q}} = \overline{\mathbb{Q}}$. □

1.2.1 Demostració del Teorema 1.2.1

Assumim les hipòtesis del Teorema 1.2.1. Cal veure que l'extensió de cossos de funcions $L/\mathbb{C}(T)$, corresponent al recobriment f, es pot obtenir per extensió d'escalars d'una extensió de $\overline{\mathbb{Q}}(T)$ (per força del mateix grau, pel Lema 1.2.2). Denotarem per $S \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ el conjunt de ramificació de f (i de $L/\mathbb{C}(T)$).

REDUCCIÓ: És suficient veure que, si $L/\mathbb{C}(T)$ és de Galois, aleshores existeix una extensió de Galois de $\overline{\mathbb{Q}}(T)$ amb el 'mateix' grup de Galois G i no ramificada fora de S. Justifiquem-ho.

Per l'Observació 1.1.4, només hi ha un nombre finit d'extensions de Galois de $\mathbb{C}(T)$ amb grup (isomorf a) G i no ramificades fora de S (en una clausura algebraica de $\mathbb{C}(T)$ fixada). La composició de totes elles és una extensió de Galois *finita* $\widetilde{L}/\mathbb{C}(T)$ amb un cert grup de Galois $\widetilde{G}$, caracteritzada per ser l'*única* extensió de Galois de $\mathbb{C}(T)$ no ramificada fora de S amb grup $\widetilde{G}$. Que és única és clar; altrament, obtindríem "noves"extensions de Galois de $\mathbb{C}(T)$ amb grup G i no ramificades fora de S.

Suposem que ja hem provat que existeix alguna extensió de Galois $\widetilde{L_0}/\overline{\mathbb{Q}}(T)$ no ramificada fora de S amb grup $\widetilde{G}$. Aplicant-li extensió d'escalars obtenim, necessàriament, l'extensió $\widetilde{L}/\mathbb{C}(T)$ (pel Lema 1.2.2 i per la unicitat esmentada). De fet, l'extensió $\widetilde{L_0}/\overline{\mathbb{Q}}(T)$ també és única: si n'hi hagués una altra, el grau de la seva composició hauria de ser $[\widetilde{L} : \mathbb{C}(T)] = [\widetilde{L_0} : \overline{\mathbb{Q}}(T)]$, pel Lema 1.2.2. Finalment, el morfisme de restricció $\mathrm{Gal}(\widetilde{L}/\mathbb{C}(T)) \to \mathrm{Gal}(\widetilde{L_0}/\overline{\mathbb{Q}}(T))$ és un isomorfisme i, per la correspondència fonamental de la Teoria de Galois, tota subextensió (galoisiana o no) de $\widetilde{L}/\mathbb{C}(T)$ també s'obté per extensió d'escalars d'una única subextensió de $\widetilde{L_0}/\overline{\mathbb{Q}}(T)$.

A partir d'ara suposarem, doncs, que $L/\mathbb{C}(T)$ és una extensió de Galois finita ramificada exactament en $S \subset \mathbb{P}^1(\overline{\mathbb{Q}})$. Per comoditat, suposarem també que $\infty \in S$ (si cal, fem canvi de variable).

ESPECIALITZACIÓ: Considerem un element primitiu α per a $L/\mathbb{C}(T)$, que podem suposar enter sobre $\mathbb{C}[T]$. Sigui $f(T, X) \in \mathbb{C}[T, X]$ el polinomi mínim de α sobre $\mathbb{C}(T)$. Òbviament, existeix una $\overline{\mathbb{Q}}$-àlgebra *finitament generada* $B \subset \mathbb{C}$ tal que $f(T, X) \in B[T, X]$. L'extensió de $\overline{\mathbb{Q}}(T)$ que volem trobar s'obtindrà com a cos de descomposició del polinomi $f^\omega(T, X)$ deduït de $f(T, X)$ per un morfisme (d'especialització) convenient $\omega : B \to \overline{\mathbb{Q}}$ (amb B convenient, també).

Convenim que ω sempre denotarà un (epi)morfisme de $\overline{\mathbb{Q}}$-àlgebres $\omega : B \to \overline{\mathbb{Q}}$ (variable), amb B una $\overline{\mathbb{Q}}$-àlgebra finitament generada continguda en $\mathbb{C}$ (que ampliarem successivament). Denotarem per K_B el cos de fraccions de B.

Per comoditat, direm que una propietat $*$ (que depèn de ω) és *genèricament* certa si existeix algun $b \in B\backslash\{0\}$ de manera que $*$ és certa per a tot ω tal que $\omega(b) \neq 0$. En aquest cas, podem redefinir B com $B[b^{-1}]$ i suposar que la propietat $*$ és certa per a tot ω.

El punt clau per a concloure la demostració és el següent cas particular del Teorema de Bertini-Noether (cf. [30, Lemma 7.6]): genèricament, $f^\omega(T,X)$ és un polinomi irreductible en $\overline{\mathbb{Q}}[T,X]$. A partir d'ara, només considerarem els morfismes ω amb aquesta propietat.

Definim $L^\omega := \overline{\mathbb{Q}}(T)[\alpha^\omega]$, amb $\alpha^\omega \in \overline{\mathbb{Q}(T)}$ una arrel de $f^\omega(T,X)$ (com a polinomi en X).

Per a qualsevol $\beta \in L = \mathbb{C}(T)[\alpha]$, podem (ampliar B i) suposar que $\beta \in K_B(T)[\alpha]$ i, genèricament, podem donar sentit a l'expressió $\beta^\omega \in L^\omega$; de fet, si considerem $a(T) \in B[T]$ tal que $a(T)\beta \in B[T,\alpha]$, aleshores és suficient demanar $a^\omega(T) \neq 0$. A més, si $\beta_1, \beta_2 \in K_B(T)[\alpha]$ són diferents, aleshores, genèricament, $\beta_1^\omega \neq \beta_2^\omega$.

En particular, podem suposar que, genèricament, L^ω conté totes les arrels de $f^\omega(T,X)$. En aquest cas, l'extensió $L^\omega/\overline{\mathbb{Q}}(T)$ és de Galois i es comprova que la bijecció natural entre les arrels de f i de f^ω defineix un isomorfisme entre els grups de Galois de $L/\mathbb{C}(T)$ i de $L^\omega/\overline{\mathbb{Q}}(T)$ (com a grups de permutacions).

Només falta justificar que també podem suposar que, genèricament, l'extensió $L^\omega/\overline{\mathbb{Q}}(T)$ és no ramificada fora de S.

Recordem que, per hipòtesi, $\infty \in S$. D'altra banda, tot primer finit $(T-t)$ de $\overline{\mathbb{Q}}[T]$ que ramifica en $L^\omega/\overline{\mathbb{Q}}(T)$ correspon a una arrel $t \in \overline{\mathbb{Q}}$ del discriminant (en X) de $f^\omega(T,X)$, $D_X(f^\omega(T,X)) = D_X^\omega(f(T,X))$. Així, podem suposar que, genèricament, $t = t_0^\omega$ per alguna arrel $t_0 \in B$ de $D_X(f(T,X))$.

Suposem $(T - t_0^\omega) \notin S$. Com que $S \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ i la restricció de ω sobre $\overline{\mathbb{Q}}$ és la identitat, el primer $(T-t_0)$ no pot pertànyer a S i, per tant, no ramifica en $L/\mathbb{C}(T)$. Així, $(T-t_0)$ descompon completament en la clausura entera $\mathcal{O}_L$ de $\mathbb{C}[T]$ en L i, per tant, es té un isomorfisme $\mathcal{O}_L/(T-t_0)\mathcal{O}_L \cong \mathbb{C}^n$. Si $\gamma \in \mathcal{O}_L$ és una antimatge d'un element qualsevol $(x_i)_i \in \mathbb{C}^n$ tal que $x_i \neq x_j$ si $i \neq j$, aleshores γ és un element primitiu per a $L/\mathbb{C}(T)$ i el seu polinomi mínim $g(T,X) \in$

$\mathbb{C}[T,X]$ satisfà $g(t_0,X)=\prod_i(X-x_i)$ (donat que $(g(t_0,x_i))_i=0\in\mathbb{C}^n$). És clar que podem suposar que, genèricament, $L^\omega=\overline{\mathbb{Q}}(T)[\gamma^\omega]$. Com que $D_X(g(t_0,X))\neq 0$, també podem suposar que, genèricament, $D_X(g^\omega(t_0^\omega,X))\neq 0$ (com abans) i, per tant, que $(T-t_0^\omega)$ no ramifica en $L^\omega/\overline{\mathbb{Q}}(T)$.

1.3 El Teorema de Belyi i conseqüències

En aquesta secció provem el Teorema de Belyi (dels tres punts) pròpiament dit, és a dir, la implicació $(i)\Rightarrow(ii)$ del Teorema 1.0.1. Tot i que podríem anomenar-la la "part no òbvia"del Teorema de Belyi, es tracta d'un resultat de caràcter molt més elemental que la "part òbvia"$(i)\Rightarrow(ii)$, provada a la Secció 1.2. En la literatura es troben diverses adaptacions de la demostració original de Belyi [3]. Nosaltres seguim [22].

1.3.1 Demostració del Teorema de Belyi

Suposem donada una corba projectiva i llisa X sobre $\overline{\mathbb{Q}}$. Volem provar l'existència d'algun morfisme no constant $f:X\longrightarrow\mathbb{P}^1_{\mathbb{C}}$ ramificat en, com a màxim, tres punts. Donarem, de fet, un "algorisme"per a obtenir (un possible) f amb ramificació només en $\{0,1,\infty\}$. El procés parteix d'una funció racional no constant qualsevol $f_0\in\overline{\mathbb{Q}}(X)$, és a dir, d'un morfisme no constant $f_0:X\longrightarrow\mathbb{P}^1_{\overline{\mathbb{Q}}}$ definit sobre $\overline{\mathbb{Q}}$. Evidentment, f_0 ramifica en un conjunt finit de punts $ram(f_0)$, tots ells $\overline{\mathbb{Q}}$-racionals. El recobriment desitjat s'obtindrà com una composició $P\circ f_0:X\longrightarrow\mathbb{P}^1_{\mathbb{C}}$, amb $P(T)\in\mathbb{Q}(T)$ convenient.

PRIMER: $f_1:X\longrightarrow\mathbb{P}^1_{\mathbb{C}}$ amb $ram(f_1)\subset\mathbb{P}^1(\mathbb{Q})$.

Definim $irram(f_0):=\{t\in ram(f_0)\text{ tal que }t\notin\mathbb{P}^1(\mathbb{Q})\}$. Afegint tots els $G_{\mathbb{Q}}$-conjugats d'elements de $irram(f_0)$, obtenim un conjunt finit $S\subset\mathbb{P}^1(\overline{\mathbb{Q}})\backslash\{\infty\}$ que conté $irram(f_0)$ i que és invariant per l'acció de $G_{\mathbb{Q}}$.

Considerem el polinomi $P_1(T):=\prod_{t\in S}(T-t)\in\mathbb{Q}[T]$ i el conjunt $S_1:=\{P_1(\alpha)\text{ amb }\alpha\text{ arrel del polinomi derivat }P_1'(T)\}\subset\mathbb{P}^1(\overline{\mathbb{Q}})\backslash\{\infty\}$. El morfisme $P_1:\mathbb{P}^1_{\mathbb{C}}\longrightarrow\mathbb{P}^1_{\mathbb{C}}$, definit per $P_1(T)$, envia tots els punts de

S a 0. Així, el recobriment $P_1 \circ f_0 : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ satisfà $ram(P_1 \circ f_0) \subset \mathbb{P}^1(\overline{\mathbb{Q}})$, $irram(P_1 \circ f_0) \subseteq S_1$ i, clarament, S_1 és un conjunt $G_{\mathbb{Q}}$-invariant de cardinal estrictament més petit que S.

Repetint aquest procés tants cops com calgui, "al final" obtindrem un recobriment $f_1 : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ amb $irram(f_1) = \emptyset$.

SEGON: $f_2 : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ amb $ram(f_2) \subseteq \{0, 1, \infty\}$.

Composant f_1 amb una transformació lineal fraccionària convenient (definida sobre $\mathbb{Q}$), podem suposar que $ram(f_1) \subseteq \{0, 1, \infty\}$ (i hem acabat) o bé que $\{0, 1, \infty, a\} \subseteq ram(f_1)$, amb $0 < a < 1$.

En el segon cas, expressem $a = \frac{m}{m+n}$, amb m, n naturals, i definim $P_2(T) := \left(\frac{T}{a}\right)^m \left(\frac{1-T}{1-a}\right)^n$. Òbviament, $P_2(a) = 1$ i $P_2(0) = P_2(1) = 0$. A més, el polinomi derivat $P_2'(T)$ només s'anul.la en $0, a, 1$ i, per tant, es té $ram(P_2) = \{0, 1, \infty\}$. D'aquesta manera, el recobriment $P_2 \circ f_1 : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ satisfà $ram(P_2 \circ f_1) \subset \mathbb{P}^1(\mathbb{Q})$ i el conjunt $ram(P_2 \circ f_1)$ té cardinal estrictament més petit que $ram(f_1)$.

Repetint aquest procés successivament, obtenim un recobriment $f_2 : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ amb $ram(f_2) \subseteq \{0, 1, \infty\}$.

1.3.1 Observació. De la demostració donada es dedueix, també, que si la corba X està definida sobre un cos de nombres K, aleshores podem suposar que el morfisme f està definit sobre K; només cal partir de $f_0 \in K(X)$.

1.3.2 Conseqüències del Teorema de Belyi

Com a conseqüència del Teorema 1.2.1, s'obté el següent cas particular (gènere 0) de [14, XIII, Cor. 2.12]:

1.3.2 Teorema. *Si $S \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ és un conjunt finit de cardinal $s+1$, aleshores*

$$\pi_1^{alg}\left(\mathbb{P}^1_{\overline{\mathbb{Q}}} \backslash S\right) \cong \widehat{F_s}.$$

DEMOSTRACIÓ: En la demostració del Teorema 1.2.1 hem vist, de fet, que es té una bijecció entre les subextensions de Galois finites de $\mathbb{C}(T)^S/\mathbb{C}(T)$ i de $\overline{\mathbb{Q}}(T)^S/\overline{\mathbb{Q}}(T)$, i que els morfismes naturals (de

restricció) entre els corresponents grups de Galois són isomorfismes (compatibles amb subextensions). Per tant, el morfisme natural entre els límits projectius $\pi_1^{alg}\left(\mathbb{P}^1_{\mathbb{C}}\backslash S\right) \longrightarrow \pi_1^{alg}\left(\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash S\right)$ és un isomorfisme. □

En la resta d'aquesta secció, convenim

$$S := \{0, 1, \infty\}.$$

Com que $S \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ és invariant per $G_{\mathbb{Q}}$ (és a dir, $\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash S$ està definit sobre $\mathbb{Q}$), l'extensió $\overline{\mathbb{Q}}(T)^S/\mathbb{Q}(T)$ és de Galois i es té una successió exacta

$$1 \to \pi_1^{alg}\left(\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash S\right) \to \pi_1^{alg}\left(\mathbb{P}^1_{\mathbb{Q}}\backslash S\right) \to G_{\mathbb{Q}} \to 1,$$

que dóna lloc a un morfisme canònic

$$\pi : \ G_{\mathbb{Q}} \longrightarrow \mathrm{Out}\left(\pi_1^{alg}\left(\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash S\right)\right) \cong \mathrm{Out}\left(\widehat{F_2}\right),$$

on $\mathrm{Out}(*) := \mathrm{Aut}(*)/\mathrm{Inn}(*)$ denota el grup d'automorfismes externs.

1.3.3 Teorema. (Belyi [3]) *π és un monomorfisme.*

Demostració: $G_{\mathbb{Q}}$ actua fidelment en el conjunt de classes d'isomorfisme de corbes el.líptiques sobre $\overline{\mathbb{Q}}$, donat que ho fa sobre els seus invariants j. En particular, pel Teorema de Belyi, $G_{\mathbb{Q}}$ actua fidelment sobre les classes d'isomorfisme de recobriments finits de $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ no ramificats fora de $S = \{0, 1, \infty\}$. Equivalentment, per a qualsevol $id \neq \sigma \in G_{\mathbb{Q}}$, existeix algun subgrup $\Gamma \subset \widehat{F_2}$ d'índex finit tal que Γ i Γ^σ no són conjugats. □

1.3.4 Observació. Si $t_0 \in \mathbb{P}^1(\mathbb{Q})\backslash S$, aleshores $(T - t_0)$ és inert en l'extensió $\overline{\mathbb{Q}}(T)/\mathbb{Q}(T)$ i descompon completament en $\overline{\mathbb{Q}}(T)^S/\overline{\mathbb{Q}}(T)$. Per tant, tot subgrup de descomposició de $\mathrm{Gal}(\overline{\mathbb{Q}}(T)^S/\mathbb{Q}(T))$ en t_0 és un complement de $\mathrm{Gal}(\overline{\mathbb{Q}}(T)^S/\overline{\mathbb{Q}}(T))$, isomorf al grup de Galois de l'extensió residual corresponent, és a dir, a $G_{\mathbb{Q}}$. Així, l'epimorfisme $\pi_1^{alg}\left(\mathbb{P}^1_{\mathbb{Q}}\backslash S\right) \to G_{\mathbb{Q}}$ admet una (infinites) secció i es té:

$\pi_1^{alg}\left(\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash S\right) \cong \widehat{F_2} \rtimes G_{\mathbb{Q}}$. A més, cadascuna d'aquestes seccions defineix un aixecament (no canònic) de π, $\widetilde{\pi} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}\left(\widehat{F_2}\right)$, que és un monomorfisme pel Teorema 1.3.3. Treballs de Drinfeld, Ihara i altres conclouen que $G_{\mathbb{Q}}$ està contingut, via un aixecament "natural"de π, en un subgrup explícit de $\mathrm{Aut}\left(\widehat{F_2}\right)$, conegut com el grup de Grothendieck-Teichmüller. Es conjectura, a més, que aquesta inclusió és una igualtat, fet que donaria una presentació de $G_{\mathbb{Q}}$. Veure [17] per a més detalls i referències.

Un **parell de Belyi** (X, β) consisteix en una corba projectiva i llisa X sobre $\overline{\mathbb{Q}}$ i un recobriment $\beta : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ tal que $ram(\beta) \subseteq \{0, 1, \infty\}$. Un **dibuix** serà (veure capítol següent) una classe d'isomorfisme de parells de Belyi. Pel Teorema 1.3.3, $G_{\mathbb{Q}}$ actua fidelment en el conjunt de dibuixos i, per la demostració donada, també ho fa sobre els dibuixos en gènere 1. De fet, es pot veure (cf. [22]) que $G_{\mathbb{Q}}$ també actua fidelment sobre els dibuixos en gènere 0 i, encara més, sobre els **arbres** (classes de recobriments de gènere 0 totalment ramificats en ∞).

1.3.5 Observació. En el capítol següent parlarem de **dibuixos nets**. Per definició, correspondran a parells de Belyi (X, β) tals que l'índex de ramificació en qualsevol punt de $\beta^{-1}(1)$ és exactament 2. Per a qualsevol corba X projectiva i llisa sobre $\overline{\mathbb{Q}}$ existeix algun parell de Belyi net (X, β). De fet, si (X, f) és un parell de Belyi (existeix pel Teorema de Belyi) i considerem el polinomi $P(T) := 4T(1-T)$, aleshores el parell de Belyi $(X, P \circ f)$ és net. Només cal notar que el morfisme $P : \mathbb{P}^1_{\mathbb{C}} \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ ramifica exactament en $\{1, \infty\}$ (amb índexs de ramificació 2) i satisfà $P(0) = P(1) = 0$, $P(\infty) = \infty$ i $P(1/2) = 1$.

1.4 ABC implica Mordell

L'objectiu d'aquesta secció és veure un resultat d'Elkies [11] que permet deduir la validesa de la conjectura de Mordell (Teorema de Faltings) de la conjectura ABC. A més de la seva simplicitat, l'interès principal de la demostració és la seva "efectivitat". Concretament, donada una corba X de gènere $g \geq 2$ sobre un cos de nombres L, una versió efectiva de ABC (sobre L) proporciona una fita per a l'alçada

dels punts L-racionals de X. És a dir, "ABC efectiva" implica el que es coneix com "Mordell efectiu"(no provat). Elkies obté aquest resultat aplicant el Teorema de Belyi i, naturalment, la seva efectivitat. Per simplicitat, nosaltres només considerarem el cas $L = \mathbb{Q}$. A més de [11], la referència bàsica en aquesta secció és [28].

1.4.1 La conjectura ABC

Comencem recordant l'enunciat de la conjectura ABC de Masser i Oesterlé (1983).

1.4.1 Conjectura ABC (sobre $\mathbb{Q}$) *Per a cada $\varepsilon > 0$, existeix una constant $K > 0$ amb la propietat següent: si A, B, C són enters no nuls coprimers entre ells tals que $A + B + C = 0$, aleshores:*

$$\prod_{p|ABC} p \geq K \left(max\{|A|, |B|, |C|\}\right)^{1-\varepsilon}.$$

La motivació original d'aquesta conjectura va ser que implicava "Fermat assimptòtic". De fet, si x, y, z són enters no nuls coprimers entre ells i considerem $(A, B, C) = (x^n, y^n, z^n)$, aleshores el *radical* (o conductor) $\prod_{p|ABC} p = |xyz|$ està afitat superiorment per $(max\{|A|, |B|, |C|\})^{3/n}$. Així, si $x^n + y^n + z^n = 0$ i fixem $0 < \varepsilon < 1$, aleshores la desigualtat en la conjectura ABC dóna lloc a una fita superior per a $max\{|x^n|, |y^n|, |z^n|\}$, vàlida per a tot $n > \frac{3}{1-\varepsilon}$. Per a n prou gran, haurà de ser $max\{|x|, |y|, |z|\} = 1$, contradient les hipòtesis fetes.

A continuació reformularem la Conjectura 1.4.1. Recordem primer que en $\mathbb{P}^n(\mathbb{Q})$ es pot definir una funció **alçada**:

$$H(x_0 : \cdots : x_n) := \prod_{v \in \Sigma} max\{|x_0|_v, \cdots, |x_n|_v\},$$

on Σ denota el conjunt de totes les places de $\mathbb{Q}$. Aquesta funció està ben definida gràcies a la fórmula del producte. De fet, treballarem amb l'**alçada logarítmica**

$$h(x_0 : \cdots : x_n) := \log H(x_0 : \cdots : x_n).$$

A part de la pròpia definició, l'única propietat que usarem d'aquesta funció és la següent conseqüència d'un resultat de Néron (cf. [28, 6.1], [11, p. 104-105], [24, p. 26]):

1.4.2 Lema. *Sigui X una corba projectiva i llisa sobre $\mathbb{Q}$. Donades dues funcions racionals $f, g \in \mathbb{Q}(X)$, existeix una constant C (que només depèn de X, f i g) tal que:*

$$h(g(R)) \leq \frac{deg(g)}{deg(f)} h(f(R)) + C\sqrt{h(f(R))},$$

per a tot $R \in X(\overline{\mathbb{Q}})$.

També serà convenient introduir la següent funció en $\mathbb{P}^1(\mathbb{Q})\backslash\{0, 1, \infty\}$:

$$N(x : 1) := \prod_{p \in I} p\,,$$

on I denota el conjunt de nombres primers p tals que $v_p(x(1-x)) \neq 0$.

Si A, B, C són enters coprimers no nuls tals que $A + B + C = 0$, aleshores $(-A/B : 1) \in \mathbb{P}^1(\mathbb{Q})\backslash\{0, 1, \infty\}$ i es satisfà:

- $max\{|A|, |B|, |C|\} = H(A : B : C) = H(-A/B : -1 : 1+A/B)$, d'on es dedueix que, per a $\lambda_\infty \in [1, 2]$ convenient, es té
$$max\{|A|, |B|, |C|\} = H(-A/B : 1).\lambda_\infty.$$
- $\prod_{p|ABC} p = N(-A/B : 1)$.

Així, es comprova que la Conjectura 1.4.1 equival a:

1.4.3 Conjectura ABC (sobre $\mathbb{Q}$) *Per a cada $\varepsilon > 0$, existeix una constant K tal que, si $Q \in \mathbb{P}^1(\mathbb{Q})\backslash\{0, 1, \infty\}$, aleshores:*

$$\log N(Q) \geq (1 - \varepsilon)h(Q) + K.$$

1.4.4 Observació. Aquesta formulació de la conjectura admet una generalització natural per a cossos de nombres qualsevols enlloc de $\mathbb{Q}$ (prenent normes d'ideals primers en la definició de $N(x : 1)$). En el cas general, la constant K depèn (de ε i) del cos de nombres considerat.

1.4.2 Demostració del resultat d'Elkies

Es tracta de provar (sobre $\mathbb{Q}$) el resultat d'Elkies "ABC efectiva $\Rightarrow$ Mordell efectiu", que generalitza la implicació "ABC efectiva $\Rightarrow$ Fermat assimptòtic efectiu"esmentada anteriorment.

Volem veure com, assumint la Conjectura 1.4.3, es poden calcular tots els punts $\mathbb{Q}$-racionals d'una corba de gènere $g \geq 2$ (en un temps afitable a priori).

Dades: Suposem donada una corba projectiva i llisa X sobre $\mathbb{Q}$ de gènere $g \geq 2$. Fixem una funció de Belyi $f : X_{\mathbb{Q}} \longrightarrow \mathbb{P}^1_{\mathbb{Q}}$ definida sobre $\mathbb{Q}$ (existeix, per l'Observació 1.3.1).

Objectiu: Demostrarem que existeix una constant N, que depèn només del parell (X, f), amb la següent propietat: si $R \in X(\mathbb{Q})$ i $f(R) \notin \{0, 1, \infty\}$, aleshores $h(f(R)) \leq N$. Així, tot punt $\mathbb{Q}$-racional de X pertany al conjunt (finit efectivament calculable)

$$f^{-1}\left(\{0, 1, \infty\} \cup \{Q \in \mathbb{P}^1(\mathbb{Q}) \text{ tal que } h(Q) \leq N\}\right).$$

Per a qualsevol punt $\mathbb{Q}$-racional $a \in \mathbb{P}^1(\mathbb{Q})$, els punts de la fibra $f^{-1}(a)$, comptats amb multiplicitats (índexs de ramificació), defineixen un divisor $f^*(a)$ de X efectiu, de grau $deg(f)$ i definit sobre $\mathbb{Q}$.

Considerem la descomposició en divisors irreductibles (sobre $\mathbb{Q}$):

$$f^*(0) + f^*(1) + f^*(\infty) = \sum_{1 \leq i \leq s} e_i D_i \qquad (e_i \in \mathbb{Z}_{>0}).$$

Per a $M \in \mathbb{Z}_{>0}$ prou gran, cadascun dels divisors MD_i és el divisor de pols d'una funció racional $f_i \in \mathbb{Q}(X)$ (per Riemann-Roch és suficient $M = 2g$, cf. [28, Lemma 6.3]). És a dir, $MD_i = f_i^*(\infty)$.

Denotem per S_{bad} el conjunt (finit) de primers de mala reducció per a $X_{\mathbb{Q}}$, f, $\{D_i\}_i$ o $\{f_i\}_i$.

Sigui $R \in X(\mathbb{Q})$ tal que $f(R) \notin \{0, 1, \infty\}$. En particular, $f_i(R) \neq \infty$, per a tot $1 \leq i \leq s$.

Recordem que un nombre primer p contribueix a $N(f(R))$ exactament quan $v_p(f(R)) > 0$, $v_p(f(R)) < 0$ o bé $v_p(1 - f(R)) > 0$. Per a $p \notin S_{bad}$, això equival a $\overline{f}(\overline{R}) \in \{\overline{0}, \overline{1}, \overline{\infty}\}$; és a dir, $\overline{R}$ pertany

al suport d'algun $\overline{f_i^*(\infty)}$, per força amb multiplicitat $\geq M$. Així, si $p \notin S_{bad}$ divideix $N(f(R))$, aleshores existeix $i \in \{1, \cdots, s\}$ tal que $-v_p(f_i(R)) \geq M$ i, per tant,

$$p \leq \prod_{1\leq i\leq s} max\left\{1, p^{-v_p(f_i(R))/M}\right\} = \left(\prod_{1\leq i\leq s} max\left\{1, |f_i(R)|_p\right\}\right)^{1/M}.$$

D'aquesta manera, s'obté

$$\begin{aligned} N(f(R)) &\leq \prod_{p\in S_{bad}} p \cdot \prod_{v\in\Sigma}\left(\prod_{1\leq i\leq s} max\left\{1, |f_i(R)|_v\right\}\right)^{1/M} \\ &= \prod_{p\in S_{bad}} p \cdot \prod_{1\leq i\leq s}\left(\prod_{v\in\Sigma} max\left\{1, |f_i(R)|_v\right\}\right)^{1/M} \\ &= \prod_{p\in S_{bad}} p \cdot \prod_{1\leq i\leq s} H(f_i(R))^{1/M}. \end{aligned}$$

És a dir, hem vist que:

$$\log N(f(R)) \leq \frac{1}{M}\sum_{1\leq i\leq s} h(f_i(R)) + \sum_{p\in S_{bad}} \log p.$$

Aplicant el Lema 1.4.2 amb $g = f_i$ i tenint en compte que $deg(f_i) = M deg(D_i)$, concloem que existeixen constants K_1, K_2 tals que:

$$\log N(f(R)) \leq \frac{\sum_{1\leq i\leq s} deg(D_i)}{deg(f)} h(f(R)) + K_2\sqrt{h(f(R))} + K_1.$$

Així, si definim $d := \frac{\sum_{1\leq i\leq s} deg(D_i)}{deg(f)}$ i apliquem la Conjectura 1.4.3 obtenim (per a certa constant K que només depèn d'un $\varepsilon > 0$ fixat):

$$(*) \qquad (1-\varepsilon)h(f(R)) + K \leq d\, h(f(R)) + K_2\sqrt{h(f(R))} + K_1.$$

D'altra banda, les hipòtesis "$g \geq 2$" i "f de Belyi"(no usades encara) ens permeten concloure que $d < 1$. De fet, $\sum_{1\leq i\leq s} deg(D_i) = \sharp f^{-1}(\{0, 1, \infty\})$ i la fórmula de Riemann-Hurwitz aplicada al parell de Belyi (X, f) garanteix que $\sharp f^{-1}(\{0, 1, \infty\}) = deg(f) - 2g + 2$.

En conclusió, podem prendre $\varepsilon > 0$ tal que $1 - \varepsilon > d$ i, en aquest cas, la desigualtat $(*)$ dóna lloc a una fita superior per a $h(f(R))$.

1.4.5 Observació. En [29] es demostra que la Conjectura ABC implica la validesa, per a corbes, d'una conjectura de Vojta, usant també el Teorema de Belyi. D'aquesta implicació se'n dedueix, d'una banda, el resultat d'Elkies i, de l'altra, un resultat "anàleg"de Bombieri de 1994 que estableix "ABC $\Rightarrow$ Teorema de Roth"(corresponent al cas $X = \mathbb{P}^1$). Veure també [28].

També com a conseqüència del Teorema de Belyi, i en la línia del resultat d'Elkies, es pot obtenir la implicació "ABC efectiva $\Rightarrow$ Teorema de Siegel efectiu", cf. [27].

Bernat Plans
Departament de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Av. Diagonal, 647, 08028 Barcelona
bernat.plans@upc.es

Capítol 2

Introducció als Dibuixos d'Infants

Xavier Xarles

Introducció

Com ja sabeu tots molt bé, l'any 1970 Alexander Grothendieck es va retirar de la vida matemàtica quan estava en un moment especialment àlgid. A partir d'aleshores era un misteri per a la comunitat matemàtica si seguia fent recerca (el que era d'esperar) i, si era així, quin tipus de problemes estava estudiant i quins nous mètodes estava investigant.

L'objectiu d'aquestes xerrades es intentar fer una introducció modesta a un dels temes que, després del seu *Esquisse d'un Programme* [15], sabem que va estar treballant. Segons explica ell mateix, les exigencies de l'ensenyament universitari que s'adreça a estudiants amb un bagatge matemàtic modest (i sovint menys que modest) van fer que comences a reflexionar sobre temes que creia podien ser compresos de manera intuïtiva, independentment del llenguatge tècnic i fins hi tot anterior a tal llenguatge. Essencialment estava pensant en la intuïció geomètrica, la topologia de les formes, essencialment de dimensió dos. Va ser aleshores quan es va adonar que podia determinar una estructura de superfície de Riemann (i per tant de corba

algebraica sobre $\mathbb{C}$) només dibuixant un "graf"sobre la superfície topològica associada; però el més sorprenent és que les corbes així obtingudes estaven de fet automàticament definides sobre un cos de nombres! Grothendieck ens explica a [15] que va arribar a preguntar a Deligne si podria ser que es poguessin obtenir així totes les corbes (llises, projectives, geomètricament connexes), però ho varen desestimar per massa "agosarat". Però al cap de poc G. V. Belyĭ [3] va demostrar en el seu famós teorema "dels tres punts"que la resposta a aquesta pregunta era efectivament que sí.

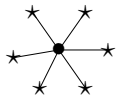
La denominació de dibuix d'infants està extreta d'aquestes notes, on menciona, després de comentar aquestes idees, que: *Cette découverte, qui techniquement se réduit à si peu de choses, a fait sur moi une impression très forte, et elle représente un tournant décisif dans le cours de mes réflexions, qui soudain s'est trouvé fortement localisé. Je ne crois pas qu'un fait mathématique m'ait jamais autant frappé que celui-là, et ait eu un impact psychologique comparable. Cela tient sûrement à la nature tellement familière, non technique, des objets considérés, dont tout dessin d'enfant griffonné sur un bout de papier (pour peu que le graphisme soit d'un seul tenant) donne un exemple parfaitement explicite. A un tel dessin se trouvent associés des invariants arithmétiques subtils, qui seron chamboulés completement dès qu'on y rajoute un trait de plus.*

2.1 Què és un Dibuix d'Infants?

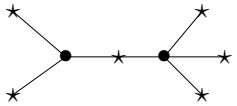
Un dibuix d'infants és un graf connex dibuixat sobre una superfície orientable, compacte i connexa, de manera que les cares del graf són cel·les (o sigui, homeomorfes al disc), i amb dos tipus de vèrtexs, $\bullet$ i $\star$, de manera que tota aresta té un vertex de cada tipus, o sigui és de la forma

Anem a veure uns quants exemples.

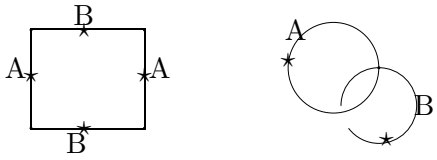
2.1.1 Exemples. 1. A l'esfera (o sigui, al pla):



2.



3. Al tor:



Anem a fer aquesta definició una mica més rigorosa, a més d'introduir els dibuixos nets i pre-nets.

2.1.2 Definició Un dibuix d'infants és una tripleta $X_0 \subset X_1 \subset X_2$ on

- X_2 és una superfície compacte i orientable.
- X_0 és un conjunt finit de punts de dos tipus (els vèrtexs).
- X_1 és un tancat connex de manera que $X_1 \setminus X_0$ es una unió finita de segments oberts (les arestes).
- $X_2 \setminus X_1$ és una unió finita de cel·les obertes (les cares).

i tal que dos punts de X_0 units per un segment de $X_1 \setminus X_0$ tenen tipus diferents (i.e. el graf té una estructura bipartita).

Un dibuix d'infants net és com abans un tripleta $X_0 \subset X_1 \subset X_2$ verificant totes les condicions però amb vèrtexs només d'un tipus.

Un dibuix d'infants pre-net és com un dibuix net, o sigui una tripleta $X_0 \subset X_1 \subset X_2$ verificant totes les condicions, amb vèrtexs només d'un tipus, però on les arestes de X_1 poden acabar obertes.

Denotem com és usual la valència d'un vertex com el nombre d'arestes que el contenen; i la valència d'una cara com el nombre de arestes que l'envolten. Podem pensar aleshores (i així ho farem tota l'estona) que un dibuix net és un dibuix on tots els vèrtexs $\star$ tenen valència 2; al esborrar-los obtenim un dibuix net (per exemple, el tercer dibuix és net). Igualment, un dibuix pre-net és un dibuix on tots els vèrtexs $\star$ tenen valència ≤ 1 (per exemple, el dos primers dibuixos anteriors són pre-nets).

Diem que dos dibuixos d'infants (X_0, X_1, X_2) i (X_0', X_1', X_2') són equivalents si existeix un homeomorfisme de X_2 a X_2' *preservant l'orientació* tal que ens dóna un homeomorfisme de X_i a X_i' per a $i = 0$ i a 1. Per exemple, el dos dibuixos de la Figura 2.1 no són equivalents, ja que tot homeomorfisme de l'esfera que passa d'un a l'altre canvia l'orientació.

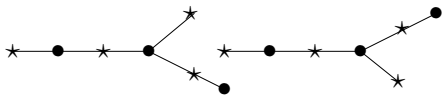


Figura 2.1: Dos dibuixos homeomorfs però no equivalents

Donat un dibuix $D = (X_0, X_1, X_2)$, tenim un primer invariant que ens serà de molta utilitat: la seva llista de valències $\tau(D)$. Consisteix en tres llistes corresponents a les valències dels vèrtexs $\bullet$, dels vèrtexs $\star$ i de les cares, on la valència d'una cara és per definició el nombre d'arestes que l'acoten *dividit per 2* (és un nombre enter, ja que els nostres grafs són bipartits!). Ho denotarem de la següent manera: $\tau(D) = (V_0, V_1, V_\infty)$, amb $V_0 = (u1, u2, \cdots, u_r)$, on u_i és el nombre de vèrtexs $\bullet$ amb valència u_i, i anàlogament per V_1 i per V_∞. Observem que

$$\sum_{i=1}^{s} u_i i = n$$

on n és el nombre de arestes de D, i igualment per a V_1 i per V_∞.

Així també podem pensar (per exemple Birch ho fa així al seu article [4]) que donar les llistes de valències és el mateix que donar tres particions de n. Una altre notació molt utilitzada (i molt útil quan tenim vèrtexs o cares amb valència alta) és: $V_0 = [i_1]^{u_{i_1}} \cdots [i_t]^{u_{i_t}}$ amb el significat que tenim u_j vèrtexs de valència j.

Anem a veure maneres diferents de donar un dibuix d'infants.

2.2 Interpretacions algebraiques, topològiques i modulars

Una de les principals riqueses de la teoria dels dibuixos d'infants són les interpretacions molt variades que tenen, algunes en camps aparentment allunyats. Aquest fet, com és habitual en matemàtiques, fa que es puguin resoldre problemes en un camp interpretant-los en un dels altres camps. Anem a veure només algunes de les més interessants.

2.2.1 Dibuixos via permutacions

Donat un dibuix d'infants, numerem arbitràriament les arestes de 1 a n (=el nombre d'arestes). Aleshores podem assignar a cada vertex la permutació de $\{1, \ldots, n\}$ obtinguda al girar al voltant del vertex en sentit "anti-horari"(recordem que X_2 és orientable, i podem fixar una orientació). Observem que les permutacions que obtenim dels vèrtexs $\bullet$ són totes disjuntes entre si; denotem per σ_0 el seu producte l'ordre no importa!). Igualment, les que obtenim dels vèrtexs $\star$ també són disjuntes entre si; denotem per σ_1 el seu producte.

2.2.1 Exemples. Anem a buscar les permutacions σ_0 i σ_1 dels dibuixos anteriors.

1. Numerem les arestes de la manera "natural". Obtenim que $\sigma_0 = (1, 2, 3, 4, 5, 6)$ i que $\sigma_1 := id$.

2. Numerem les arestes tal com mostra el dibuix 2.3. Aleshores obtenim que $\sigma_0 = (1, 2, 3)(4, 5, 6, 7)$ i que $\sigma_1 = (3, 4)$.

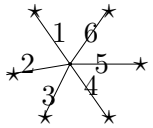


Figura 2.2: Estrella de 6 puntes

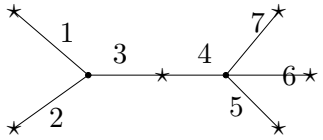


Figura 2.3: Doble estrella

3. Numerem les arestes tal com mostra el dibuix 2.4. Aleshores obtenim que $\sigma_0 = (1, 3, 2, 4)$ i que $\sigma_1 = (1, 2)(3, 4)$.

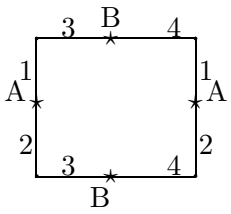


Figura 2.4: Dibuix en el tor

Definim a més σ_∞ com la permutació $(\sigma_0\sigma_1)^{-1}$; també es pot calcular com la permutació obtinguda al *girar dins de les cares, prenen una de cada dos arestes.*

Tenim aleshores una equivalència entre Dibuixos d'Infants (mòdul equivalència) amb n arestes i tripletes de permutacions $(\sigma_0, \sigma_1, \sigma_\infty)$ de S_n, tals que el subgrup que generen és transitiu en els símbols permutats per S_n, mòdul conjugació simultània per un element de S_n.

Per exemple, si denotem per n_i el nombre de cicles disjunts en que descompon cada σ_i, $i = 0, 1, \infty$, podem recuperar el gènere g de X_2 amb la "fórmula de Hurwitz":

$$2g - 2 = n - n_0 - n_1 - n_\infty,$$

altrament dita fórmula d'Euler:

$$2(1 - g) = n_0 + n_1 - n + n_\infty,$$

(Vèrtexs=$n_0 + n_1$, arestes=n, cares=n_∞).

Donat un dibuix D, podem així associar un altre invariant, el *grup de monodromia* $M(D)$; és el subgrup de S_n generat per σ_0, σ_1 i σ_∞. És una mena de "grup de Galois"del dibuix.

2.2.2 Dibuixos via recobriments de l'esfera menys tres punts

Anem a veure que donar un dibuix d'infants és equivalent a donar un recobriment topològic de l'esfera menys tres punts. La construcció és purament topològica i serè una mica imprecís.

Prenem D un dibuix d'infants i posem al centre de cada cara un vèrtex nou, que denotarem $\circ$. Ara, dibuixem arestes d'aquest nou vèrtexs als vèrtexs $\bullet$ i $\star$ que estan a la seva frontera, les suficients fins a obtenir una triangulació de X_2. Tenim dos tipus de triangles segons l'orientació: els triangles que al girar (segons diu l'orientació) al voltant d'una cara obtenim la seqüència $\circ$, $\bullet$ i $\star$ (1), i els que obtenim $\circ$, $\star$ i $\bullet$ (2). Podem veure per exemple "l'estrella de tres puntes"en la figura 2.5.

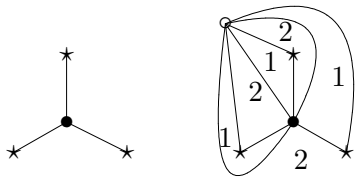


Figura 2.5: Triangulació de l'estrella de 3 puntes

Seguidament, anem identificant els triangles adjacents preservant l'orientació: o sigui, els triangles de tipus 1 entre si i els triangles de tipus 2 entre si. Al final obtenim una "papallona", formada per un triangle de tipus 1 amb un triangle de tipus 2 adjacent, compartint un vèrtex $\circ$ i un vèrtex $\bullet$. Finalment identifiquem els dos vèrtexs $\star$ i les arestes que surten d'aquests vèrtexs: obtenim finalment una esfera "triangulada"per dos triangles (un "interiorï l'altre "exterior"), amb tres punts destacats. D'aquesta manera tenim definida una aplicació continua $f\colon X_2 \to S^2$, que podem comprovar és no-ramificada fora dels vèrtexs (de tres tipus), amb grau de ramificació n =nombre d'arestes. Per tant tenim un recobriment finit i étale de

$$f\colon X_2 \setminus X_0 \longrightarrow S^2 \setminus \{\bullet, \circ, \star\}.$$

A l'inrevés, donat un recobriment $f\colon X \to S^2 \setminus \{\bullet, \circ, \star\}$, per resultats de topologia sobradament coneguts, podem compactificar-lo a un morfisme continu $f\colon \overline{X} \to S^2$, on $\overline{X}$ és una superfície compacta i orientable. Per obtenir un dibuix a $\overline{X}$ només ens cal prendre l'antiimatge d'un segment (camí) qualsevol de $\bullet$ a $\star$.

Es comprova que aquests dos processos són inversos un del altre (mòdul les equivalències corresponents).

2.2.3 Dibuixos via el grup lliure amb dos generadors

Anem a veure que donar un dibuix d'infants és equivalent a donar un subgrup del grup lliure amb dos generadors. Per a veure-ho utilitzarem la construcció topològica de la subsecció anterior.

En la subsecció anterior em vist que donar un dibuix és equivalent a donar un recobriment

$$f\colon X_2 \setminus X_0 \longrightarrow S^2 \setminus \{\bullet, \circ, \star\}.$$

Això correspon a donar un subgrup Γ d'index finit $= n$ del grup d'homotopia $\pi_1(S^2 \setminus \{\bullet, \circ, \star\}, x)$, on em fixat un punt x arbitrari. Degut a aquesta el·lecció del punt x aquest subgrup està ben definit mòdul conjugació. Ara només cal recordar que

$$\pi_1(S^2 \setminus \{\bullet, \circ, \star\}, x) = \langle l_0, l_1, l_\infty \mid l_0 l_1 l_\infty = 1\rangle \cong F_2$$

on denotem com és usual F_2 pel grup lliure amb dos generadors, i em denotat per l_i el camí que dóna la volta a cadascun dels vèrtexs (que a la llarga denotarem 0, 1 i ∞).

2.2.4 Dibuixos via corbes modulars

Una interpretació molt interessant dels dibuixos d'infants s'obté d'identificar el grup lliure amb dos generadors F_2 amb el grup modular

$$\Gamma(2) := \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv Id \,(\mathrm{mod})2\}\,,$$

amb generadors

$$A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{i } B := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Tenim per tant que donar un dibuix d'infants és equivalent a donar un subgrup Γ d'index finit de $\Gamma(2)$ (mòdul conjugació). En aquest cas podem interpretar X_2 com $\overline{\mathbb{H}}/\Gamma$, on $\mathbb{H}$ és el semiplà superior de Poincaré i $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{Q} \cup \infty$, i on Γ actua de manera usual. La interpretació topològica també és clara: tenim associada de manera canònica

$$f\colon \overline{\mathbb{H}}/\Gamma \longrightarrow \overline{\mathbb{H}}/\Gamma(2) \cong \mathbb{P}^1(\mathbb{C}) \cong S^2$$

que està ramificada sols sobre les "puntes"de $\overline{\mathbb{H}}/\Gamma(2)$, o sigui 0, 1 i ∞.

2.2.2 Remarca. Què passa si enlloc de prendre el grup modular $\Gamma(2)$ prenem el grup $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$? Observem que $\mathrm{SL}_2(\mathbb{Z})$ no és un grup lliure, i està generat per

$$A := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{i } B := \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

d'ordres 2 i 3 respectivament. Així, donat un subgrup Γ de $\Gamma(1)$, el morfisme que obtenim

$$f\colon \overline{\mathbb{H}}/\Gamma \longrightarrow \overline{\mathbb{H}}/\Gamma(1) \cong \mathbb{P}^1(\mathbb{C}) \cong S^2$$

està ramificat a sobre de 0 amb grau de ramificació ≤ 3 i amb grau de ramificació sobre de $1 \leq 2$. Això correspon en els dibuixos a que

les valències dels vèrtexs $\bullet$ són ≤ 3 i les valències dels vèrtexs $\star$ són ≤ 2.

És clar que donat dibuix qualsevol li correspon un subgrup Γ de $\Gamma(2)$, que podem veure també com un subgrup de $\Gamma(1)$ de forma canònica. Per tant a qualsevol dibuix li correspon un dibuix verificant que les valències dels vèrtexs $\bullet$ són ≤ 3 i les valències dels vèrtexs $\star$ són ≤ 2. Tenim una construcció natural en el món dels dibuixos que fa exactament això!. Primer ens cal considerar la triangulació que em construït abans i posar tots els vèrtexs $\bullet$, $\star$ i $\circ$ com a vèrtexs $\bullet$; això ens determina un dibuix net on totes les cares tenen valència 3. Seguidament posem vèrtexs $\star$ al mig de les arestes i vèrtexs $\circ$ al mig de les cares, i finalment intercanviem els vèrtexs $\circ$ i els vèrtexs $\bullet$. Vegis com a exemple l'estrella de tres puntes de la Figura 2.6.

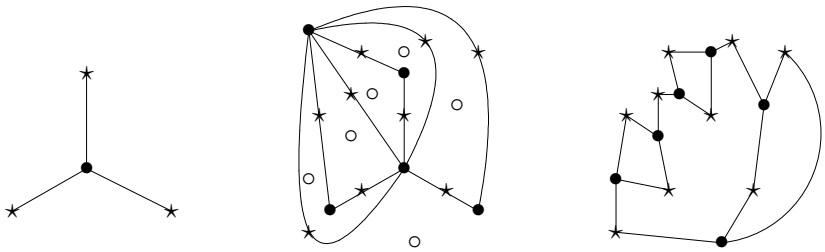


Figura 2.6: Triangulació de l'estrella de 3 puntes

Observem que els subgrups que ens surten no són en general subgrups de congruència, i per tant les corbes que obtenim no són corbes modulars "clàssiques"; tot i així, aquestes corbes tenen sovint propietats aritmètiques semblants, encara que no han estat estudiades amb detall (vegis l'article de B. Birch [4], i l'article de T. Scholl [23])

Amb tot el que em explicat fins ara ja tenim els ingredients necessaris per a entendre perfectament la interpretació que ens interessarà més: la correspondència de Grothendieck.

2.2.5 Dibuixos via grups triangulars

Anem a veure encara una altre caracterització dels dibuixos, via subgrups de uns certs grups (en general infinits). Siguin p, q i r tres nombres naturals, tots tres mes grans que 1, o, si un d'ells val 1, els altres dos son iguals i més grans que 1.

Definim el grup

$$\Delta := \Delta_{p,q,r} := \langle \sigma_0, \sigma_1, \sigma_\infty \mid \sigma_0^p = \sigma_1^q = \sigma_\infty^r = (\sigma_0\sigma_1\sigma_\infty) = 1 \rangle$$

anomenat grup triangular.

Habitualment es divideixen en tres tipus:

1. Si $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$, el cas esfèric. Fora permutacions, tenim els casos: $(p,q,r) = (1,n,n)$, $(2,2,n)$, $(2,3,3)$, $(2,3,4)$ i $(2,3,5)$.
2. Si $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$, el cas euclidià. Aquí només tenim els tres casos $(p,q,r) = (2,3,6)$, $(3,3,3)$ i $(2,4,4)$.
3. Si $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, el cas hiperbòlic.

Considerem ara, en cadascun dels casos, el triangle T amb angles π/p, π/q i π/r dibuixats en l'esfera S^2, el pla $\mathbb{C}$ o bé el pla hiperbòlic $\mathbb{H}$.

Aleshores podem fer actuar, també depenen de cada cas, el grup triangular Δ, a l'esfera (o, millor, a $\mathbb{P}^1(\mathbb{C})$), al pla o bé a $\mathbb{H}$, tenint com a domini fonamental el triangle T juntament amb la seva reflexió respecte algun dels costats.

Per exemple, en el cas esfèric, podem pensar el grup Δ com un subgrup finit de $\mathrm{PGL}_2(\mathbb{C})$. Aquests subgrups són coneguts de fa molt i són $\mathbb{Z}/n\mathbb{Z}$, D_{2n} amb $n \geq 2$, A_4, S_4 i A_5. Dibuixant el triangle T juntament amb els seus traslladats obtenim uns dibuixos en l'esfera si posem cada vertex com a $\bullet$, $\star$ o $\circ$.

En el cas euclidià obtenim certs subgrups infinits de $\mathrm{SL}_2(\mathbb{Z})$, que després comentarem.

Finalment, en el cas hiperbòlic obtenim grups Fuchsians cocompactes, subgrups de $\mathrm{PSL}_2(\mathbb{R})$, també molt estudiats.

En cadascun d'aquests casos el quocient $\Delta\backslash\mathbb{P}^1(\mathbb{C})$, $\Delta\backslash\mathbb{C}$ i $\Delta\backslash\mathbb{H}$ és isomorf de manera natural a $\mathbb{P}^1(\mathbb{C})$. Per exemple, en l'últim cas l'isomorfisme bé donat per la funció triangle de Schwartz (els altres dos casos són molt més fàcils).

Prenent l'antiimatge d'un segment de $\bullet$ a $\star$ (o si és vol, de $[0,1]$) obtenim "dibuixos" $D_{p,q,r}$ en cadascun d'ells: en l'esfera, els que em obtingut abans; en els altres dos casos obtenim dibuixos infinits que es poden construir també traslladant els triangles per l'acció del grup més les reflexions respecte els costats.

Ara, donat un dibuix D, considerem p un múltiple comú de les valències dels vèrtexs $\bullet$, q un múltiple comú de les valències dels vèrtexs $\star$ i r un múltiple comú de les valències de les cares. Tenim aleshores que el nostres dibuix D pot ser obtingut com a quocient del dibuix universal $D_{p,q,r}$ per l'acció d'un cert subgrup Γ de Δ. Clarament podem fer el procés invers per obtenir que és equivalent donar un dibuix que donar un subgrup del grup triangular Δ.

El recobriment de $\mathbb{P}^1(\mathbb{C})$ que correspon a un dibuix és aleshores el morfisme natural donat per (en el cas hiperbòlic): $\Gamma\backslash\mathbb{H} \longrightarrow \Delta\backslash\mathbb{H}$. El dibuix, com ja em dit, es pot obtenir purament fent quocient del dibuix universal amb valencies (p,q,r).

De fet, si considerem els casos en que p, q o r poden ser ∞, aleshores obtenim subgrups fuchsians que ja no són cocompactes, però podem fer el mateix amb el semiplà "completat" $\overline{\mathbb{H}}$. Per exemple, el cas $p=q=r=\infty$ obtenim el que em fet a la secció anterior (el grup corresponent és $\Gamma(2)$); en el cas $p=2$, $q=3$ i $r=\infty$ obtenim el grup modular $\Gamma(1)$; en el cas $p=2$, $q=r=\infty$ el grup cartogràfic orientat, etc.

Aquesta interpretació ens serveix per a estudiar molt bé els casos dels recobriments "normals". Situem-nos en el cas hiperbòlic. Aleshores el recobriment donat per $\mathbb{H} \to \mathbb{H}/\Gamma$ és el recobriment universal si i només si p, q i r són les valencies de cada vèrtex $\bullet$, $\star$ o $\circ$ respectivament, i per tant tots els vèrtex de cada tipus tenen les mateixes valències: es diu aleshores que el dibuix és equilibrat (*balanced* en anglès). Això correspon també a que Γ sigui un subgrup normal i lliure de torsió de Δ.

2.3 La correspondència de Grothendieck

Recordem que en la primera xerrada em vist l'anomenat "Teorema dels tres punts"de Belyî: Una corba C (projectiva i no singular) sobre $\mathbb{C}$ és isomorfa a una corba definida sobre $\overline{\mathbb{Q}}$ si i només si hi ha un morfisme $f\colon C \to \mathbb{P}^1$ ramificat només a sobre de 0, 1 i ∞.

Anomenarem un tal morfisme f un morfisme de Belyî. Observem que una corba donada pot tenir (i de fet té) molts morfismes diferents de Belyî. El punt que ens interessa ara és que

2.3.1 Teorema. *Donar un dibuix d'infants D és equivalent a donar una parella (C, f) on C és una corba projectiva i no singular sobre $\overline{\mathbb{Q}}$ i f és un morfisme de Belyî, mòdul isomorfisme de parelles; és a dir que (C, f) i (C', f') són isomorfs si existeix un isomorfisme $\psi : C \to C'$ tal que el següent diagrama és commutatiu:*

$$\begin{array}{ccc} C & \xrightarrow{\psi} & C' \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f'} & \\ & \mathbb{P}^1 & \end{array}$$

La demostració és fàcil de fer del que em vist fins ara. Per exemple, per obtenir el dibuix del morfisme f sols em de "dibuixar" $f^{-1}([0,1])$; els vèrtexs $\bullet$ són els punts de $f^{-1}(0)$ i els vèrtexs $\star$ són els punts de $f^{-1}(1)$ (les antiimatges de ∞ corresponen a les cares).

Al revés, donar un dibuix és equivalent a donar un recobriment continu finit $f\colon X_2 \to S^2$, ramificat només en tres punts (vegis la subsecció 2.2.2) . Identifiquem S^2 amb $\mathbb{P}^1(\mathbb{C})$ enviant els tres punts a 0, 1 i ∞ adequadament. Utilitzant el morfisme f podem dotar d'estructura de superfície de Riemann a X_2, i per GAGA X_2 és així el conjunt de punts complexos de una corba algebraica, projectiva i no-singular. El morfisme f (vist ara com a morfisme de corbes algebraiques) és un morfisme de Belyî i per la part fàcil del teorema de Belyî esta definit sobre $\overline{\mathbb{Q}}$.

Una altre manera: utilitzant la interpretació modular, tenim que donar un dibuix és equivalent a donar un subgrup Γ de $\Gamma(2)$, i per tant un morfisme de corbes algebraiques sobre $\mathbb{C}$

$$f\colon C := \overline{\mathbb{H}}/\Gamma \longrightarrow \overline{\mathbb{H}}/\Gamma(2) = X(2) \cong \mathbb{P}^1(\mathbb{C}).$$

Una interpretació modular "adequada"ens pot servir per a veure que C està definida de fet sobre un cos de nombres.

Finalment, la interpretació via els grups triangulars també ens dona el morfisme de Belyî buscat.

2.3.2 Propietats. Sigui D un dibuix d'infants i $f\colon C \to \mathbb{P}^1$ la funció de Belyî associada. Aleshores

1. Cada vèrtex $\bullet$ del dibuix correspon a un punt $P \in \mathbb{P}^1(\overline{\mathbb{Q}})$ amb $f(P) = 0$. A més la valència del vèrtex és igual al índex de ramificació de f en P.

2. Cada vèrtex $\star$ del dibuix correspon a un punt $Q \in \mathbb{P}^1(\overline{\mathbb{Q}})$ amb $f(Q) = 1$. A més la valència del vèrtex és igual al índex de ramificació de f en Q.

3. Cada cara del dibuix correspon a un punt $R \in \mathbb{P}^1(\overline{\mathbb{Q}})$ amb $f(R) = \infty$. A més la valència de la cara és igual al índex de ramificació de f en R.

4. El grup de monodromia de D és igual al grup de Galois de la clausura galoisiana de $f\colon C \to \mathbb{P}^1$; o sigui de la clausura galoisiana de l'extensió de cossos $\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(T)$ associada a f, on T és una indeterminada i $K(C)$ és el cos de funcions de C.

Anem a veure uns quants exemples bàsics de funcions de Belyî amb els seus dibuixos associats. Observem primer que a l'hora de calcular la funció de Belyî associada a un dibuix tenim la llibertat d'escollir alguns punts del dibuix amb valors concrets. Per exemple, per a dibuixos en el pla (i.e. en gènere 0) la funció quedara completament definida (no només fora d'isomorfisme) si fixem tres punts del pla; és habitual en aquest cas fixar que el punt ∞ vagi al punt ∞, i escollir dos vèrtexs del dibuix que siguin 0 i 1. Per gènere 1 és habitual també demanar que el 0 de la corba el·líptica associada l'enviem a ∞ (però no sempre obtenim així els dibuixos més "bonics"). Un dibuix juntament amb un punt fixat que va a parar a ∞ s'anomena un dibuix *marcat*.

2.3.3 Exemples. 1. L'estrella de n-puntes, com l'estrella de 6 puntes que em vist abans a l'exemple 1 de 2.1.1, té una funció

de Belyĭ molt evident: $f(z) = z^n$. De fet són els únics dibuixos que estan ramificats només sobre de dos punts (el 0 i l'infinit). El centre de l'estrella és el zero i les puntes de l'estrella són les arrels enèsimes de l'unitat.

2. La doble estrella amb n i m puntes, com la doble estrella amb 3 i 4 puntes (l'exemple 2 de 2.1.1), correspon també a una funció de Belyĭ que ja coneixem. Si prenem que un dels centres sigui 0 i l'altre sigui 1, volem una funció que s'anul·li en el 0 amb multiplicitat n i en el 1 amb multiplicitat m. Si considerem la funció $z^n(1-z)^m$ compleix això, però els altres punts de ramificació (de fet l'altre punt, que és $n/(n+m)$, corresponen al vertex $\star$ entre 0 i 1 amb valència 2) no té imatge 1. Per que tingui imatge 1 cal normalitzar la funció: obtenim

$$f(z) := \frac{(n+m)^{n+m}}{m^m n^n} z^n (1-z)^m,$$

que com ja us heu donat compte és la funció que Belyĭ utilitza en la demostració del seu teorema.

3. Un exemple general també molt utilitzat és el que correspon al dibuix

o sigui, n vèrtexs, la meitat $\bullet$ i l'altre meitat $\star$ si n és parell, i si n és senar un més de $\bullet$. La idea és considerar el polinomi de Txebixev

$$P_n(z) := \cos((n-1)\arccos(z)))$$

Aquest polinomi val ± 1 pels valors $z = \cos(\frac{i\pi}{n-1})$ amb $i = 0, \ldots, n-1$, i són els únics valors on s'anul·la la derivada. Podem convertir-la a la funció de Belyĭ que ens interessa prenen

$$f_n(z) := \frac{1}{2}(1 - P_n(z)).$$

Veurem alguns exemples per a gènere > 0 en la última secció. Anem a veure un primer procediment fàcil per a calcular la funció de Belyĭ associada a un dibuix pel cas de gènere 0.

2.4 Càlcul explícit per gènere 0

Comencem primer per un cas ja suficientment interessant: el cas dels arbres. Un dibuix en el pla és un arbre si només té una cara (l'exterior). En aquest cas, si seguim el procediment habitual de demanar que ∞ vagi a ∞ tenim que la funció de Belyî corresponent és un polinomi. Els polinomis que apareixen són, en certa manera, generalitzacions naturals dels polinomis de Txebixev, i certs autors els anomenen polinomis de Shabat. En general ens interessen polinomis que sols tenen dos punts crítics, en el sentit que les imatges dels zeros de la derivada només prenen dos valors (habitualment 0 i 1, o bé ± 1).

Associem a l'arbre T donat dues llistes de valències: les valències $V_0 = \{u_1, \ldots, u_n\}$ de manera que tenim u_i vèrtexs $\bullet$ de valència i, i $V_1 = \{v_1, \ldots, v_m\}$ igualment amb els vèrtexs $\star$. Considerem ara polinomis mònics $P_i(z)$ de grau u_i i $Q_j(z)$ de grau v_j, on els coeficients són indeterminades. Aleshores el polinomi que busquem és un polinomi $P(z)$ tal que

$$P(z) = \prod_{i=1}^{n} P_i(z)^i \quad \text{i} \quad P(z) - k = \prod_{j=1}^{m} Q_j(z)^j,$$

on k és una constant també indeterminada, que demanarem no valgui 0(de manera que el polinomi tindrà com a valors crítics 0 i k). Aquestes igualtats ens donen unes equacions però no tenen una solució única doncs encara tenim masses graus de llibertat. Una possible opció es fixar dos vèrtexs concrets i dir que seran el 0 i el 1. Anem a veure en un exemple concret com funciona això (he fet servir Maple per a fer els càlculs).

2.4.1 Exemple. Considerem l'arbre

Les llistes de valències són $V_0 = \{1, 1, 1\}$ i $V_1 = \{2, 2\}$. Fixarem que l'únic vèrtex $\bullet$ de valència 3 sigui l'1, i que l'únic vèrtex $\bullet$ de valència 2 sigui el 0. Aleshores tenim que

$$P_1(z) := z + A \qquad P_2(z) = z \qquad P_3(z) = z - 1$$

i que

$$Q_1(z) = z^2 + D_{1,1}z + D_{1,0} \qquad Q_2(z) = z^2 + D_{2,1}z + D_{2,0}$$

Obtenim finalment l'equació que s'ha de verificar és

$$(z+A)z^2(z-1)^3 - k = (z^2 + D_{1,1}z + D_{1,0})(z^2 + D_{2,1}z + D_{2,0})^2.$$

Desenvolupant obtenim un sistema d'equacions per resoldre que ens donaran les possibles solucions. És clar que entre d'aquestes solucions n'hi haurà de no vàlides (per exemple, amb $k = 0$). Un cop tretes aquestes solucions maple ens diu que, si denotem $D_{2,1} = \alpha$, aleshores tenim que

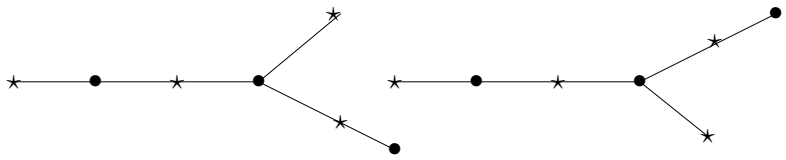
$$k = -\frac{1}{125}\left(8 + 10\,\alpha + 3\,\alpha^2\right)(2\,\alpha + 1)^2, \quad D_{1,1} = \frac{-4}{5}\,\alpha - \frac{12}{5},$$

$$D_{2,0} = \frac{-2}{5}\,\alpha - \frac{1}{5}, \quad D_{1,0} = \frac{3}{5}\,\alpha^2 + 2\,\alpha + \frac{8}{5}, \quad A = \frac{3}{5} + \frac{6}{5}\,\alpha$$

i que α és arrel del polinomi $s(z) := 2 + 18X + 18X^2 + 5X^3$. Aquest polinomi té tres arrels, una real i dues complexes. La funció de Belyî que busquem és

$$f(z) = \frac{1}{k}(z+A)z^2(z-1)^3$$

on α és l'arrel real. Els dibuixos corresponents a les dues arrels complexes són els dibuixos



que com podeu comprovar tenen les mateixes llistes de valències (i són "conjugats"respecte la conjugació complexa!).

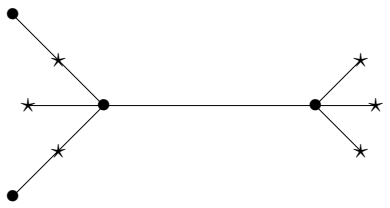
2.4.2 Observació. 1. Observem d'aquest exemple varies coses: el mètode de càlcul que proposem només depend de les llistes de valències. Per tant tindrà com a mínim tantes solucions com nombre de dibuixos diferents amb les mateixes llistes de valències.

2. Si una funció de Belyî està definida sobre un cos de nombres $\neq \mathbb{Q}$, podem fer actuar un element σ de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ i obtenir una altre funció de Belyî f^σ. Aleshores el dibuix associat a f^σ tindrà les mateixes llistes de valències.

3. No sempre podrem associar a un vèrtex el 0 i a un altre vèrtex l'1 i obtenir el dibuix definit en un cos K el més petit possible, doncs potser aquells vèrtexs no corresponen a punts K-racionals de la corba C.

Anem a veure un parell de exemples per a comprovar aquesta última observació. Els he calculat amb el programa en Maple que he detallat abans.

2.4.3 Exemple. Considerem el següent arbre, que a simple vista no és veu cap arbre conjugat



Tenim que les llistes de valències són $V_0 = (2,0,0,2)$ i $V_1 = (4,3)$. Posem el 0 i l'1 en els dos vèrtexs amb valència 4. Al fer els càlculs obtenim dues funcions de Belyî

$$\widetilde{f}(z) := \frac{729}{32}\left(18z^2 - (18+10\sqrt{5})z - 5\sqrt{5} + 15\right)(z-1)^4 z^4$$

depenen de prendre una arrel quadrada de 5. Però els dibuixos per a cada una d'elles són equivalents, sols intercanviant els papers del 0 i del 1. Si posem $\pm\sqrt{5}$ als dos vèrtexs de valència 4 obtenim sols una funció de Belyî, definida a $\mathbb{Q}$:

$$f(z) := \frac{3^6}{2^{14}5^5}(9z^2 - 50z + 105)(z^2-5)^4$$

De fet, si posem els vèrtexs a $\pm 1/\sqrt{5}$ encara obtenim una funció més senzilla:

$$f(z) := \frac{3^6}{2^{14}}(45z^2 - 50z + 21)(5z^2 - 1)^4,$$

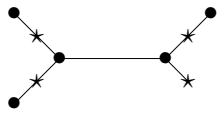
i tenim que

$$f(z)-1 = \frac{5^2}{2^{14}}(405z^4+360z^3-90z^2-168z-43)(1+15z-45z^2+45z^3)^2$$

El fet que surtin aquestes potencies de 2, de 3 i de 5 està lligat a que aquests són els nombres primers que surten a les valencies dels vèrtexs i de la cara (podeu comprovar que la cara té valencia 10).

Vegem un altre exemple, que aquest cop no està definit sobre $\mathbb{Q}$.

2.4.4 Exemple. Considerem el següent arbre, que té clarament un arbre "conjugat".



Tenim que les llistes de valències són $V_0 = (3, 0, 2)$ i $V_1 = (1, 4)$. Posem el 0 i el 1 en els dos vèrtexs de valència 3. Al fer els càlculs obtenim quatre funcions de Belyî depenen de prendre una arrel de $1 - 3X + 18X^2 + 42X^3 + 21X^4$, que són

$$-\frac{1}{2} \pm \frac{1}{42}\sqrt{567 \pm 210\sqrt{-3}}.$$

Dues d'aquestes arrels,

$$\alpha_1 := -\frac{1}{2} + \frac{1}{42}\sqrt{567 + 210\sqrt{-3}} \text{ i } \alpha_2 := -\frac{1}{2} - \frac{1}{42}\sqrt{567 + 210\sqrt{-3}}$$

ens donen dibuixos isomorfs, amb els vèrtexs corresponents a 0 i a 1 intercanviats. Si posem ara els vèrtexs amb valència 3 a les dues arrels α_1 i α_2 obtenim dues funcions de Belyî, depenen ara d'escollir

$\pm\sqrt{-3}$. Concretament la funció que obtenim és

$$f(z) = \frac{1}{2^{11}7^{16}}(600659397 + 445987849\sqrt{-3})(14406z^3 + \\ (33516 + 4410\sqrt{-3})z^2 + +(9441 + 4983\sqrt{3})z - 16182 - 3478\sqrt{-3}) \\ (-42z^2 - 42z + 3 + 5\sqrt{-3})^3$$

Observem que aquesta funció de Belyî té a simple vista mala reducció en el 2 i en el 7. Ens podem preguntar si és possible trobar una altre funció de Belyî amb coeficients més petits, i probablement és així, però després veurem que no és possible treure del denominador el 2 i el 7.

Si enlloc de considerar arbres volem considerar dibuixos generals en el pla, un possible mètode de càlcul és utilitzar un procediment semblant al anterior: considerem $V_0 = \{u_1, \ldots, u_n\}$, $V_1 = \{v_1, \ldots, v_m\}$ i $V_\infty = \{w_1, \ldots, w_s\}$ les llistes de valències sobre de 0, 1 i ∞ respectivament. Fixem per exemple que ∞ estigui a la cara amb valència més gran, i la treiem de la llista de valències. Definim com abans polinomis mònics $P_i(z)$ de grau u_i, $Q_j(z)$ de grau v_j i $R_k(z)$ de grau w_k, i considerem

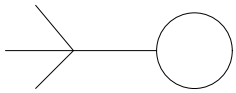
$$P(z) = \prod_{i=1}^{n} P_i(z)^i \ , \ Q(z) = \prod_{j=1}^{m} Q_j(z)^j \ \text{ i } \ R(z) = C\prod_{k=1}^{s} R_k(z)^k,$$

on C és una constant diferent de 0. La condició que s'ha de complir aleshores és que

$$P(z) - R(z) = \pm Q(z)$$

on el signe depend de si $P(z)$ té el grau més gran que $R(z)$ o no. Si a més em fixat dues condicions més (per exemple dos vèrtexs que posem en el 0 i en el 1), aquesta equació sols té un nombre finit de solucions; una de les solucions ens dona la funció de Belyî que busquem posant $P(z)/R(z)$. Per a resoldre el sistema obtingut una possible manera és utilitzant bases de Gröbner (vegeu el capítol 3 on es detalla aquest mètode).

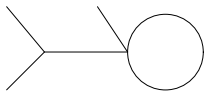
2.4.5 Exemple. Considerem el següent dibuix net



Les llistes de valències són $V_0 = (3, 0, 1, 1)$, 5 vèrtexs $\star$ de valència 2 corresponents a les arestes, i dues cares, una de valència 1 (l'interior) i una altre de valència 9, l'exterior (recordeu que quan es passa per una aresta pels dos costats es conta dos cops!). La cara de valència 9 és la que té ∞, i posem els vèrtexs de valència 4 i 3 en el 0 i l'1 respectivament. Aleshores obtenim tres solucions, depenen de prendre una arrel α de $147X^3 + 468X^2 + 468X + 140$:

$$f(z) = -\frac{3^3}{2^8 5^4 7}\frac{z^4(z-1)^3}{(5z - 7\alpha - 9)}(160765 + 453681\alpha + 265923\alpha^2)$$
$$(175z^3 + (700\alpha + 525)z^2 + (2268\alpha^2 + 1680 + 4116\alpha)z - 1260 -$$
$$1836\alpha^2 - 3432\alpha)$$

Aquest polinomi té una arrel real, que ens dóna el nostre dibuix, i dues arrels complexes que ens donen el dibuix



i el seu conjugat evident.

Podeu veure a les figures 2.7 i 2.8, com són realment els dibuixos associats a aquestes funcions de Belyî. Han estat dibuixades amb maple trobant l'antiimatge per la funció de Belyî d'uns quants punts a l'interval $[0, 1]$.

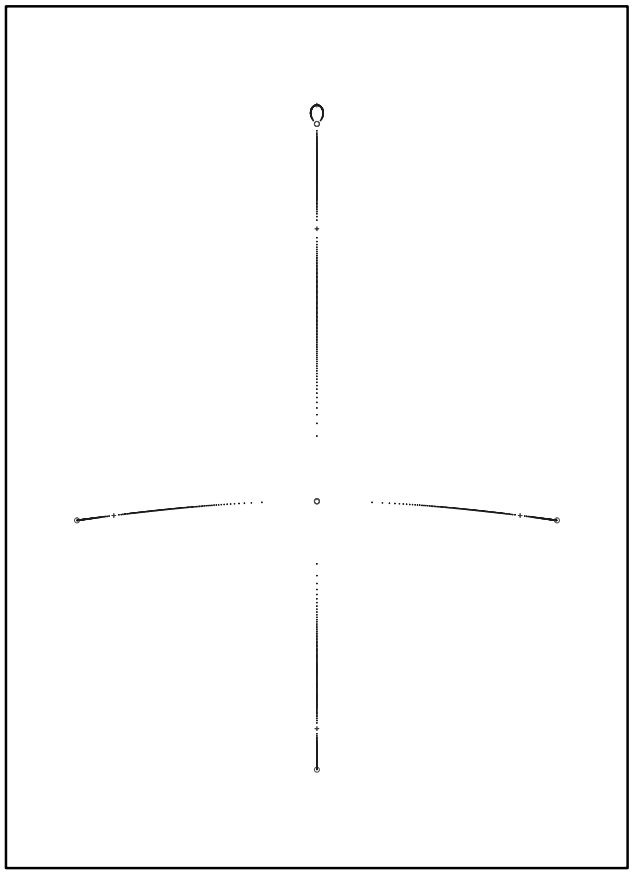


Figura 2.7: Dibuix associat a l'arrel real.

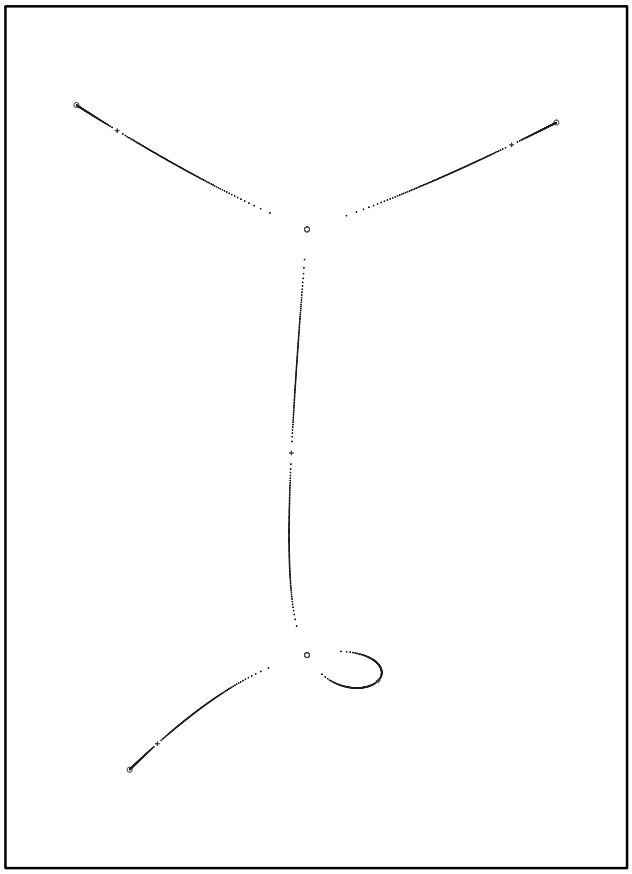


Figura 2.8: Dibuix associat a una arrel complexa.

2.5 Cos de definició i cos de moduli

A l'hora de calcular la funció de Belyî associada a un dibuix ens interessa trobar-la definida en el cos el més petit possible. Anem a estudiar si realment existeix tal cos, i a més si podem calcular una cota pel grau sobre $\mathbb{Q}$.

2.5.1 Definició Sigui D un dibuix d'infants i sigui $f\colon C \to \mathbb{P}^1$ una funció de Belyî associada. Donada $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, sigui f^σ la funció de Belyî obtinguda de f al composar amb σ. Aleshores D^σ denotarà el dibuix associat a f^σ.

Direm que un dibuix està definit sobre un cos $K \subset \mathbb{C}$ si existeix $f\colon C \to \mathbb{P}^1$ una funció de Belyî associada definida sobre K.

El teorema de Belyî ens assegura que tot dibuix està definit sobre $\overline{\mathbb{Q}}$, i per tant sobre algun cos de nombres K. Anem a veure si existeix el cos més petit on D està definit.

Comencem per observar que

2.5.2 Lema. *Donat un dibuix D i $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, el dibuix conjugat D^σ té la mateixa llista de valencies $\tau(D)$ i el mateix grup de monodromia $G(D)$.*

La demostració és molt fàcil i us la deixem com a exercici.

D'aquest lema elemental obtenim de manera evident el següent resultat.

2.5.3 Proposició. *Donat un dibuix D, considerem el subgrup H_D de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ format per les σ tal que D^σ és equivalent a D. Aleshores*

$$K_D := (\overline{\mathbb{Q}})^{H_D}$$

és una extensió finita de $\mathbb{Q}$. A més, si denotem per n_D el nombre de dibuixos D' diferents amb $\tau(D) = \tau(D')$ i $G(D) = G(D')$ (n'hi ha clarament un nombre finit), aleshores

$$[K\colon \mathbb{Q}] \leq n_D.$$

El cos K_D que acabem de definir s'anomena el cos de moduli de D. Aquest és el candidat natural a ser el mínim cos de definició de D, però es pot veure que no sempre podem definir el dibuix en el seu cos de moduli.

2.5.4 Exemple. El dibuix prenet de la Figura 2.9 té cos de moduli real, però no pot ser definit en els reals.

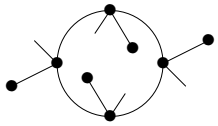


Figura 2.9: Cos de moduli real no definit a $\mathbb{R}$.

La demostració d'aquest fet la podeu veure a l'article de J.-M. Couveignes i L. Granboulan [8].

Per tal d'obtenir un cos on el dibuix estigui definit podem optar per a treballar amb dibuixos marcats. Un dibuix marcat (D, P) és un dibuix D juntament amb un punt P fixat a dins d'una cara (i per tant tal que la funció de Belyĭ associada envia P a ∞). Dos dibuixos marcats són equivalents si hi ha una equivalència que envia els punts marcats d'un a l'altre. Per exemple, en el cas dels dibuixos en gènere 0 que em considerat abans de fet els em considerat com a dibuixos marcats doncs en certa manera fixavem la cara exterior (o sigui, deiem que ∞ anava a ∞). En l'exemple anterior tenim una equivalència de dibuixos entre el dibuix i ell mateix que no és una equivalència com a dibuixos marcats; és la que envia la cara interior a la cara exterior. Anàlogament, en el cas de gènere 1 posarem el 0 de la corba el·líptica en una cara.

Direm que un dibuix marcat està definit sobre un cos K si la funció de Belyĭ ϕ està definida sobre el cos K, i el punt fixat P de C sobre ∞ és K-racional.

2.5.5 Teorema. *Sigui (D, P) un dibuix marcat i sigui $m = m_{(D,P)}$ el nombre de dibuixos marcats (D', P') (mòdul equivalència de dibuixos*

marcats) tals que $\tau(D) = \tau(D')$ *i* $G(D) = G(D')$*. Aleshores tenim un cos* K *minimal de definició del dibuix marcat amb*

$$[K\colon \mathbb{Q}] \leq m.$$

La demostració és senzilla utilitzant el criteri de Weil: prenem com abans el subgrup H de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ format per les σ's que fixen el dibuix marcat i construïm el cos de moduli K del dibuix marcat. El punt en la corba que hem fixat és clarament fix per H, i per tant està definit sobre K. Això és el que ens permet veure que la corba i el morfisme estan els dos definits sobre K. Per a ser estrictes cal tractar primer el cas en que el dibuix marcat no té automorfismes (que és el cas general); el cas amb automorfismes es dedueix d'aquest observant que el grup d'automorfismes del dibuix marcat ha de ser un grup cíclic, i al fer quocient respecte aquest grup obtenim un dibuix marcat sense automorfismes (podeu consultar un esbós més detallat de la demostració a [4]).

Com a conseqüència òbvia tenim que si hi ha un sola cara, per exemple en el cas dels arbres, el cos de moduli és un cos de definició.

2.5.6 Exercici. Sigui D un dibuix tal que té un únic vèrtex $\bullet$ o un únic vèrtex $\star$ o una única cara amb una valència fixada. Aleshores el cos de moduli de D és un cos de definició de D.

També utilitzant aquest resultat podem veure la relació entre el cos de moduli i el cos de definició d'un dibuix (ara sense marcar) (vegeu [7]).

2.5.7 Corol·lari. *Sigui* D *un dibuix i* K_D *el seu cos de moduli. Aleshores* K_D *és l'intersecció de tots els cossos de definició de* D*.*

En el cas dels dibuixos en gènere zero, tenim una manera elemental de veure que el cos de moduli d'un dibuix marcat és un cos de definició: diem que una funció de Belyĭ $f(z)$ que envia ∞ a ∞ està en forma standard si la suma dels zeros de f val 0 i la suma dels zeros de $f(z) - 1$ val 1.

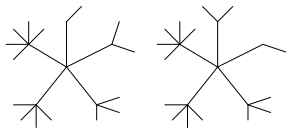
2.5.8 Lema. *Tot dibuix marcat en gènere 0 li correspon una única funció de Belyĭ standard. Aquesta funció de Belyĭ esta definida en el cos de moduli del dibuix marcat.*

La demostració de la existència i la unicitat és un exercici fàcil. De la unicitat és clar aleshores que ha de ser fixa pels elements del grup de Galois absolut que deixen el dibuix marcat invariant, i per tant que té coeficients en el cos de moduli del dibuix marcat.

El problema fonamental de la teoria dels dibuixos d'infants és poder determinar el cos de moduli d'un dibuix (o d'un dibuix marcat) utilitzant propietats "topològiques" del dibuix. Es tractaria per exemple de donar una llista d'invariants associats a un dibuix, o sigui classe de conjugació per Galois d'un dibuix, de manera que dos dibuixos siguin conjugats per Galois si i només si tenen els mateixos invariants. Si es conegués aquesta llista completa d'invariants podriem saber el grau del cos de moduli d'un dibuix calculant el nombre de dibuixos amb els mateixos invariants que el nostre dibuix.

Com a exemples de invariants de dibuixos tenim la llista de valencies i el grup de monodromia. Però es sabut que aquests invariants no són suficients. L'exemple més conegut són les "flors de Leila".

2.5.9 Exemple. Considereu el següents arbres:



amb l'estructura bipartita natural (o sigui, un $\bullet$ al vèrtex del mig, $\star$ als següents vèrtexs i $\bullet$ als vèrtexs finals de valència 1). Podeu veure clarament que aquests dibuixos no són iguals, però tenen la mateixa llista de valències. De fet hi ha 24=4! dibuixos amb la mateixa llista de valències. A més tots ells tenen el mateix grup de monodromia igual a S_{20}. Però aquests dos arbres concrets no són conjugats de Galois. De fet (podeu veure l'article de L. Schneps [22] on detalla el resultat) els dibuixos en qüestió estan definits sobre un cos de grau 12, i tenen cadascun d'ells 12 conjugats de Galois (contant-los a ells mateixos). Així la classe de valències es trenca en dues classes de conjugació. Vegis també l'article de L. Zapponi [37] on es troba un invariant que els diferencia.

En aquests sentit s'ha proposat altres possibles invariants per a dibuixos en general, com el grup cartogràfic (que no és res més que

el grup de monodromia del dibuix net associat), el grup d'automorfismes, les classes de Nielsen racionals, i altres invariants semblants proposats a [35], i per a certs tipus de dibuixos: dibuixos en gènere zero [12] i arbres [37].

Un cop sabem alguna cota sobre el grau del cos de definició, podem preguntar-nos si podem dir alguna cosa sobre la reducció de la corba, o del recobriment, o també sobre els primers del cos K on ramifiquen. Direm, com és usual, que un morfisme $\phi\colon C \to \mathbb{P}^1$ definit sobre un cos de nombres K té bona reducció en $\mathfrak{p}$ un primer de K si existeix un model $\psi\colon \mathcal{C} \to \mathbb{P}^1$ de ϕ definit en el localitzat per $\mathfrak{p}$ de l'anell d'enters de K amb $\mathcal{C}$ llisa i projectiva i tal que la reducció de ψ mòdul $\mathfrak{p}$ té la mateixa ramificació que ϕ (o sigui, que ramifica amb el mateix nombre de punts i amb els mateixos índexs de ramificació).

El següent resultat és una conseqüència fàcil de la teoria del grup fundamental étale de Grothendieck, i va ser demostrat explícitament per S. Beckmann [2].

2.5.10 Teorema. *Sigui (D, P) un dibuix marcat i K el seu cos de definició. Sigui $G = G(D)$ el seu grup de monodromia i considerem $\mathfrak{p}$ un primer de K que no divideixi l'ordre de G. Aleshores tenim un model (C, ϕ, P) de D definit sobre K amb bona reducció mòdul $\mathfrak{p}$, i a més $\mathfrak{p}$ no ramifica a K.*

La demostració utilitza de manera essencial el lema d'Abhyankar, a part de la teoria del grup fonamental étale de Grothendieck. De fet, com segurament ja heu vist, el punt clau és que estem estudiant recobriment amb ramificació *moderada*.

Què podem dir dels primers que divideixen l'ordre de G? Observem primer que els primers que divideixen l'ordre d'alguna de les permutacions σ_0, σ_1 o σ_∞ són clarament de mala reducció de ϕ.

A part d'aquest resultat fàcil tenim el següent resultat recent de S. Wewers ([32],[33]), basat en els resultats de Raynaud sobre aixecament de recobriments de Galois en característica p.

2.5.11 Teorema. *Sigui D un dibuix i K el seu cos de moduli. Sigui $G = G(D)$ el seu grup de monodromia i considerem p un primer que divideixi estrictament l'ordre de G (o sigui que p^2 no divideixi l'ordre*

de G). Aleshores p és com a molt moderadament ramificat a K.

2.6 Alguns exemples per gènere > 0

Anem a veure alguns exemples de resultats per el cas en que el gènere és més gran que zero. Pel que jo sé no hi ha un mètode efectiu per, donat un dibuix D en gènere > 0, calcular la corba i el morfisme de Belyî associats. Però en certs casos concrets es pot calcular per exemple reduint-se al cas de gènere zero. Més que un tractament sistemàtic el que farem serà anar donant un llista d'exemples i resultats.

2.6.1 Funcions de Belyî per a corbes el·líptiques

Comencem per a pensar un moment com podem trobar donada una corba el·líptica E sobre $\mathbb{Q}$ (per simplificar) un morfisme de Belyî $\phi\colon E \to \mathbb{P}^1$ també definit sobre $\mathbb{Q}$.

Considerem la involució hiperel·líptica ι i prenem $E/\iota \cong \mathbb{P}^1$. Aleshores el morfisme quocient $f\colon E \to \mathbb{P}^1$ que ens determina és un morfisme de grau 2 ramificat fora de quatre punts (els punts hiperellítpics). Concretament, si donem E amb una equació de Weierstrass $Y^2 = P(X)$, on $P(X)$ és un polinomi de grau tres amb coeficients a $\mathbb{Q}$, aleshores el morfisme que estem considerant és en la part afí $f(X, Y) = X$, i els punts sobre d'on ramifica són les tres arrels de $P(X)$ i el punt de l'infinit.

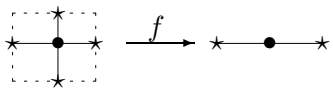
Anem a construir un funció de Belyî utilitzant aquest morfisme; l'únic que hem de fer és construir una funció de Belyî $\beta\colon \mathbb{P}^1 \to \mathbb{P}^1$ definida sobre $\mathbb{Q}$ tal que porti els tres punts anteriors i l'infinit a $\{0, 1, \infty\}$. Per exemple, si els tres punts són racionals (o sigui, si la corba E té els punts d'ordre 2 definits a $\mathbb{Q}$), podem enviar l'arrel més petita a 0 i l'arrel més gran a 1. La tercera arrel serà un nombre racional entre 0 i 1, o sigui de la forma $\frac{n}{n+m}$ per a n i m naturals. Aleshores la funció

$$\beta(X) = \frac{(n+m)^{n+m}}{m^m n^n} X^n (1-X)^m$$

és la funció que busquem (després d'aplicar isomorfisme portant les tres arrels a 0, 1 i $\frac{n}{n+m}$).

Per exemple, si prenem la corba el·líptica $Y^2 = X^3 - X$, les tres arrels són 0, 1 i -1, i podem purament aplicar $\beta(X) = X^2$. Obtenim una funció de Belyî de grau 4.

El dibuix associat és



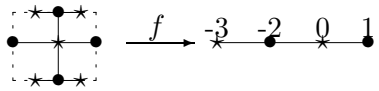
Fixeu-vos que el dibuix obtingut és el mateix que em fet en l'exemple 1 (enviant però el punt ∞ de E a 0). O sigui que l'exemple 1 és la corba $Y^2 = X^3 - X$ amb el morfisme de Belyî $\phi(X, Y) = 1/X^2$.

Un altre exemple: la corba el·lítpica $Y^2 = X(X-1)(X+2)$ té arrels 0, 1 i -2. Aplicant $\tau(X) = X/3 + 2/3$ enviem -2 a 0, 1 a 1 i 0 a 2/3. Aplicant ara

$$\beta(X) = \frac{3^3}{2^2} X^2(1 - X)$$

enviem 0 i 1 a 0 i 2/3 a 1. La composició $\phi(X, Y) = \beta(\tau(X)) = -(1/4)X^3 - (3/4)X^2 + 1$ obtenim una funció de Belyî de grau 6.

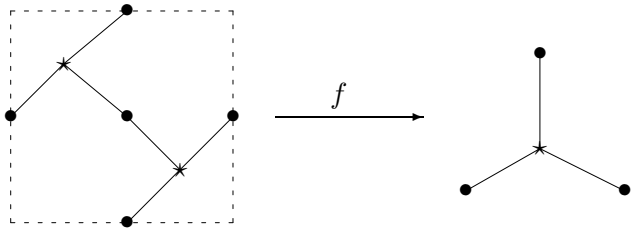
El dibuix associat és



Si les tres arrels no són racionals, podem aplicar el procediment de Belyî per a trobar una funció adequada que les porti a nombres racionals. Per exemple, si prenem $\beta_1(X) = P(X)$, aquesta funció porta ∞ a ∞ i les tres arrels a 0. A més ramifica als zeros de la derivada $P'(X)$, que són dos. Si l'imatge per $P(X)$ d'aquests dos punts fos un punt ja estariem: multiplicant $P(X)$ per l'invers de la imatge d'aquests dos punts, que ha de ser un nombre racional, obtenim la funció de Belyî β que envia aquests dos punts a 1, els altres tres punts a 0 i ∞ a ∞.

Per exemple, si prenem la corba el·líptica $Y^2 = X^3 - 1$, aleshores tenim que les arrels de $P'(X)$ són el zero amb multiplicitat 2, i la seva imatge és -1. Prenem per tant $\beta(X) = X^3 + 1$, i tenim que

$\phi := \beta \circ f$ és una funció de Belyî de grau 6. A nivell de dibuixos obtenim aproximadament



Seguim en la situació general: si les imatges per $P(X)$ de les dos arrels de $P'(X)$ són dos valors diferents α_1 i α_2, prenem $Q(X) = (X/\alpha_1 - 1)(X/\alpha_2 - 1) \in \mathbb{Q}[X]$. Considerem ara $\beta_2(X) := Q(\beta_1(X)) = Q(P(X))$. Aquest polinomi envia les arrels de $P(X)$ a 1 i les arrels de $P'(X)$ a 0, té grau 6 i a més les imatges dels punts de ramificació són racionals. En efecte, els punts de ramificació són els punts tals que $P'(X) = 0$, o sigui punts amb imatge 0, i els punts tals que $P(X) = 1/2(\alpha_1 + \alpha_2) \in \mathbb{Q}$, i per tant amb imatge un nombre racional concret. En resum, la funció $\beta_2 \circ f \colon E \to \mathbb{P}^1$ està ramificada a sobre de 4 punts, el 0, l'1, l'∞ i un punt racional. Podem aplicar aleshores el procediment anterior per a calcular la funció de Belyî.

Observem que amb aquest mètode sempre obtindrem morfismes de Belyî de grau parell, i clarament no tots els morfismes de Belyî en gènere 1 s'obtenen així. Sovint podem obtenir morfismes de Belyî de grau més petit; però no conec cap procediment efectiu per a calcular-los. Tot i així, els graus dels morfismes de Belyî tendeixen a ser grans, encara que els primers dividint el grau del morfisme de Belyî "minimal"estan lligats al conductor, tal com em vist en la secció anterior.

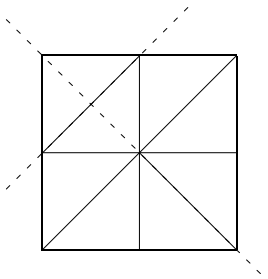
Per exemple, si prenem la corba $Y^2 = (X - 5/9)(X^2 - 15/4X + 15/4)$ (150A3 amb la notació de Cremona), el morfisme que obtenim seguint els passos anteriors té grau 898893610 (que podem simplificar molt utilitzant que tenim una arrel racional). Però la corba té el morfisme de Belyî $\phi(X, Y) = -9/16(XY + (5/9X^2 - 5/2X + 1))$ de grau 5 (comproveu-ho!). El dibuix d'infants associat té una cara de

valència 5, un vèrtex $\bullet$ de valència 5 (el punt $(1, 2/3)$) i tres vèrtexs $\star$, un de valència 3 (el punt $(5/3, -5/9)$) i dos de valència 1 (els punts $(\sqrt{-5/3}, -5/2 - (5/6)\sqrt{-5/3})$). Observeu que el vèrtex $\bullet$ és un punt d'ordre 5 de la corba el·líptica; per què?. Hi ha dos dibuixos amb aquesta llista de valències, i l'altre correspon a la corba 75C1 ("donat"també per un punt d'ordre 5).

2.6.2 Dibuixos en gènere 1

Anem a dir dues paraules sobre com calcular la corba el·líptica i la funció de Belyĭ associades a certs dibuixos en gènere 1. La idea és que els dibuixos obtinguts com a la secció anterior a partir d'un recobriment de grau 2 del pla ramificat en 4 punts han de tenir una involució, i per tant són "fàcils"de reconèixer.

2.6.1 Exemple. Considerem el dibuix net en gènere 1 donat pel dibuix següent:

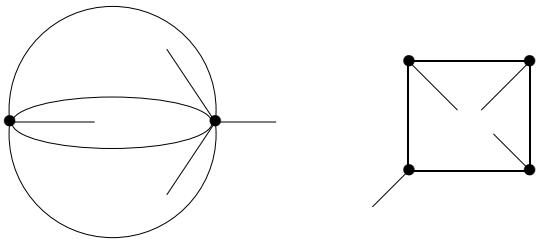


Tenim dos vèrtexs amb valència 7 (el vèrtex i el centre del quadrat) i dos vèrtexs amb valència 5. A part tenim 12 arestes (corresponents a 12 vèrtexs $\star$) i 8 cares amb valència 3.

Aquest dibuix està tractat per Shabat i Voevodsky a [21], tot i que ells no expliquen els càlculs que han fet.

Tenim clarament dos eixos de simetria que ens donen dues involucions s_1 i s_2; però aquestes involucions no preserven l'orientació! Per tant no ens donen una involució de la corba el·lítica. Però $\tau = s_1 \circ s_2$ si que ens dóna una involució preservat l'orientació ja que $\tau^2 = 1$. Els punts fixos per l'involució són els centres dels 4 quadradets (aquests correspondran als punts d'ordre ≤ 2). La involució intercanvia els vèrtexs amb les mateixes valencies.

Al fer quocient respecte l'involució τ obtenim el dibuix prenet al pla següent, juntament amb el seu dibuix dual (intercanviant vèrtexs per cares):



Aquest dibuix podem calcular-li la funció de Belyî fent servir les tècniques explicades a la secció 4. Obtenim:

$$f-1 := \frac{1}{z^5(1397875858735104\alpha + 3698399643697152)}$$
$$[z^4 + 156z^3 + (17150 + 4256\alpha)z^2 + (4452140 + 1690304\alpha)z -$$
$$- 279416375 - 105644000\alpha][z^4 + 48z^3 + (698 + 224\alpha)z^2 +$$
$$(-112000\alpha - 295000)z + 101828125 + 38500000\alpha]^2$$

on $\alpha = \sqrt{7}$. L'he escrit així doncs el que ens interessa més són els zeros simples de $f-1$, ja que ens donen els punts de Weierstrass. Així la corba el·lítica en qüestió que busquem ve donada per l'equació

$$Y^2 = z^4 + 156z^3 + (17150 + 4256\alpha)z^2 + (4452140 + 1690304\alpha)z -$$
$$- 279416375 - 105644000\alpha$$

amb invariant j igual a

$$j := 457208 - 172564\sqrt{7}$$

el que ens confirma que no es pot definir sobre $\mathbb{Q}$. De pas observem que tenim un dibuix "conjugat"donat per la conjugació $\sqrt{7} \to -\sqrt{7}$

Fixeu-vos que per tal que un dibuix en gènere 1 sigui un recobriment de grau 2 d'un dibuix en gènere 0 cal que:

1. Tingui 4 vèrtexs o cares amb valència parell
2. Pel reste de vèrtexs i cares n'hi hagi un nombre parell de cada valència i tipus.

Però amb això no és suficient!

2.6.2 Exemple. Considerem un dibuix en gènere zero tal que té dues cares amb valència 3, dos vèrtexs $\bullet$ amb valència 4 i 2 i dos vèrtexs $\star$ amb valència 4 i 2. Si prenem que els punts de Weierstrass estiguin sobre els vèrtexs obtenim un recobriment de grau 2 del dibuix en el pla amb una cara de valencia 3, dos vèrtexs $\bullet$ amb valència 2 i 1 i dos vèrtexs $\star$ amb valència 2 i 1, i.e.

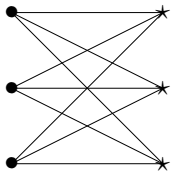
Aquest dibuix ja l'hem estudiat i fent els càlculs obtenim la corba $y^2 = (x^2 - 1)(x^2 - 4)$.

Però tenim un altre dibuix amb les mateixes valències, que no s'obté com un recobriment de grau 2 del pla; és la corba $y^2 = -x^4 - 2x^3 + 3x^2 - 4x + 4$, prenen la funció de Belyî $f(x, y) = (x + 2)y$; té invariant $j = 3^3 7^3/2^3$.

2.6.3 Corbes de Fermat

Un cas molt concret en que podem calcular una funció de Belyî i el dibuix associat per a una corba és el cas de les corbes de Fermat F_n, donades per l'equació afí $X^n + Y^n = 1$ amb $n > 2$. En aquest cas el morfisme $\phi\colon F_n \to \mathbb{P}^1$ definit per $\phi(X, Y) = Y^n$ és un morfisme de Belyî de grau n^2. Els punts de ramificació són els següents: els punts de la forma $(0, \xi)$ i els punts $(\xi, 0)$, on ξ és una arrel enèsima de 1, són punts amb imatge 1 i 0 respectivament, i tots ells tenen índex de ramificació n; i els punts de l'infinit (n'hi ha n, amb coordenades projectives $[\xi : 1 : 0]$), també amb index de ramificació n.

Així el dibuix associat és un dibuix amb n vèrtexs $\bullet$ de valència n i n vèrtexs $\star$ de valència n. Això correspon al graf complet bipartit $K_{n,n}$. Per exemple, per a $n = 3$ tenim un graf que dibuixat al pla (amb interseccions) és



De la mateixa manera podem considerar les corbes $X^n + Y^m = 1$ amb la funció de Belyî Y^m, i obtenim el graf complet bipartit amb n vèrtexs $\bullet$ i m vèrtexs $\star$.

2.6.4 Corbes amb molts automorfismes

Diem que una corba C sobre $\mathbb{C}$ de gènere $g > 1$ és una corba amb molts automorfismes si el punt corresponent en l'espai de moduli M_g de les corbes de gènere g té un entorn (en la topologia complexa) tal que tota corba corresponent a un punt d'aquest entorn té un grup d'automorfismes estrictament menor que la corba C. Per exemple, si $g > 3$ és sabut que aquests punts corresponen a les singularitats aïllades de M_g. Un altre exemple de corbes amb molts automorfismes són les corbes de Fermat F_n.

Anem a veure com podem caracteritzar aquestes corbes utilitzant dibuixos i funcions de Belyî. Aquesta caracterització es deguda a P. Beazley Cohen i J. Wolfart (vegis [1] i, sobretot [34]).

2.6.3 Teorema. *Sigui C una corba sobre $\mathbb{C}$ amb molts automorfismes, i considerem $A := Aut_{\mathbb{C}}(C)$ (és un grup finit doncs $g > 1$). Aleshores $C/A \cong \mathbb{P}^1$ i el morfisme $\phi\colon C \to C/A \cong \mathbb{P}^1$ és un morfisme de Belyî. A més el recobriment donat per ϕ és normal (i per tant l'extensió de cossos corresponent és de Galois).*

Utilitzant ara el teorema de Belyî podem demostrar per tant un resultat que alguns de vosaltres ja coneixereu:

2.6.4 Corol·lari. *Tota corba amb molts automorfismes està definida sobre $\overline{\mathbb{Q}}$, i per tant sobre un cos de nombres.*

De fet, la última afirmació del teorema anterior ens dona una caracterització de les corbes amb molts automorfismes.

2.6.5 Teorema. *Sigui C una corba de gènere > 1 definida sobre $\mathbb{C}$. Aleshores C té molts automorfismes si i només si existeix una funció de Belyî $\phi\colon C \to \mathbb{P}^1$ definint un recobriment normal.*

La idea de demostració és la següent: observem primer que si tenim un recobriment normal aleshores tots els vèrtexs $\bullet$ tenen la mateixa valència p, tots els vèrtexs $\star$ tenen la matèixa valència q i totes les cares tenen la mateixa valència r (o sigui el dibuix es equilibrat).

Considerem el grup triangular $\Delta_{p,q,r}$ i el subgrup normal Γ corresponent a la funció de Belyî (tal com em vist a la subsecció 2.5); ja em vist que Γ aleshores és lliure de torsió i que la funció

$$\mathbb{H} \to \Gamma\backslash\mathbb{H} \cong C(\mathbb{C})$$

és el recobriment universal de $C(\mathbb{C})$. Així el grup Δ/Γ actua a C i és de fet el grup de Galois de la extensió de cossos corresponent. De fet es pot veure que el normalitzador de Γ dins de $\mathrm{PSL}_2(\mathbb{R})$ és un grup triangular (Fuchsià i cocompacte), ja que el normalitzador conté a Δ i és un grup Fuchsià (això caracteritza els grups triangulars). El resultat es dedueix aleshores del següent lema.

2.6.6 Lema. *Una superfície de Riemann té molts automorfismes si i només si el normalitzador del seu grup recobridor universal a dins de $\mathrm{PSL}_2(\mathbb{R})$ és un grup triangular.*

X. Xarles
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
xarles@mat.uab.es

Capítol 3

Càlcul explícit del recobriment associat a un dibuix en gènere 0

Joaquim Roé

Introducció

En aquest capítol ens proposem descriure mètodes que permeten trobar, a partir d'un dibuix d'infants, equacions (sobre un cos de nombres apropiat) d'una corba algebraica C i un morfisme $C \longrightarrow \mathbb{P}^1$, ramificat només en $\{0, 1, \infty\} \subset \mathbb{P}^1$, els quals existeixen gràcies a la part "òbvia" del teorema de Belyĭ. Ens centrarem en dos mètodes, que usen com a eines fonamentals les bases de Gröbner i les sèries de Puiseux respectivament, tal com els exposen Couveignes i Granboulan a [8]. Les bases de Gröbner són útils sobre tot quan el gènere del dibuix és 0, cas en el qual la corba és automàticament $\mathbb{P}^1$ i només cal trobar equacions per al morfisme. Les sèries de Puiseux permeten, en principi, atacar el cas general, però condueixen a un mètode basat en aproximacions i de més complexitat numèrica.

Al llarg de tot el capítol suposarem donat un dibuix d'infants $X_0 \subset X_1 \subset X_2$ (vegeu la definició a 2.1.2) i l'objectiu serà determinar

una corba projectiva llisa $C \subset \mathbb{P}^r_{\mathbb{C}}$ i un morfisme $f : C \longrightarrow \mathbb{P}^1$ ramificat sobre $\{0, 1, \infty\} \subset \mathbb{P}^1$, de manera que hi hagi un homeomorfisme $h : X_2 \longrightarrow C$ preservant la orientació i amb $X_1 = (f \circ h)^{-1}([0, 1])$ i $X_0 = (f \circ h)^{-1}(\{0, 1\})$.

3.1 Bases de Gröbner

En tota aquesta secció suposarem que X_2 és l'esfera, amb la qual cosa la corba C queda determinada essent isomorfa a l'esfera de Riemann $\mathbb{P}^1_{\mathbb{C}}$. Llavors, el morfisme f es pot interpretar com una funció racional $f \in \mathbb{C}(z)$, i el problema que tenim plantejat es redueix a trobar els coeficients (o equivalentment, les arrels) dels polinomis numerador i denominador de f. Dit d'una altra manera, tenim una esfera topològica X_2 i un dibuix d'infants traçat sobre seu; el mètode de la triangulació ens dóna una aplicació contínua sobre l'esfera de Riemann $f : X_2 \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ que és un recobriment topològic fora dels vèrtexs $\bullet$ (els quals tenen imatge 0) i $\star$ (amb imatge 1) i dels centres de les cares del dibuix (amb imatge ∞), i tal que $X_1 = f^{-1}([0, 1])$. El que cal fer és donar a X_2 estructura holomorfa (fixar-hi una coordenada, "z") de manera que f sigui un morfisme entre superfícies de Riemann.

Calculem primerament les valències $V_0 = (u_1, u_2, \cdots, u_r), V_1 = (v_1, v_2, \cdots, v_s), V_\infty = (w_1, w_2, \cdots, w_t)$ associades al dibuix. Per a cada $u_i \neq 0$, anomenem $\alpha_{i,1}, \ldots, \alpha_{i,u_i}$ les coordenades z dels u_i vèrtexs $\bullet$ de valència i, i de forma semblant anomenem $\beta_{i,j}$ i $\gamma_{i,j}$ les coordenades dels vèrtexs $\star$ i dels centres de les cares. Aquestes coordenades són incògnites del problema. Com que f (o z) està determinada només mòdul automorfismes de C, i en aquest cas $C = \mathbb{P}^1_{\mathbb{C}}$, tenim certa llibertat per triar-la de forma "senzilla". Ho farem fixant la posició (la coordenada z) de 3 punts, la qual cosa ens eliminarà tres incògnites. El centre de la cara de valència més gran serà $\gamma_{t,1} = \infty$, i dos vèrtexs del dibuix (que normalment escollirem de valència gran, però es poden seguir altres criteris, segons les simetries del dibuix, per exemple) seran $z = 0, 1$.

Si determinem el valor de les incògnites restants haurem resolt el

problema, ja que llavors

$$f(z) = \frac{\prod_{i,j}(z-\alpha_{i,j})^i}{k\prod_{i,j}(z-\gamma_{i,j})^i},$$

on hem omès el factor $(z-\gamma_{i,j})^i$ corresponent al $\gamma_{t,1}=\infty$ i per tant el grau del numerador supera en t el del denominador, i on $k\in\mathbb{C}$ és tal que

$$\prod_{i,j}(z-\alpha_{i,j})^i - k\prod_{i,j}(z-\gamma_{i,j})^i = \prod_{i,j}(z-\beta_{i,j})^i. \tag{3.1}$$

La igualtat (3.1) de polinomis de $\mathbb{C}[z]$ equival a un sistema d'equacions algebraiques en $k, \alpha_{i,j}, \beta_{i,j}$ i $\gamma_{i,j}$ que, a priori, podria no tenir solució, però que sabem que en té si més no una, la corresponent a la funció de Belyî que estem buscant. A més, qualsevol solució del sistema *on totes les* $\alpha_{i,j}, \beta_{i,j}$ *i* $\gamma_{i,j}$ *siguin diferents* correspon a una funció de Belyî, possiblement amb un dibuix associat diferent però amb les mateixes valències. Com que el nombre de dibuixos d'infants amb les mateixes valències és finit, i per a cada dibuix obtenim com una solució de (3.1) (ja que hem eliminat els automorfismes de $C=\mathbb{P}^1_{\mathbb{C}}$ fixant tres punts) concloem que el nombre de solucions de (3.1) és finit (eliminant valors repetits de les incògnites, vegeu la secció 3.1.3). Així doncs, el que es necessita per calcular explícitament el recobriment associat a un dibuix en gènere zero és un mètode de resolució de sistemes d'equacions algebraiques amb un nombre finit de solucions. Una possibilitat per fer això és l'ús de bases de Gröbner.

3.1.1 Remarca. Tal com hem plantejat el problema, tenim una col·lecció d'incògnites, que són les arrels dels polinomis $P_i(z)=\prod_{j=1}^{u_i}(z-\alpha_{i,j})$, $Q_i(z)=\prod_{j=1}^{v_i}(z-\beta_{i,j})$, $R_i(z)=\prod_{j=1}^{w_i}(z-\gamma_{i,j})$, i unes equacions, equivalents a $\prod_i P_i(z)+\prod_i Q_i(z) = k\prod_i R_i$. El mateix es pot fer usant com a incògnites els *coeficients* dels polinomis; com que aquests són funcions simètriques de les arrels, podem esperar obtenir així equacions de grau més baix.

3.1.2 Remarca. La única informació del dibuix que s'utilitza en aquest mètode és la llista de valències. Això fa que no necessàriament s'obtingui una sola solució, sinó que obtenim equacions per tots els

recobriments associats a dibuixos amb les mateixes valències. Per determinar quina de les solucions obtingudes és la que buscàvem caldrà que sapiguem fer el dibuix associat a un morfisme de Belyî, però això és relativament fàcil de fer (si més no en gènere 0).

3.1.1 Ordres monomials

Fixem k un cos (que per simplicitat suposarem algebraicament tancat, ja que ho volem aplicar a $\mathbb{C}$ o $\bar{\mathbb{Q}}$, malgrat que quasi tot el que diem en aquest apartat no necessita aquesta hipòtesi). Sigui $A = k[\alpha_1, \ldots, \alpha_n]$ l'anell dels polinomis en n variables, i fixem un *ordre total* $\geq$ en el conjunt dels monomis d'A, que satisfaci les propietats següents:

1. Si m_1 i m_2 són monomis amb $m_1 \geq m_2 \geq m_1$ llavors $m_1 = m_2$,
2. si m_1 i m_2 són monomis amb $m_2 | m_1$ llavors $m_1 \geq m_2$, i
3. si m_1 i m_2 són monomis amb $m_1 \geq m_2$ llavors per tot monomi m_3, $m_1 m_3 \geq m_2 m_3$.

3.1.3 Exemple. Un exemple senzill d'ordre monomial que satisfà les propietats anteriors és l'*ordre lexicogràfic*, en el qual $\alpha_1^{a_1} \ldots \alpha_n^{a_n} \geq \alpha_1^{b_1} \ldots \alpha_n^{b_n}$ si per al mínim i tal que $a_i \neq b_i$ (en cas que existeixi) $a_i > b_i$.

3.1.4 Definicions. El *terme inicial* d'un polinomi $P = \sum_m c_m m$ (on m recorre els monomis d'A i $c_m = 0$ quasi per tot m) es defineix com $\mathrm{In}(P) := c_{m_{\max}} m_{\max}$, on $m_{\max} = \max\{m | c_m \neq 0\}$. Així mateix definim l'*ideal inicial* d'un ideal $I \subset A$ com aquell generat pels termes inicials dels polinomis de I: $\mathrm{In}(I) := (\mathrm{In}\, P)_{P \in I}$.

3.1.5 Remarca. Anomenem $B = k[\alpha_{m-r+1}, \ldots, \alpha_n] \subset A$ el subanell dels polinomis en les r últimes variables. Llavors, usant l'ordre lexicogràfic, es té

$$\mathrm{In}(P) \in B \Longrightarrow P \in B. \tag{3.2}$$

Aquesta propietat (que és compartida per altres ordres i no només pel lexicogràfic) ens serà d'utilitat més endavant.

Des del punt de vista computacional, els ideals generats per monomis (com els $\mathrm{In}(I)$ que acabem de definir) són relativament "senzills", en el sentit que és fàcil decidir si un polinomi determinat hi pertany o no, o si dos ideals són iguals, fer càlculs de sumes i interseccions, etc. D'altra banda, l'ideal inicial d'un ideal I donat conté abundant informació sobre I, i pel que acabem de dir aquesta informació és (computacionalment) més fàcil de llegir en $\mathrm{In}(I)$ que no pas directament en I. Com a exemple il·lustratiu tenim el resultat següent:

3.1.6 Lema. *Siguin $I \subset J \subset A$ dos ideals amb $\mathrm{In}(I) = \mathrm{In}(J)$. Llavors $I = J$.*

Demostració: Observem primer que qualsevol conjunt de monomis M d'A té mínim. Efectivament, l'ideal (M) està generat per un subconjunt finit $\{m_1, \ldots, m_r\}$ perquè A és noetherià, i llavors $\min\{m_1, \ldots, m_r\} \leq m \, \forall m \in M$ per la propietat 2 de l'ordre $\geq$ i perquè tot element de M és un múltiple, per un monomi, d'un dels m_i.

Suposem ara que $I \neq J$, i siguin m el mínim dels monomis inicials de polinomis $P \in J \setminus I$, i $P_m \in J \setminus I$ amb $\mathrm{In}(P_m) = m$. Llavors, $m \in \mathrm{In}(J) = \mathrm{In}(I)$, per tant existeix $Q \in I$ amb $\mathrm{In}(Q) = m$. Això implica que $P - Q \in J \setminus I$, i $\mathrm{In}(P - Q) < m$, en contradicció amb l'elecció de m. □

3.1.7 Definició Una *base de Gröbner* d'un ideal I (respecte de l'ordre $\geq$) és un sistema de generadors $\{P_1, \ldots, P_r\}$ de I tals que

$$(\mathrm{In}(P_1), \ldots, \mathrm{In}(P_r)) = \mathrm{In}(I).$$

3.1.8 Remarca. Hi ha un algorisme "senzill" (algorisme de Buchberger, [10, Cap. 15]) per saber si un sistema de generadors és base de Gröbner i, si no ho és, completar-lo a un que ho sigui.

3.1.2 Resolució de sistemes d'equacions algebraiques

Vegem ara com les bases de Gröbner ens permeten resoldre sistemes d'equacions amb un nombre finit de solucions. Suposem que tenim un ideal $I = (P_1, \ldots, P_r) \subset A$ amb $\dim_k A/I$ finit (això és equivalent a

què el sistema $P_1 = \cdots = P_r = 0$ tingui un nombre finit de solucions). Vegem, per recurrència en el nombre de variables n de A, com trobar les solucions.

Si $n = 1$, és a dir $A = k[\alpha]$, llavors $I = (P)$ és principal i les solucions del sistema són les arrels del polinomi P. Suposem doncs que $n > 1$, $A = k[\alpha_1, \ldots, \alpha_n]$ i definim $B = k[\alpha_n] \subset A$. Observem que $I \cap B \neq 0$, ja que $\dim_k B = \infty$ i $\dim_k A/I < \infty$; per tant $I \cap B = (P)$ amb $P \neq 0$ un polinomi en la variable α_n. Suposem que coneixem el polinomi P. Llavors, com que $P \in I$, P ha de valdre zero sobre totes les solucions del sistema $P_1 = \cdots = P_r = 0$, és a dir, en tota solució $(\alpha_1, \ldots, \alpha_n)$ del sistema, α_n ha de ser arrel de P. (Geomètricament, les arrels de P són les projeccions sobre l'eix de la coordenada α_n dels punts solució del sistema). Siguin doncs $a_1, \ldots, a_d \in k$ les arrels de P. Substituint cadascun d'aquests valors en els polinomis $P_1, \ldots, P_r$ obtenim d nous sistemes d'equacions en una variable menys (possiblement amb els coeficients en un cos més gran), que resoldrem eliminant successivament les variables. La col·lecció de totes les solucions que obtenim ens dóna la solució al sistema original.

Vegem, per acabar, com les bases de Gröbner ens permeten calcular efectivament $I \cap B$ i per tant trobar el polinomi P, que com hem vist és l'únic que ens cal per resoldre el problema.

3.1.9 Proposició. *Sigui $\geq$ un ordre monomial que satisfà (3.2), sigui $I \subset A$ un ideal i sigui $\{P_1, \ldots, P_r\}$ una base de Gröbner de I. Llavors $\{P_1, \ldots, P_r\} \cap B$ és una base de Gröbner de $I \cap B$.*

Demostració: Ordenem els elements de la base de Gröbner de manera que $\{P_1, \ldots, P_\ell\} = \{P_1, \ldots, P_r\} \cap B$, i posem $J = (P_1, \ldots, P_\ell) \subset B$. La inclusió $J \subset I \cap B$ és clara, i per tant 3.1.6 ens diu que serà suficient demostrar la igualtat $\mathrm{In}(J) = \mathrm{In}(I \cap B)$, o simplement que $\mathrm{In}(I \cap B) \subset (\mathrm{In}(P_1), \ldots, \mathrm{In}(P_\ell))$.

Sigui doncs $m \in \mathrm{In}(I \cap B)$ un monomi; com que $m \in \mathrm{In}(I) = (\mathrm{In}(P_1), \ldots, \mathrm{In}(P_r))$, un dels $\mathrm{In}(P_i)$ divideix m, diguem-li $\mathrm{In}(P_{i_m})$. Com que $m \in B$, $\mathrm{In}(P_{i_m}) \in B$, i per la propietat (3.2) de l'ordre que estem usant, $P_{i_m} \in B$, és a dir, $i_m \leq \ell$ i $m \in (\mathrm{In}(P_1), \ldots, \mathrm{In}(P_\ell))$ tal com volíem demostrar. □

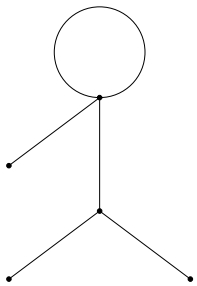


Figura 3.1: Dibuix net de l'exemple 3.1.3.

3.1.3 Exemples

Considerem el dibuix net de la figura 3.1. Les seves valències són $V_0 = (3,0,1,1)$, $V_1 = (0,5)$ i $V_\infty = (1,0,0,0,0,0,0,0,0,1)$, i correspon a un morfisme $f : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ de grau 10. Donant nom a les incògnites com hem fet abans, podem expressar-lo, en certes coordenades, com

$$f(z) = \frac{(z-\alpha_{1,1})(z-\alpha_{1,2})(z-\alpha_{1,3})(z-\alpha_3)^3(z-\alpha_4)^4}{k(z-\gamma)},$$

i se satisfarà l'equació

$$\begin{aligned}(z-\alpha_{1,1})(z-\alpha_{1,2})(z-\alpha_{1,3})(z-\alpha_3)^3(z-\alpha_4)^4 - k(z-\gamma) = \\ = (z-\beta_1)^2(z-\beta_2)^2(z-\beta_3)^2(z-\beta_3)^2(z-\beta_4)^2(z-\beta_5)^2. \quad (3.3)\end{aligned}$$

Podem triar dos valors per a les incògnites; l'opció més raonable és "eliminar" les que apareixen amb grau més alt, fent $\alpha_4 = 0$ i $\alpha_3 = 1$. Igualment, podem simplificar les equacions a resoldre usant les funcions simètriques en les incògnites com a noves incògnites, com hem indicat a la remarca 3.1.1. Així doncs, escrivim

$$\begin{gathered}(z-\alpha_{1,1})(z-\alpha_{1,2})(z-\alpha_{1,3}) = z^3 + a_2z^2 + a_1z + a_0, \\ (z-\beta_1)(z-\beta_2)(z-\beta_3)(z-\beta_3)(z-\beta_4)(z-\beta_5) = \\ = z^5 + b_4z^4 + b_3z^3 + b_2z^2 + b_1z + b_0.\end{gathered}$$

D'aquesta manera les equacions deduïdes de (3.3) igualant terme a

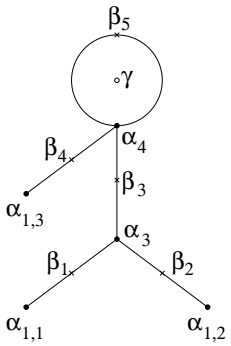


Figura 3.2: Dibuix de l'exemple 3.1.3, amb noms per les incògnites.

terme que han de satisfer les noves incògnites són:

$$\gamma k = b_0^2, \tag{3.4}$$
$$k = -2b_0b_1, \tag{3.5}$$
$$0 = b_1^2 + 2b_0b_2, \tag{3.6}$$
$$0 = b_1b_2 + b_0b_3, \tag{3.7}$$
$$a_0 = -(b_2^2 + 2(b_1b_3 + b_0b_4)), \tag{3.8}$$
$$a_1 = 3a_0 - 2(b_0 + b_2b_3 + b_1b_4), \tag{3.9}$$
$$a_2 = 3(a_1 - a_0) - 2(b_1 + b_2b_4) - b_3^2, \tag{3.10}$$
$$a_0 = 2b_2 + 3(a_1 - a_2) + 2b_3b_4 + 1, \tag{3.11}$$
$$a_1 = 2b_3 + 3(a_2 - 1) + b_4^2, \tag{3.12}$$
$$a_2 = 2b_4 + 3. \tag{3.13}$$

Eliminant les variables que hem aïllat en (3.5) i (3.11)–(3.13) obtenim el sistema de sis equacions format per (3.6, 3.7) i les següents:

$$0 = b_0(b_0 + 2b_1\gamma), \tag{3.14}$$
$$0 = (b_2 + 1)^2 + 6b_3 + 2b_1b_3 + 2b_0b_4 + 2b_3b_4 + 3(b_4 + 2)^2 - 3, \tag{3.15}$$
$$0 = (b_3 - 3)(8 - b_2 + 3b_4) - b_0 - b_1b_4 + 4(b_4 + 3)^2, \tag{3.16}$$
$$0 = 15 + 2b_1 + 6b_2 + 12b_3 + b_3^2 + 20b_4 + 2b_2b_4 + 6b_3b_4 + 6b_4^2. \tag{3.17}$$

La primera d'aquestes, 3.14, ens dóna dues opcions: o bé $b_0 = 0$ (però llavors $\beta_i = \alpha_4 = 0$, cas que podem descartar perquè tindríem dos vèrtexs coïncidents) o bé podem aïllar $\gamma = -b_0/2b_1$. Finalment

obtenim un sistema de cinc equacions amb cinc incògnites donades per l'anul·lació dels polinomis de (3.6), (3.7) i (3.15)–(3.17). Calculem (amb el programa SINGULAR) una base de Gröbner per l'ideal que generen aquests polinomis; per fer això hem d'escollir primer un ordre. Triem l'ordre lexicogràfic amb $b_4 > b_3 > b_2 > b_1 > b_0$, per tal d'eliminar la variable b_0. Obtenim un sistema de quinze generadors, dels quals un depèn només de b_0:

$$28588707\, b_0^5 - 3503088\, b_0^4 - 255744\, b_0^3 - 4096\, b_0^2.$$

Tot i ser de grau cinc, com que aquest polinomi té l'arrel zero amb multiplicitat 2 (i sabem que $b_0 \neq 0$), podem deduir que el valor de b_0 que busquem és una de les altres tres arrels. Això no és sorprenent, ja que hi ha dos dibuixos diferents del nostre amb les mateixes valències, i per tant podem esperar obtenir tres solucions diferents al nostre sistema. Mirant la figura ja intuïm que l'arrel real correspondrà al dibuix simètric, mentre que les dues arrels conjugades correspondran als dos dibuixos conjugats, un d'ells el nostre.

Substituint en les cinc equacions cadascun dels tres valors obtinguts, tornaríem a calcular la base de Gröbner amb les quatre coordenades restants, *eliminant a cada pas les possibles solucions que comportessin vèrtexs coincidents*, i així fins determinar completament els tres dibuixos.

3.2 Sèries de Puiseux

El segon mètode que il·lustrarem, basat en l'ús de sèries de Puiseux, té tres avantatges sobre l'anterior: utilitza tota la informació que inclou el dibuix (i no només les valències), les equacions a resoldre són lineals en lloc d'algebraiques, i finalment és (potencialment) aplicable en gènere $g > 0$. Cal mencionar, però, certs inconvenients: només ens dóna solucions aproximades, que cal després convertir en solucions algebraiques exactes, i pot ser numèricament més costós que l'anterior.

Com ja hem fet a l'apartat anterior, partim de l'aplicació contínua $X_2 \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ determinada pel dibuix, que restringida al complementari del conjunt de vèrtexs és un recobriment topològic $X_2 \setminus X_0 \longrightarrow \mathbb{P}^1_{\mathbb{C}} \setminus$

$\{0, 1, \infty\}$, i pretenem explicitar l'estructura holomorfa de X_2 que fa d'aquesta aplicació contínua un morfisme de superfícies de Riemann.

La idea al darrere del mètode ens porta, en cert sentit, a l'origen històric de la noció de superfície de Riemann, que s'introduí com a eina per comprendre les 'funcions multivaluades'. De fet, el problema de trobar una superfície de Riemann (compacta, connexa) i un morfisme f sobre l'esfera de Riemann és equivalent a trobar una funció multivaluada, i en mirar-ho així les condicions imposades pel dibuix d'infants es tradueixen en condicions sobre la ramificació d'aquesta funció multivaluada. En el cas de gènere zero podem pensar que la funció multivaluada que busquem és la inversa $f^{-1} : \mathbb{P}^1 \longrightarrow C$ que ens dóna la coordenada z de $C = \mathbb{P}^1_{\mathbb{C}}$; en el cas de gènere $g > 0$ necessitaríem de fet un sistema lineal de funcions multivaluades per donar la immersió de la superfície de Riemann dins un espai projectiu adequat.

El fet que C sigui una superfície compacta dóna limitacions molt fortes sobre les funcions multivaluades que li associem; de fet en resulta que localment tenen un desenvolupament en *sèrie de Puiseux*.

3.2.1 Definicions. Una sèrie de potències amb exponents fraccionaris és una expressió $\sum_{i \geq i_0} a_i t^{i/n}$, on $a_i \in \mathbb{C}$, i i_0, n són enters fixats amb $n > 0$. Si $i_0 \geq 0$, diem que és una sèrie de Puiseux. Per simplicitat, suposarem que $\gcd(n, \{i | a_i \neq 0\}) = 1$; llavors n s'anomena ordre de polidromia de la sèrie. Les sèries de potències amb exponents fraccionaris (de tots els ordres de polidromia) formen un cos, que denominem $\mathbb{C}\langle\langle x \rangle\rangle$.

Certes sèries amb exponents fraccionaris foren estudiades i utilitzades ja per Newton, tot i que no és clar que fos conscient de la importància que els exponents tinguin un denominador comú. Aquest fet va ser posat de relleu per Victor Puiseux (1820-1883), a la mateixa època que Riemann introduí a la seva tesi les superfícies que ara en porten el nom.

3.2.2 Teorema. (Puiseux) *Sigui $f(x, z) \in \mathbb{C}[[x, z]]$ una sèrie en dues variables. Llavors existeix una descomposició única*

$$f(x, z) = x^r u(x, z) \prod (z - s_i(x)),$$

on $s_1(x), \ldots, s_k(x)$ *són sèries de Puiseux,* $r \geq 0$ *és un enter, i* $u(x,z) \in \mathbb{C}[[x,z]]$ *una sèrie invertible. A més, si* f *és convergent, llavors les sèries* s_i *són també convergents.*

Una demostració en llenguatge modern d'aquest teorema la podeu trobar a [5, Cap. 1]. Observem que una possible interpretació del teorema de Puiseux és que el cos $\mathbb{C}\langle\langle x\rangle\rangle$ és una clausura algebraica del cos $\mathbb{C}((x))$ de les sèries de Laurent. Efectivament, usant el teorema de preparació de Weierstrass es pot veure que el teorema de Puiseux és equivalent a l'enunciat $\mathbb{C}\langle\langle x\rangle\rangle = \overline{\mathbb{C}((x))}$.

En el cas que ens interessa, tenim $x = f(z)$, on f és una funció meromorfa; a l'entorn d'un vèrtex $\alpha_{i,j}$ (amb imatge 0) podem expressar-la com una sèrie de potències $f(z) = \sum_{k \geq i} a_k (z - \alpha_{i,j})^k$ (amb $a_i \neq 0$ perquè $\alpha_{i,j}$ és un vèrtex $\bullet$ de valència exactament i).

El teorema de Puiseux ens diu que

$$x - f(z) = \prod_{\mathbf{i}=0}^{i-1} (z - s_{i,j,\mathbf{i}}(x)),$$

on les $s_{i,j,\mathbf{i}}$ són sèries de Puiseux amb ordre de polidromia exactament i. A més són sèries conjugades, més concretament, $s_{i,j,\mathbf{i}}(x) = s_{i,j,0}(\zeta^{\mathbf{i}} x)$, amb ζ una arrel i-èsima primitiva de la unitat, i amb $s_{i,j,\mathbf{i}}(0) = \alpha_{i,j}$ el vèrtex de partida. En conseqüència, per tot $x = f(z)$ es té que $z = s_{i,j,\mathbf{i}}(x)$ per algun $\mathbf{i}$, és a dir, les sèries de Puiseux $s_{i,j,\mathbf{i}}$ ens dónen les i determinacions de la funció inversa de f.

Les sèries de Puiseux $s_{i,j,\mathbf{i}}$ tenen radi de convergència 1, i les imatges del segment $(0,1)$ per $s_{i,j,\mathbf{i}}$ són les i arestes que troben el vèrtex $\alpha_{i,j}$.

De manera anàloga sabem que hi ha sèries de Puiseux que ens descriuen la inversa de f a l'entorn de tots els vèrtexs ($\bullet$, $\star$ i $\circ$). Per a cada aresta de la triangulació existeixen, doncs, dues sèries (centrades a cadascun dels dos extrems) descrivint la inversa de la funció f restringida a un entorn de l'aresta. Com que aquesta inversa està únicament determinada, se'n dedueix que les sèries de Puiseux hi han de coïncidir: d'aquí n'obtindrem relacions (equacions lineals) entre els coeficients de les sèries.

Amb aquest mètode, doncs, les incògnites a trobar són els (in-

finits) coeficients de les sèries de Puiseux, i les (infinites) equacions es dedueixen de la coincidència de les funcions sobre les arestes. Per fer-lo efectiu es treballa amb truncacions de les sèries i de les equacions, per les quals s'obtenen solucions aproximades. Llavors, mitjançant mètodes estàndard com l'algorisme [19], es converteixen aquestes aproximacions en solucions exactes. Sempre és possible comprovar que el morfisme obtingut és de Belyĭ, i en cas contrari augmentar la precisió de l'aproximació escollida fins obtenir el resultat buscat.

J. Roé
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
jroe@mat.uab.es

Capítol 4

Dessins d'enfants en gènere 1

Teresa Crespo

Estudiem el cas dels dibuixos de gènere 1, seguint l'article de Leonardo Zapponi [36]. L'objectiu és trobar explícitament un parell de Belyĭ associat a un dibuix donat i veure quines propietats aritmètiques de la corba el·líptica corresponent poden veure's en el dibuix. Zapponi considera dues famílies de dibuixos.

Recordem del capítol 2 que podem considerar els dibuixos prenets com a dibuixos amb vèrtexs només de tipus $\bullet$ i afegir un vèrtex $\star$ al mig de cada aresta per obtenir un dibuix net.

Recordem també que les valències donen particions de $N =$ nombre d'arestes i la notació

$V_0 = [1]^{n_1}[2]^{n_2}\cdots[k]^{n_k}$, on n_i és el nombre de vèrtexs $\bullet$ de valència i,

$V_\infty = [1]^{m_1}[2]^{m_2}\cdots[k]^{m_k}$, on m_i és el nombre de cares de valència i.

4.1 Primera família de dibuixos

4.1.1 Descripció

Per a cada $N > 1$, definim $\mathcal{F}_N$ com la família de dibuixos nets amb $2N$ arestes induint les particions

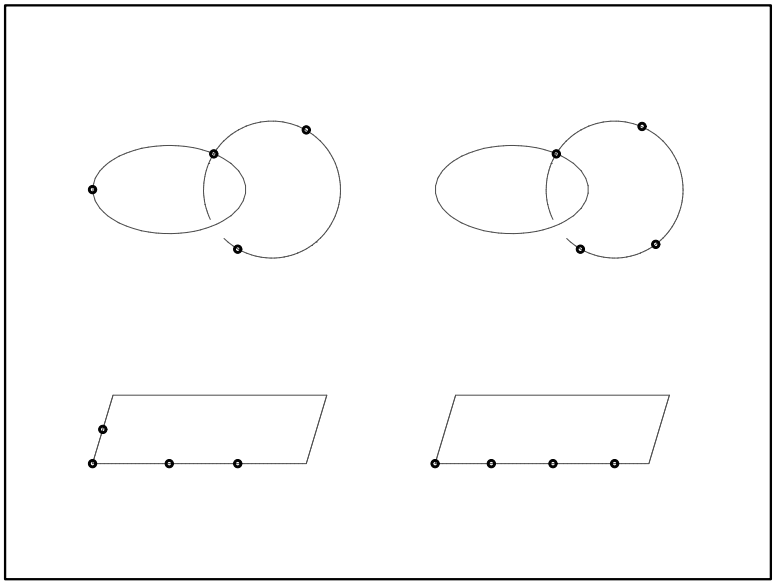
$$V_0 = [2]^{N-2}[4]^1 \text{ i } V_\infty = [2N]^1$$

A partir de la fòrmula d'Euler, tenim que tots aquests dibuixos tenen gènere 1.

Tenim una bijecció

$$\begin{array}{ccc} \{1, 2, \cdots [\frac{N}{2}]\} & \longleftrightarrow & \mathcal{F}_N \\ k & \mapsto & D_k, \text{dibuix amb k vèrtexs} \\ & & \text{en un dels bucles} \end{array}$$

Com a exemple, dibuixem a continuació els dos elements D_2 i D_1 de $\mathcal{F}_5$, indicant els vèrtexs en els dos bucles i en els costats del paral·lelogram fonamental corresponent al tor.



Per descriure el grup cartogràfic de $D_k \in \mathcal{F}_N$, numerem les arestes en la forma següent. Numerem de 1 a k les arestes $\bullet - \star$ del bucle amb k vèrtexs començant pel vèrtex de valència 4, numerem de $k+1$ a N les arestes $\bullet - \star$ de l'altre bucle començant pel vèrtex de valència 4, a continuació, numerem de $N+1$ a $N+k$ les arestes $\star - \bullet$ del bucle amb k vèrtexs acabant en el vèrtex de valència 4 i de $N+k+1$ a $2N$ les arestes $\star - \bullet$ de l'altre bucle acabant en el vèrtex de valència 4.

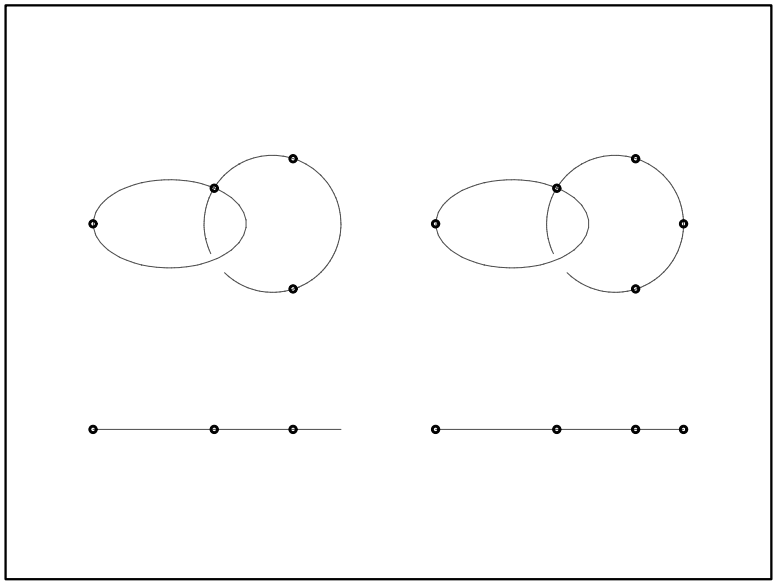
Tenim:

$$\sigma_1 = (1, N+k)(2, N+k-1)\cdots(k, N+1)(k+1, 2N)\cdots(N, N+k+1)$$
$$\sigma_\infty = (1\,,\,2\,,\,3\cdots,\,2N)$$

i σ_0 queda determinat per $\sigma_0 = (\sigma_1\sigma_\infty)^{-1}$. En particular tenim una involució ϕ donada per

$$\phi = (1\,,\,N+1)(2\,,\,N+2)\cdots(k\,,\,N+k)\cdots(N\,,\,2N)$$

que té quatre punts fixos i correspon a l'involució canònica de la corba el·líptica corresponent. El dibuix quocient depen només de N i no de k. Il·lustrem a continuació els casos $N = 5$ i $N = 6$.



Recordem (vegeu 2.3.3) que un parell de Belyĭ corresponent a un dibuix amb N vèrtexs del tipus $\bullet - \star - \cdots - \bullet$ (N senar) o $\bullet - \star - \cdots - \bullet - \star$ (N parell) és $(\mathbb{P}^1, T_N)$, on T_N és el polinomi de Txebixev definit per

$$T_N(\cos\theta) = \cos(N\theta).$$

Considerem ara $D_k \in \mathcal{F}_N$ i posem $\lambda_k = \Re(e^{\pi i \frac{k}{N}}) = \cos(\pi\frac{k}{N})$. Com que $0 < k \leq \dfrac{n}{2}$, tenim $0 \leq \lambda_k < 1$. Considerem la corba el·líptica

$$C_k : Y^2 = (X^2 - 1)(X - \lambda_k)$$

i $\pi(X, Y) = X$ el seu recobriment canònic. Sigui $f_k = (-1)^k T_N \pi$.

4.1.1 Proposició. *El parell (C_k, f_k) és de Belyĭ i el seu dibuix corresponent és D_k.*

Prova. Tenim π ramificat en $1, -1, \lambda_k, \infty$. Ara $\lambda_k = \cos(\pi\dfrac{k}{N}) \Rightarrow T_N(\lambda_k) = \cos(\pi k) = (-1)^k$ i els graus de ramificació de f_k en $1, -1, \infty$ són $2, 4, 2N$. □

4.1.2 Acció del grup de Galois

El grup $\mathbf{\Gamma} = \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ opera de manera natural sobre els parells de Belyĭ en la forma $(C, f) \to (C^\sigma, f^\sigma)$. Pels dibuixos de $\mathcal{F}_N$, tenim

4.1.2 Proposició. *La família $\mathcal{F}_N$ descompon en $d(N) - 1$ òrbites per l'acció de $\mathbf{\Gamma}$, on $d(N)$ indica el nombre de divisors de N. Sigui $D \in \mathcal{F}_N$ i posem $c(D) = \dfrac{n}{(k, N)}$ on k és el nombre d'arestes en un dels bucles (observem $(k, N) = (N - k, N)$). Aleshores $c(D)$ és un invariant galoisià absolut, és a dir, D i D' són conjugats si i només si $c(D) = c(D')$. A més, si j és l'invariant j de la corba associada a D, aleshores $\mathbb{Q}(j)|\mathbb{Q}$ és una extensió abeliana de grau $\dfrac{1}{2}\varphi(c(D))$, on φ indica la funció d'Euler.*

Prova. En el model (C_k, f_k), el recobriment f_k està definit sobre $\mathbb{Q}$. Per tant l'acció de $\mathbf{\Gamma}$ es redueix a l'acció sobre la corba, és a dir sobre λ_k. Sigui $\mathbb{Q}_{N,k} = \mathbb{Q}(\lambda_k) \subset \mathbb{Q}(\zeta_{2N})$. Tenim

$$\begin{array}{rcl} \lambda_k, \lambda_h \text{ conjugats} & \Leftrightarrow & \exists \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{2N})|\mathbb{Q}) \text{ amb } \sigma(e^{i\pi\frac{k}{N}}) = e^{i\pi\frac{h}{N}} \\ & \Leftrightarrow & (k,N) = (h,N) \\ & \Leftrightarrow & c(D_k) = c(D_h) \end{array}$$

Per tant $\mathcal{F}_N$ descompon en $d(N) - 1$ òrbites per l'acció de $\mathbf{\Gamma}$ (ja que no pot ser $c(D) = 1$). Per a la corba C_k, tenim

$$j = 32\frac{(7 + \cos(2\pi\frac{k}{N}))^3}{(1 - \cos(2\pi\frac{k}{N}))^2}.$$

Si $D \in \mathcal{F}_N$, $\mathbb{Q}(j) \subset \mathbb{Q}(\zeta_{c(D)})$. A més l'automorfisme $\sigma : \zeta_{c(D)} \mapsto \zeta_{c(D)}^{-1}$ és l'únic que fixa j. En deduim que $\mathbb{Q}(j)|\mathbb{Q}$ és galoisiana, amb grup de Galois $(\mathbb{Z}/c(D)\mathbb{Z})^*/\{\pm 1\}$. En particular $[\mathbb{Q}(j) : \mathbb{Q}] = \frac{1}{2}\varphi(c(D))$ si $c(D) \neq 2$. En el cas $c(D) = 2$, j és racional. □

A partir de la proposició anterior, tenim j racional $\Leftrightarrow$ $c(D) \in \{2, 3, 4, 6\}$ i els corresponents valors de j són

$$\begin{array}{ll} c(D) = 2 & j = 1728 \quad \text{(en aquest cas } k = \frac{N}{2}\text{)} \\ c(D) = 3 & j = \frac{35152}{9} \\ c(D) = 4 & j = 10976 \\ c(D) = 6 & j = 54000 \end{array}$$

4.1.3 Exemples

N=5.

En aquest cas, tenim $\mathcal{F}_5 = \{D_1, D_2\}$ i $d(5) - 1 = 1$. Per tant els dos dibuixos són conjugats. L'invariant j corresponent a D_1 és $j = \frac{71224 + 26664\sqrt{5}}{5}$ i l'invariant j corresponent a D_2 és $j = \frac{71224 - 26664\sqrt{5}}{5}$.

N=10.

En aquest cas, tenim $\sharp\mathcal{F}_{10} = 5$ i $d(10) = 4$. Pel dibuix D_5 tenim $c(D) = 2$ i $j = 1728$. Per $c(D) = 5$, trobem $\frac{1}{2}\varphi(5) = 2$ dibuixos conjugats, D_2 i D_4. Les corbes corresponents són les mateixes que per a $N = 5$. Per a $c(D) = 10$, tenim els dibuixos D_1 i D_3 i els invariants de les corbes corresponents són $j = 211688 \pm 92168\sqrt{5}$.

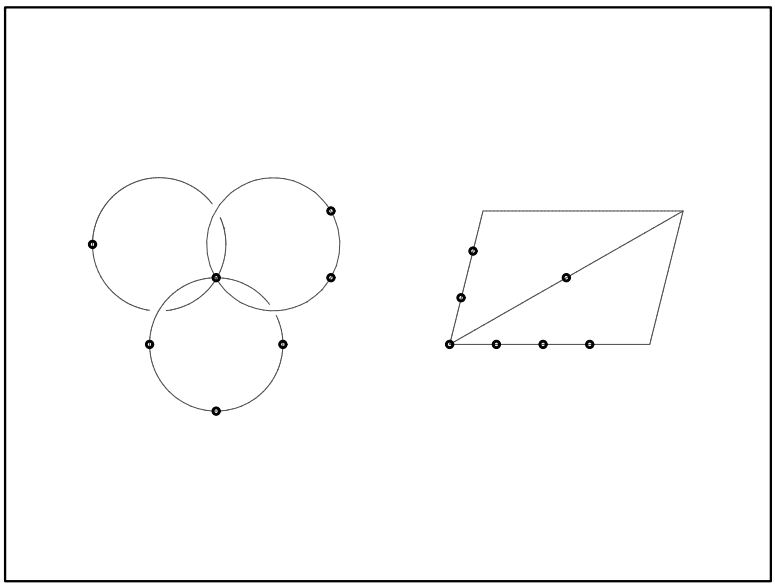
4.2 Segona família de dibuixos

4.2.1 Descripció

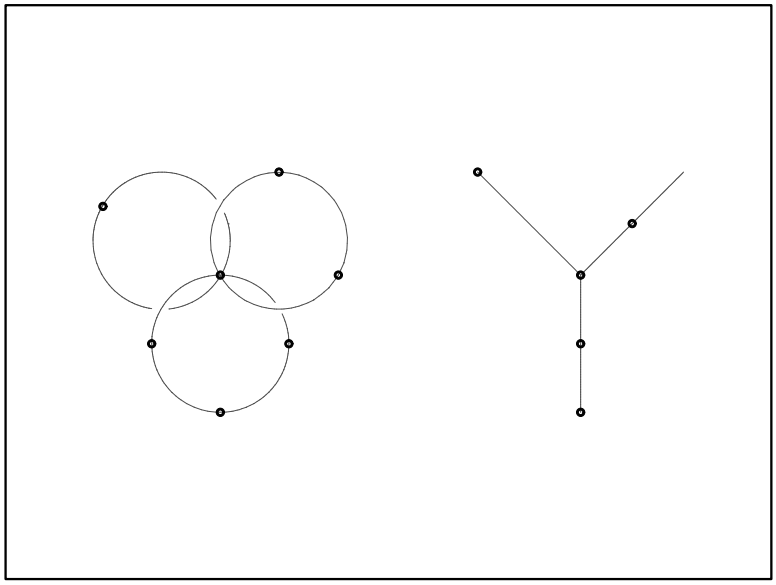
La família $\mathcal{E}_N$ està formada per dibuixos nets amb $2N$ arestes induint les particions

$$V_0 = [2]^{N-3}[6]^1 \quad \text{i} \quad V_\infty = [N]^2.$$

Dibuixem un exemple amb $N = 9$.



Tots aquests dibuixos tenen una involució amb quatre punts fixos que permuta les dues cares. Podem ordenar cíclicament el nombre de vèrtexs a cada bucle al voltant del vèrtex de valència 6. Aleshores $D \in \mathcal{E}_N$ queda determinat per (N_1, N_2, N_3) tripleta d'enters positius amb $N_1 + N_2 + N_3 = N$, mòdul permutació cíclica. Podem fer un estudi de $\mathcal{E}_N$ amb els mètodes utilitzats per a $\mathcal{F}_N$. L'involució σ fixa el vèrtex de valència 6 i, a més, fixa el vèrtex central del bucle i si N_i és parell i l'aresta central si N_i és senar. El quocient dóna un arbre amb un vèrtex de valència 3 (dibuix pre-net).

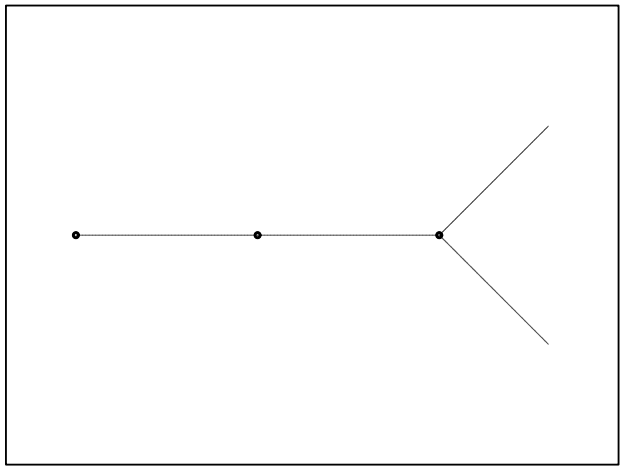


Els parells de Belyĭ associats a aquests arbres són del tipus $(\mathbb{P}^1, P_N)$, on P_N és un polinomi de Shabat, o de Txebixev generalitzat, i.e. amb dos punts crítics sobre $\mathbb{C}$. Suposant P_N determinat, considerem els punts e_1, e_2, e_3 corresponent als "extrems"de l'arbre i e el vèrtex de valència 3. Sigui C la corba el·líptica

$$C : Y^2 = (X - e)(X - e_1)(X - e_2)(X - e_3)$$

i $\pi(X, Y) = X$. Aleshores $(C, P_N\pi)$ és un parell de Belyĭ asociat a D_{N_1,N_2,N_3}. Però obtenir els polinomis de Shabat no és simple i en

general no estàn definits sobre $\mathbb{Q}$. Per exemple, el corresponent a l'arbre que dibuixem a continuació no ho està (veure [22]).



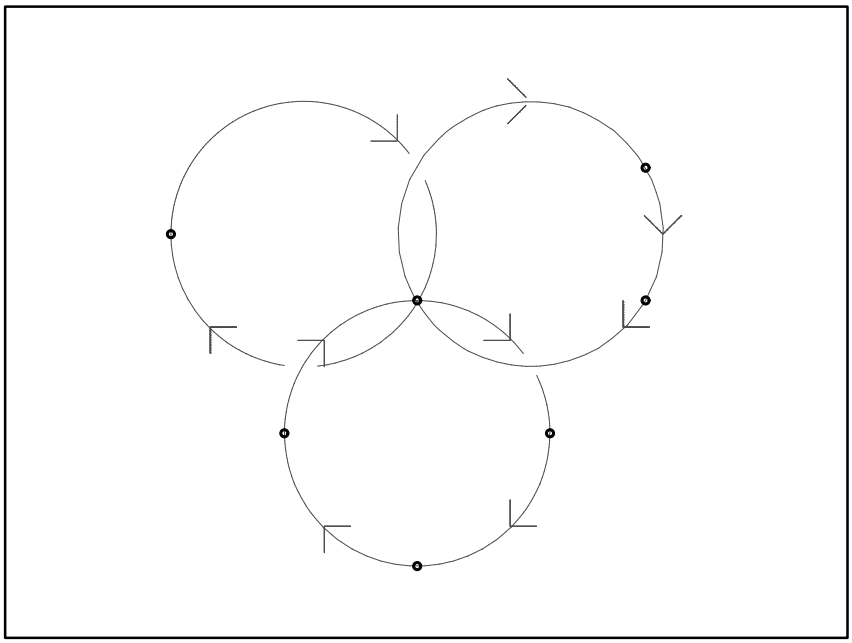
Per tant farem servir un altre mètode per a $\mathcal{E}_N$.

4.2.2 Dibuixos orientables

Un dibuix orientat és un dibuix on les arestes estàn orientades de forma admissible (i.e. les arestes d'una mateixa cara estàn orientades coherentment). Si existeix orientació, és única tret del signe. Un dibuix és orientable si admet una orientació admissible.

Zapponi dóna un criteri d'orientabilitat a partir del grup cartogràfic. D'aquest criteri es dedueix que, si D és orientable i (C, β) és parell de Belyĭ associat a D, aleshores β factoritza en la forma $\beta = \frac{1}{2}(\beta_0 + \frac{1}{\beta_0})$. Aquesta és la propietat que usarem dels dibuixos orientables. De fet, recentment, Zapponi ha provat que és equivalent a l'orientabilitat del dibuix.

Els dibuixos de $\mathcal{E}_N$ són orientables, en el dibuix mostrem una de les dues orientacions possibles.



4.2.3 Un invariant galoisià

Quan associem a un dibuix de la família $\mathcal{E}_N$ un parell de Belyĭ (C, β), suposarem sempre que el vèrtex de valència 6 correspon a l'element neutre de la corba C.

4.2.1 Proposició. *Sigui $D \in \mathcal{E}_N$ i (C, β) un parell de Belyĭ corresponent a D. Aleshores els dos pols de β són punts de torsió de C oposats i el seu ordre n_D divideix $2N$.*

Prova. Com que $D \in \mathcal{E}_N$ és orientable, tenim $\beta = p \circ \beta_0$ on $p(z) = \frac{1}{2}(z + \frac{1}{z})$. El divisor de β_0 és $N[P^+] - N[P^-]$ on P^+ i P^- són els dos pols de β. Per [16] ,9.2.5, tenim $N.P^+ - N.P^- = 0$ sobre C.

L'involució del dibuix permuta les cares i per tant fixa el vèrtex de valència 6 (que correspon al neutre de C). Per tant $\sigma(P) = -P \Rightarrow P^+ = -P^- \Rightarrow 2N.P^+ = 0 \Rightarrow P^+$ i $P^- \in C[2N]$. □

4.2.2 Observació. n_D és invariant galoisià.

4.2.4 Càlcul de n_D

Sigui $\Lambda = \Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$ tal que $C = \mathbb{C}/\Lambda$, $\tau \in \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$.

Recordem la funció σ de Weierstrass

$$\sigma(z) = z \exp\left(- \sum_{n>1} \frac{G_{2n}(\tau)}{2n} z^{2n} \right)$$

on $G_{2n} = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2n}$ és la $2n$-èsima sèrie d'Eisenstein i la propietat que tota funció el·líptica s'expressa en termes de la funció σ a partir del seu divisor (cf. [26], I.5.5).

Considerem $\overline{\beta}_0 : \mathbb{C} \to C \to \mathbb{P}^1_{\mathbb{C}}$ i sigui $z^+ = \frac{a}{2N} + \frac{b}{2N}\tau$ el zero de $\overline{\beta}_0$ en el paralel·logram fonamental. Aleshores

$$\overline{\beta}_0(z) = (-1)^N \frac{\sigma(z - z^+)^N}{\sigma(z + z^+)^N} e^{2z(a\eta_1 + b\eta_2)} \tag{4.1}$$

amb $\eta_1 = \zeta(\frac{1}{2}), \eta_2 = \zeta(\frac{\tau}{2}), \eta_1\tau - \eta_2 = \pi i$, on ζ és la funció ζ de Weierstrass. Recordem la relació $\zeta(z) = \frac{\sigma'(z)}{\sigma(z)}$.

A partir d'aquesta expressió explícita de $\overline{\beta}_0$, aixecant el camí $\gamma(t) = e^{\pi i t}$, $t \in [0,1]$ i la forma diferencial $\omega = \frac{1}{N}\frac{dX}{X}$ de $\mathbb{P}^1_{\mathbb{C}}$ a cada un dels bucles orientats $\gamma_1, \gamma_2, \gamma_3$ (el dibuix és orientable), obtenim

$$n_D = \frac{2N}{(N_1 + N_2, N_2 + N_3, N_3 + N_1)}.$$

4.2.5 Inversió del problema

Sigui $C = \mathbb{C}/\Lambda_\tau$, $0 \leq a, b < 2N$, a, b enters, $z^+ = \frac{a}{2N} + \frac{b}{2N}\tau$. La funció $\overline{\beta}_0$ definida com abans és el·líptica i té el divisor adequat. Només falta ajustar els graus de ramificació.

4.2.3 Proposició. *La funció $\overline{\beta}_0$ és de Belyĭ si i només si*

$$a\zeta(\frac{1}{2}) + b\zeta(\frac{\tau}{2}) = N\zeta(\frac{a}{2N} + \frac{b}{2N}\tau).$$

Prova. Hem de tenir

$$\operatorname{div}\overline{\beta}_0' = (N-1)[z^+] + 2[0] - (N+1)[-z^+].$$

Calculant a partir de l'expressió de $\overline{\beta}_0$ (4.1) i tenint en compte $\zeta(z) = \dfrac{\sigma'(z)}{\sigma(z)}$, obtenim

$$\begin{aligned}\frac{\overline{\beta}_0'(z)}{\overline{\beta}_0(z)} &= N[\zeta(z-z^+) - \zeta(z+z^+)] + 2a\eta_1 + 2b\eta_2 \\ &= N[\zeta(z-z^+) - \zeta(z+z^+) + 2\zeta(z^+)] + 2a\eta_1 + 2b\eta_2 - 2N\zeta(z^+).\end{aligned}$$

Per transformar l'última expressió, fem servir el lema següent (cf. [6], p. 55)

4.2.4 Lema. $\dfrac{\wp'(v)}{\wp(u) - \wp(v)} = \zeta(u-v) - \zeta(u+v) + 2\zeta(v)$

i obtenim

$$\frac{\overline{\beta}_0'(z)}{\overline{\beta}_0(z)} = N\frac{\wp'(z^+)}{\wp(z) - \wp(z^+)} + 2a\eta_1 + 2b\eta_2 - 2N\zeta(z^+) \Rightarrow$$

$$\overline{\beta}_0'(z) = N\overline{\beta}_0(z)\frac{\wp'(z^+)}{\wp(z) - \wp(z^+)} + \overline{\beta}_0(z)(2a\eta_1 + 2b\eta_2 - 2N\zeta(z^+)).$$

$$\text{Ara, } \operatorname{div}\frac{1}{\wp - \wp(z^+)} = 2[0] - [z^+] - [-z^+] \Rightarrow$$

$$\operatorname{div}\frac{\overline{\beta}_0}{\wp - \wp(z^+)} = (N-1)[z^+] + 2[0] - (N+1)[-z^+]$$

que és el divisor buscat. D'aquí es dedueix que $a\eta_1 + b\eta_2 = N\zeta(z^+)$).□

4.2.6 Formes modulars

$\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ opera sobre

$$R_0(n) = \{(a,b) \in \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} : \langle a,b\rangle = \mathbb{Z}/n\mathbb{Z}\}$$

per la dreta posant

$$(a,b)^M = (a',b') \text{ on } \begin{pmatrix} b' \\ a' \end{pmatrix} = M^t \begin{pmatrix} b \\ a \end{pmatrix}$$

per a $M \in \Gamma(1)$. Posem $H(a,b) = Stab_{\Gamma(1)}(a,b)$. Tenim $\Gamma(n) \subset H(a,b)$, $H(a,0) = \Gamma_1(n)$.

Definim

$$F_{a,b}(\tau) = \frac{1}{i\pi}(n\zeta(\frac{a}{n} + \frac{b}{n}\tau) - 2a\zeta(\frac{1}{2}) - 2b\zeta(\frac{\tau}{2}))$$

i posem

$$F_m(\tau) = F_{m,0}(\tau)$$

per a $m \in (\mathbb{Z}/n\mathbb{Z})^*$.

4.2.5 Proposició. *$F_{a,b}(\tau)$ és una forma modular de pes 1 per a $H(a,b)$, F_m és una forma modular de pes 1 per a $\Gamma_1(n)$.*

La funció g_m definida per

$$g_m = \frac{F_m^{12}(\tau)}{\Delta(\tau)}$$

és una funció meromorfa sobre $X_1(n)$ i holomorfa sobre $X_1(n)^0$. Per construcció els zeros de $g_m(\tau)$ corresponen als valors de τ pels quals l'aplicació $\overline{\beta}_0$ és de Belyĭ. D'aquí es dedueix una caracterització "modular"de $\mathcal{E}_N$:

4.2.6 Proposició. *Existeix una bijecció entre els zeros de g_m en $X_1(n)^0$ i els dibuixos $D \in \mathcal{E}_N$ amb invariant $n_D = n$.*

A més, a partir de les F_m es pot construir un polinomi $P_n(X) \in \mathbb{Q}[X]$ tal que els zeros de $P_n(X)$ són exactament els invariants j de les corbes associades als dibuixos $D \in \mathcal{E}_N$ tals que $n_D = n$. En particular,

$$\begin{aligned} \operatorname{gr} P_n &= \frac{r}{12} && \text{si } n \text{ és senar} \\ &= \frac{r}{12} - \frac{1}{2}\varphi(\frac{n}{2}) && \text{si } n \text{ és parell} \end{aligned}$$

on $r = \frac{1}{2}n^2 \prod_{p|n}(1 - \frac{1}{p^2})$.

4.2.7 Exemples

$N = 3$	un sol dibuix $D_{1,1,1}$	$j = 0$
$N = 4$	un sol dibuix $D_{1,1,2}$	$j = \frac{210646}{6561}$
$N = 5$	$D_{1,2,2}$ per a $n = 10$	
	$D_{3,1,1}$ per a $n = 5$	$j = \frac{20480}{243}$

Teresa Crespo
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les corts Catalanes 585, E-08007 Barcelona,
teresa.crespo@ub.edu

Bibliografia

[1] *P. Beazley Cohen, C. Itzykson i J .Wolfart*, Fuchsian triangle groups and Grothendieck dessins. Variations on a theme of Belyi,Comun. Math. Phys. 163 (1994), 605-627.

[2] *S. Beckmann*, Ramified Primes in the Field of Moduli of Branched Coverings of Curves, J. Algebra 125 (1989), 236-255.

[3] *G.V. Belyi*, On Galois extensions of a maximal cyclotomic field, Math. USSR Izv. 14 (1979) 247–256.

[4] *B. Birch*, Noncongruence subgroups, covers and drawings, a The Grothendieck Theory of Dessins d'Enfants (Luminy, 1993) (L. Schneps, ed.), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, Cambridge, 1994, pp. 25–46.

[5] *E. Casas-Alvero*, Singularities of plane curves. London Mathematical Society Lecture Note Series, 276. Cambridge University Press, Cambridge, 2000. xvi+345 pp.

[6] *K. Chandrasekharan*, Elliptic functions, Springer, 1980.

[7] *K. R. Coombes, D. Harbater*, Hurwitz families and arithmetic Galois groups. Duke Math. J., vol. 52, 1985, pp. 821-839.

[8] *J.-M. Couveignes, L. Granboulan*, Dessins from a geometric point of view. In: The Grothendieck theory of dessins d'enfants (Luminy, 1993), 79–113, London Math. Soc. Lecture Note Ser., 200, Cambridge Univ. Press, Cambridge, 1994.

[9] *P. Dèbes*, Méthodes topologiques et analytiques en théorie inverse de Galois: théorème d'existence de Riemann, en

Arithmétique des revêtements algébriques, Actes du colloque de Saint-Étienne (ed. B. Deschamps) Séminaires et Congrès 5, Soc. Math. de France, Paris, 2001. [accessible en: http://smf.emath.fr/Publications/SeminairesCongres/]

[10] *D. Eisenbud*, Commutative algebra, With a view toward algebraic geometry. Springer, New York, 1995. Graduate Texts in Math. 150.

[11] *N. D. Elkies*, ABC implies Mordell, Internat. Math. Res. Notices 1991, n. 7, 99-109 [Apèndix de Duke J. Math. 64 (3) (1991)].

[12] *J. S. Ellenberg*, Galois invariants of dessins d'enfants. In: Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 27–42, Proc. Sympos. Pure Math., 70, Amer. Math. Soc., Providence, RI, 2002.

[13] *M. Fried*, Fields of definition of function fields and Hurwits families - groups as Galois groups, Comm. Algebra 5 (1977), 17-82.

[14] *A. Grothendieck*, Revêtements étales et groupe fondamental (SGA 1), LNM, vol. 224, Springer, New York, 1971.

[15] *A. Grothendieck*, Esquisse d'un programme. In Geometric Galois Actions, vol. 1: Around Grothendieck's Esquisse d'un Programme. Cambridge University Press, 1997, Lecture Notes in Math. 242

[16] *D. Husemöller*, Elliptic curves, GTM 111, Springer, 1987.

[17] *F. Jarvis*, Grothendieck-Teichmüller theory (2003), notes del curs Braid groups and Galois theory. [accessible en: http://www.shef.ac.uk/∼pm1afj/]

[18] *B. Köck*, Belyi's theorem revisited, Beiträge Algebra Geom. 45 (2004), n§ 1, 253-265.

[19] *A. J. Lenstra, H. W. Lenstra Jr., L. Lovász*, Factoring polynomials with rational coefficients. Math. Ann. 261 (1982), no. 4, 515–534.

[20] *G. Malle and B. H. Matzat*, Inverse Galois theory, Springer, New York, 1999.

[21] *G. Shabat and V. Voevodsky*, Drawing curves over number fields. In The Grothendieck Festschrift, Vol III, pp. 199-227. - Birkhäuser, 1990, Progress in Math 88.

[22] *L. Schneps* , Dessins d'enfants on the Riemann sphere, in: Schneps L. (Ed.), The Grothendieck Theory of Dessins d'Enfants, London Math. Soc. Lecture Notes, Vol. 200, Cambdridge Univ. Press, 1994.

[23] *A. J. Scholl*, The ℓ-adic representations attached to a certain noncongruence subgroups, J. reine angew. Math. 393 (1988), 1-15.

[24] *J-P. Serre*, Lectures on the Mordell-Weil Theorem, Aspects of Mathematics E, vol. 15, Vieweg, 1989.

[25] *J-P. Serre*, Topics in Galois Theory, Jones and Bartlett, Boston, 1992.

[26] *J.H. Silverman*, Advanced topics in the arithmetic of elliptic curves, GTM 151, Springer, 1994.

[27] *A. Surroca*, Siegel's theorem and the *abc* conjecture, preprint (2004) en Arxiv, math.NT/0408168.

[28] *M. van Frankenhuysen*, The ABC conjecture implies Roth's theorem and Mordell's conjecture, Matemática Contemporânea 16 (1999), 45-72.

[29] *M. van Frankenhuysen*, The ABC conjecture implies Vojta's height inequality for curves, J. of Number Theory 95 (2002), 289-302.

[30] *H. Völklein*, Groups as Galois Groups - an Introduction, Cambr. Studies in Adv. Math., vol. 53, Cambridge Univ. Press, 1996.

[31] *A. Weil*, The field of definition of a variety, Amer. J. Math 78 (1956), 509-524.

[32] *S. Wewers*, Three point covers with bad reduction. J. Amer. Math. Soc. 16 (2003), 991-1032.

[33] *S. Wewers*, Stable reduction of three point covers, preprint a Arxiv, math.AG/0401024.

[34] *J. Wolfart*, The 'obvious' part of Belyi's theorem and Riemann surfaces with many automorphisms, en: Geometric Galois Actions, vol. 1: Around Grothendieck's Esquisse d'un Programme (ed.'s: P. Lochak and L. Schneps), Cambridge University Press, 1997, Lecture Notes in Math. 242.

[35] *M. Wood*, Belyi-extending maps and the Galois action on the algebraic fundamental group of $\mathbb{P}^1\backslash\{0, 1, infinity\}$, preprint a Arxiv, math.NT/0304489.

[36] *L. Zapponi*, Dessins d'enfants en genre 1. Geometric Galois actions, 2, 79–116, London Math. Soc. Lecture Note Ser., 243, Cambridge Univ. Press, Cambridge, 1997.

[37] *L. Zapponi*, The arithmetic of prime degree trees, preprint.