Quelques calculs en théorie des nombres

Jean-Marc Couveignes

13 novembre 1994

Remerciements

Je tiens, tout d'abord, à remercier Henri Cohen pour avoir encadré mon travail depuis le stage d'option de fin d'études à l'École Polytechnique jusqu'à aujourd'hui. Je dois à sa grande largesse d'esprit et à l'étendue de ses compétences, d'avoir pu m'intéresser à des sujets divers. Cette grande variété d'intérêts est le privilège de l'algorithmique et j'en ai beaucoup usé. Je remercie Jacques Martinet et toute l'équipe d'algorithmique de Bordeaux pour son aide, son enthousiasme et pour tous ses travaux, en particulier le système PARI grâce auquel la vie est tellement plus simple. Je n'oublie pas que c'est Jean-Marc Deshouillers (un jône de la 65) qui m'a montré le chemin de Bordeaux. Qu'il en soit remercié.

Je ne saurais trop remercier Jacques Stern pour m'avoir accueilli dans son groupe de recherche en cryptographie et complexité. La fréquentation régulière de problèmes cryptographiques a été pour moi une source constante de réflexion. Elle a influencé profondément la conduite de mon travail, et l'éventuelle originalité de cette thèse lui doit beaucoup. Merci à tous les membres de cette chaleureuse équipe.

Chacune des parties qui composent cette thèse a beaucoup bénéficié de la sollicitude de quelques mathématiciens. Je voudrais tout particulièrement remercier Joseph Oesterlé et Leila Schneps pour les dessins, Hendrik Lenstra pour la théorie de Galois et la factorisation d'entiers, François Morain pour les courbes elliptiques et Henri Cohen à peu près partout.

Je suis très redevable à ceux qui ont travaillé régulièrement avec moi. Je pense en particulier à Louis Granboulan, à Pierre Lochak, Leila Schneps et François Morain. Ce travail doit beaucoup à leur conversation.

Je suis doublement reconnaissant à la Délégation Générale pour l'Armement, pour m'avoir accueilli dans l'Option Recherche du Corps des Ingénieurs de l'Armement sous la direction de l'ICA Quenzer et pour avoir soutenu nos travaux par l'intermédiaire de contrats passés avec le GRECC, le LIX et avec l'UMR d'Algorithmique Arithmétique de Bordeaux. Antoine Joux a beaucoup fait pour le succès de cette coopération, tant par sa contribution scientifique que par son travail d'organisation. Je l'en remercie vivement.

Ce serait pour moi un grand sujet de satisfaction si l'on pouvait reconnaître dans ce qui suit, la réponse à quelques unes des questions qui nous ont été posées.

Introduction

Cette thèse présente des solutions algorithmiques à quelques problèmes de théorie des nombres. Les trois sujets abordés sont le calcul de revêtements de la sphère moins trois points, la factorisation d'entiers et le calcul de la cardinalité de courbes elliptiques sur un corps fini. Dans ces deux derniers cas, il s'agit plutôt de raffiner ou de généraliser une méthode déjà connue. Au contraire, le problème du calcul des revêtements n'avait pas été étudié pour soi auparavant et il donne lieu à de plus amples développements. Ces trois parties ont en commun de puiser largement dans le corpus de la théorie algorithmique des nombres tel qu'il apparaît dans [11] et [27].

Comme par ailleurs les questions abordées sont on ne peut plus classiques, on peut penser qu'il n'y a rien de fondamentalement nouveau dans tout ce qui va suivre. Et c'est un fait que l'algorithmique se limite quelquefois à expliciter des constructions qui se trouvaient déjà implicitement dans des travaux plus anciens. Par exemple, dans ses *Leçons sur les constructions géométriques*, [31], Henri Lebesgue s'intéresse à la paramétrisation des courbes planes de genre 0 et donne des méthodes de calcul sans jamais toutefois se poser la question de leur complexité. Il finit par la recherche de points $\mathbb{Q}$-rationnels sur une conique et rappelle une construction due à Lagrange. Cette méthode est cousine de la réduction de Gauss des formes quadratiques. En 1984, Ong, Schnorr et Shamir proposèrent un protocole cryptographique reposant sur la difficulté (supposée!) de trouver un point rationnel sur une conique à coefficients dans un anneau $\mathbb{Z}/N\mathbb{Z}$ avec $N = p.q$ un grand entier composé. Malheureusement, ce problème est simple. Il suffit de relever la conique en une conique à coefficients dans $\mathbb{Q}$ et munie de points rationnels, puis de lui appliquer l'algorithme de Lagrange. On le "découvrit" peu après.

Le premier chapitre étudie de façon exhaustive le problème suivant : étant donné un dessin d'enfant de genre 0 sous la forme d'un ensemble fini $\{1, 2, ..., n\}$ et de deux permutations σ_0 et σ_1 de cet ensemble, calculer explicitement un revêtement algébrique de $\mathbb{P}_1(\mathbb{C})$ ramifié au dessus de 0, 1 et ∞ et de monodromie (σ_0, σ_1). On veut calculer aussi le corps des modules ainsi qu'un modèle pour ce revêtement, défini sur une extension minimale de ce corps. On montre que si le groupe d'automorphismes du dessin n'est pas cyclique d'ordre pair alors le corps des modules est un corps de définition. A contrario, un exemple de dessin sans modèle sur son corps des modules est calculé explicitement. Cette étude conduit à une présentation très concrète de la descente de Weil et des symboles de Hilbert.

Dans le second chapitre nous cherchons une méthode plus générale pour le calcul de dessins en tout genre. Cela conduit à une utilisation très pratique de la notion de point base tangentiel introduite par Deligne. On trouve une caractérisation linéaire des espaces associés à des diviseurs sur un dessin, comme noyaux d'opérateurs dont

la structure par blocs reflète l'action du groupoïde fondamental. L'étude locale de la descente de $\mathbb{C}$ à $\mathbb{R}$ permet de simplifier la fabrication des obstructions à la descente. Dans ce cadre restreint, il est possible de les constater à la main, par un simple calcul sur des permutations.

La substance théorique du troisième chapitre se réduit à l'observation que si $\mathbb{K}$ est une extension finie de $\mathbb{Q}$, de degré impair, alors la norme de $\mathbb{K}$ sur $\mathbb{Q}$ est une fonction multiplicative impaire. On en tire profit dans la situation suivante. Soit C un entier algébrique donné sous la forme d'un produit de plusieurs millions de petits facteurs

$$C = \prod_i (a_i + b_i\alpha),$$

où α est un générateur du corps. On sait aussi que tous les $a_i + b_i\alpha$ sont lisses, i.e. les idéaux correspondants sont produits d'idéaux au dessus de petits nombres premiers. On s'est assuré, par l'observation des valuations et de quelques caractères, que C est un carré dans $\mathbb{K}$ et on cherche une racine. Pour éviter de manipuler de trop grands nombres, on souhaite éviter le calcul explicite du produit des $a_i + b_i\alpha$. On songe alors à une méthode modulaire, mais la donnée d'une racine carrée $R_j^2 = C \bmod q_j$ pour de nombreux q_j ne suffit pas. Le relèvement des R_j pose des problèmes de signes que l'on résout par l'examen des normes. Ce calcul de racine carrée est utile dans la dernière phase du crible algébrique, méthode de factorisation inventée par Lenstra et Pollard [10], [8].

Dans le quatrième chapitre, nous nous intéressons à la construction d'isogénies entre courbes elliptiques dans le but de calculer le cardinal de ces courbes sur un corps fini, selon une idée de Schoof, Atkin et Elkies [39], [3], [19], [4]. Si on note ℓ le degré de l'isogénie, la factorisation brutale du polynôme de ℓ-torsion permet de construire l'isogénie en $O(\ell^5)$ opérations dans le corps. Elkies propose une méthode en $O(\ell^3)$ opérations. C'est là une amélioration essentielle — que l'on songe au cas où ℓ est de l'ordre de 1000. Elkies utilise des relations entre fonctions modulaires qui ne sont pas sans rappeler les relations de Newton entre fonctions symétriques élémentaires et sommes de puissances. Lorsque la caractéristique p du corps est inférieure à ℓ, ces relations se trivialisent et la méthode d'Elkies échoue. Nous montrons comment y remédier. Notre méthode construit l'isogénie entre deux courbes réputées isogènes, sous la forme d'un morphisme de groupes formels. Nous montrons aussi que le calcul des isogénies conduit à une description précise de la partie rationnelle du module de Tate. Cette dernière, lorsqu'elle n'est pas triviale, consiste le plus souvent en deux sous-espaces propres du Frobenius. Son étude conduit à une amélioration de la méthode de Schoof-Atkin-Elkies. Tout ceci est motivé par les développements récents de la cryptographie à base de courbes elliptiques. L'utilisation des courbes elliptiques à coefficients dans de grands corps finis de caractéristique 2 est désormais possible.

Chapitre 1

Calcul et rationalité de fonctions de Belyi en genre 0

Ce chapitre a été publié dans les Annales de l'Institut Fourier [16].

Les pages qui suivent comportent une méthode de calcul de fonctions de Belyi "optimales", associées à des dessins plans. Cette étude conduit à s'interroger sur la possibilité de définir une fonction de Belyi sur le corps des modules du dessin. Pour les arbres par exemple, nous montrons que c'est toujours le cas. La preuve donne une méthode pour spécifier une telle fonction. Nous donnons ensuite un exemple de dessin qui n'admet pas de fonction de Belyi sur son corps des modules. Enfin, nous étudions la question plus générale du calcul de fonctions de Belyi pour des dessins avec ou sans automorphismes et de genre 0, et en particulier, comment calculer une fonction de Belyi définie sur le corps des modules du dessin, chaque fois que c'est possible, ou sur une extension minimale dans le cas contraire. Ceci nous conduit à présenter quelques algorithmes pour la recherche de points rationnels dans des corps de genre 0.

1.1 Introduction

A l'heure de l'affût, soit lorsque la lumière
Précipite ses traits dans l'humide séjour,
Soit lorsque le soleil rentre dans sa carrière,
Et que, n'étant plus nuit, il n'est pas encor jour,
Au bord de quelque bois sur un arbre je grimpe,
Et, nouveau Jupiter, du haut de cet Olympe,
Je foudroie, à discrétion,
Un lapin qui n'y pensait guère.
Je vois fuir aussitôt toute la nation
Des lapins, qui, sur la bruyère,
L'œil éveillé, l'oreille au guet,
S'égayaient, et de thym parfumaient leur banquet.
Le bruit du coup fait que la bande
S'en va chercher sa sûreté
Dans la souterraine cité:
Mais le danger s'oublie, et cette peur si grande
S'évanouit bientôt; je revois les lapins,
Plus gais qu'auparavant, revenir sous mes mains.

Ne reconnaît-on pas en cela les humains?

La Fontaine, *Les Lapins.*

Ce qui suit comporte 10 sections. Immédiatement après celle-ci, la deuxième est

un rappel et une mise en forme assez générale des équations conduisant au calcul d'une fonction de Belyi dans le cas des arbres. On notera cependant que des formules analogues existent pour un dessin quelconque. Dans la troisième section, une méthode de calcul est proposée. L'existence de fonctions de Belyi agréables pour les arbres est démontrée dans la quatrième section. La cinquième section présente un dessin dont le corps des modules est Q mais sans fonction de Belyi définie sur $\mathbb{Q}$ sur la sphère. Cet exemple est renforcé dans la sixième section pour conduire à un dessin sans modèle défini sur $\mathbb{Q}$ sur la sphère ni sur aucune courbe de genre 0. Dans la septième section nous montrons comment calculer une fonction de Belyi pour un dessin de genre zéro sans automorphismes, définie sur son corps des modules. Dans la huitième section, nous examinons le cas des dessins dont le groupe d'automorphismes est non trivial. Nous concluons dans la neuvième section en reprenant les résultats des sections précédentes. Pour finir, la dixième section décrit les calculs effectués sous Maple V et leurs résultats.

Une description du cadre théorique de ces calculs se trouve dans l'article de Leila Schneps donné en référence (voir aussi [9] et [6] bien sûr).

Je la remercie d'avoir attiré mon attention sur l'esquisse d'un programme de Grothendieck ([22]) où j'ai puisé les motivations de cet article, et dont bien sûr, les pages qui suivent n'abordent qu'une infime partie.

Je remercie Henri Cohen, Hendrik W. Lenstra, Jacques Martinet, et Michel Matignon pour leurs explications, et leurs conseils. Je remercie tout particulièrement Joseph Oesterlé pour ses recommandations et ses observations. Les calculs numériques et la réduction des réseaux, si utiles dans la recherche de certaines fonctions de Belyi ont étés menés grâce aux conseils et aux programmes de mes collègues du G.R.E.C.C., Antoine Joux et Louis Granboulan que je remercie chaleureusement. Je remercie de même tous les membres de l'équipe de théorie des nombres de Bordeaux, Henri Cohen et Francine Delmer en particulier, qui ont pris goût eux aussi à ces "calculs de lapins" et dont les nombreux exemples m'ont beaucoup aidé.

1.2 Fonctions de Belyi des arbres.

Une fonction de Belyi est une application rationnelle Π d'une courbe $\mathcal{C}$, à valeurs dans $P_{1/C}$ et ramifiée seulement au dessus de 0, 1 et ∞. On demande que Π et $\mathcal{C}$ soient définies sur $\bar{Q}$, ce qui est toujours possible, de par la rationalité des trois valeurs singulières 0, 1 et ∞. Un dessin d'enfant est un tel couple $(\mathcal{C}, \Pi)$ défini à $\bar{Q}$-isomorphisme près.

Lorsque $\mathcal{C} = P_{1/C}$, l'application Π est donc définie à une homographie près (et en général à un automorphisme de $\mathcal{C}$ près).

Si on demande, de plus, que l'indice de ramification en chacun des points au dessus de 1 soit exactement 2, la fonction de Belyi et le dessin sont dits propres (*clean* en anglais).

Alors, on peut considérer l'image réciproque du segment réel $[0,1]$ dans $P_{1/C}$. On obtient un graphe connexe dont les sommets correspondent aux zéros de Π avec pour multiplicités le nombre de segments arrivant au sommet. Sur chaque segment reliant deux sommets, la fonction Π prend une et une seule fois la valeur 1. Le graphe délimite des faces (cellules) au milieu desquelles se trouve un pôle dont la multiplicité est le nombre de segments qui bordent la face.

Comme on l'a vu, nous adoptons la convention suivante: les faces sont des pôles, les sommets des zéros et les cotés des uns. Noter que ce n'est pas la convention choisie dans [21].

Voyons comment rechercher une fonction de Belyi associée à un *arbre propre*. On place d'abord l'unique face à l'infini, de façon à obtenir un polynôme.

On appelle α_i les sommets et ν_i leurs multiplicités pour $1 \leq i \leq N$ où N est le nombre de sommets et $d = \sum \nu_i$ le degré de la fonction de Belyi.

On obtient alors une identité du type

$$\prod_{i \in I} (X - \alpha_i)^{\nu_i} + \lambda = Q^2(X) \tag{1.1}$$

où I est l'ensemble des indices correspondant aux sommets et λ est un paramètre lié à la normalisation du polynôme. Les racines de Q correspondent aux arêtes de l'arbre.

On notera que le polynôme

$$\Pi = \prod_{i \in I} (X - \alpha_i)^{\nu_i}$$

se factorise en

$$\Pi^+ = Q - \sqrt{\lambda} = \prod_{i \in I^+} (X - \alpha_i)^{\nu_i} \quad \text{et} \quad \Pi^- = Q + \sqrt{\lambda} = \prod_{i \in I^-} (X - \alpha_i)^{\nu_i}$$

où l'on définit I^+ comme l'ensemble des indices correspondant aux sommets α_i tels que $Q(\alpha_i) = \sqrt{\lambda}$ (et que, par exemple, on colorie en rouge) et I^- l'ensemble des indices correspondant aux sommets α_i tels que $Q(\alpha_i) = -\sqrt{\lambda}$ (et que, par exemple, on colorie en bleu). Nous pouvons ainsi considérer la fonction de Belyi comme la composée de deux morphismes: celui défini par $Q/\sqrt{-\lambda}$ et celui défini par le polynôme $X^2 + 1$. On comprend ainsi que les sommets rouges et bleus alternent le long de l'arbre, si bien qu'une fois choisie la couleur de l'un d'eux, on a déterminé celle de tous les autres.

Alors

$$\Pi = \Pi^+ \Pi^- = (Q - \sqrt{\lambda})(Q + \sqrt{\lambda})$$

Si on dérive l'identité (1.1) on obtient,

$$\Pi(\Sigma^+ + \Sigma^-) = 2QQ' \tag{1.2}$$

avec

$$\Sigma^+ = \sum_{i \in I^+} \frac{\nu_i}{X - \alpha_i} \quad , \quad \Sigma^- = \sum_{i \in I^-} \frac{\nu_i}{X - \alpha_i}$$

Comme Q est premier avec Π, on en déduit que

$$dQ = (\Sigma^+ + \Sigma^-)\Theta$$

où $\Theta = \prod_{i \in I} (X - \alpha_i)$, et si l'on pose $\sigma^+ = \Sigma^+ \Theta$ et $\sigma^- = \Sigma^- \Theta$, alors

$$dQ = (\sigma^+ + \sigma^-) \tag{1.3}$$

On veut prouver maintenant l'identité

$$d\sqrt{\lambda} = (\sigma^+ - \sigma^-) \tag{1.4}$$

Pour cela, il suffit d'observer que le membre de droite est un polynôme de degré inférieur ou égal à $N-1$ et qu'il prend la valeur $d\sqrt{\lambda}$ pour les N nombres α_i. Par exemple si α_i est un sommet rouge alors $\sigma^-(\alpha_i) = 0$ et donc $(\sigma^+ - \sigma^-)(\alpha_i) = (\sigma^+ + \sigma^-)(\alpha_i) = dQ(\alpha_i) = d\sqrt{\lambda}$.

Maintenant la somme et la différence de (1.3) et (1.4) donnent

$$2\sigma^+ = d\Pi^- \text{ et } 2\sigma^- = d\Pi^+ \tag{1.5}$$

Ces équations ont l'avantage d'un degré plus faible et elles découplent en partie les sommets rouges et les sommets bleus. Ce sont elles que l'on peut utiliser si l'on entreprend de calculer la fonction de Belyi avec un système de calcul formel. En particulier, il est toujours possible d'éliminer quelques inconnues qui apparaissent linéairement, et deux équations sont entièrement linéaires.

On peut ainsi songer à résoudre le système obtenu en développant en X le système (1.5) (ou même l'équation (1.1) en général) et en égalant les coefficients. Les inconnues choisies sont alors les α_i ou, plus habilement, leurs fonctions de Newton. On utilise l'algorithme de réduction de bases de Grobner. Pour un dessin un tant soit peu complexe, ces techniques ne sont plus raisonnables.

Nous proposons de diviser plutôt l'équation (1.4) par Θ. En posant $U = 1/X$ on trouve

$$\frac{d\sqrt{\lambda}U^{N-1}}{\prod_{i\in I}(1-U\alpha_i)} = \sum_{i\in I^+}\frac{\nu_i}{1-U\alpha_i} - \sum_{i\in I^-}\frac{\nu_i}{1-U\alpha_i} \tag{1.6}$$

et les $N-1$ premiers termes du développement donnent les équations

$$\sum_{i\in I}\bar{\nu}_i\alpha_i^k = 0 \quad \text{pour} \quad 0 \le k \le N-2 \tag{1.7}$$

où $\bar{\nu}_i = \nu_i$ pour les rouges et $\bar{\nu}_i = -\nu_i$ pour les bleus.

La première de ces $N-1$ équations est triviale :

$$\sum_{i\in I}\bar{\nu}_i = 0$$

En effet, puisque les sommets rouges et bleus alternent, la somme des multiplicités rouges égale la somme des multiplicités bleus.

Il reste $N-2$ équations non triviales. L'ensemble des solutions $\Upsilon = (\alpha_i)_{1\le i\le N}$ de ce système est invariant par les transformations affines de C agissant diagonalement sur C^N

$$(\Upsilon_i)_i \mapsto (A\Upsilon_i + B)_i$$

où $A, B \in C$.

Remarques

– Les équations (1.7) se généralisent au cas d'un dessin de genre 0 quelconque dont toutes les valences sont paires. On peut alors colorier aussi bien les faces que les sommets et affecter les multiplicités d'un signe. Si on appelle α_i les sommets et β_j les faces, si $\bar{\nu}_i$ est la multiplicité algébrique de α_i et $\bar{\mu}_j$ celle de β_j, alors à tout sommet α_i on associe une fonction ζ_{α_i} définie par

$$\zeta_{\alpha_i}(x) = \sum_j \bar{\mu}_j \frac{\alpha_i - \beta_j}{x - \beta_j}$$

et à toute face β_j, on associe une fonction ζ_{β_j} définie par

$$\zeta_{\beta_j}(x) = \sum_i \bar{\nu}_i \frac{\beta_j - \alpha_i}{x - \alpha_i}$$

Alors la fonction ζ_{α_i} admet un zéro d'ordre $|\bar{\nu}_i|/2 - 1$ en α_i et la fonction ζ_{β_j} admet un zéro d'ordre $|\bar{\mu}_j|/2 - 1$ en β_j.

En d'autres termes on a les deux séries d'équations suivantes:

pour tout i, et pour $0 \leq k < |\bar{\nu}_i|/2$

$$\sum_j \frac{\bar{\mu}_j}{(\beta_j - \alpha_i)^k} = 0,$$

et pour tout j, et pour $0 \leq k < |\bar{\mu}_j|/2$

$$\sum_i \frac{\bar{\nu}_i}{(\alpha_i - \beta_j)^k} = 0.$$

La condition de parité sur les multiplicités n'est pas restrictive. En effet, si φ est une fonction de Belyi associée à un dessin quelconque, alors la fonction ψ définie par

$$\psi = -1/4 \left(\frac{\varphi(\varphi - 1)}{\varphi - 2} \right)^2$$

est une fonction de Belyi associée à un dessin dont toutes les multiplicités sont paires au dessus de 0 et ∞ et exactement égales à deux au dessus de 1.

– Dans le cas le plus simple où l'arbre est une chaîne de longueur N, alors II est le polynôme de Tchebitchev de degré $2N$ et (1.7) donne de classiques mais toujours amusantes relations sur les cosinus correspondants.

– Les équations (1.7) forment un système de Vandermonde à l'envers puisque ce sont les α_i que l'on cherche ici, les ν_i étant connus.

On appelle Γ la fonction de C^N dans C^{N-2} définie par les membres de gauche de (1.7).

$$\Gamma(\alpha_1, ..., \alpha_N) = (\sum_{i \in I} \bar{\nu}_i \alpha_i^k)_{1 \leq k \leq N-2}$$

On note que Γ et sa différentielle Γ' sont très faciles à calculer. Le rang de Γ'_Υ est le minimum de $N-2$ et du nombre de α_i distincts.

Ces observations conduisent à la méthode numérique suivante.

1.3 Méthode de Newton.

Remarquons que les vecteurs de $C^N \setminus \{(z_1, z_2, ..., z_N) | z_1 = z_2 = ... = z_N\}$ définis à affinité près sont en fait des points de P_{N-2}.

A toute suite $(\Upsilon_i)_i$ de vecteurs de $C^N \setminus \{(z_1, z_2, ..., z_N) | z_1 = z_2 = ... = z_N\}$ définis à affinité près, on associe une suite de P_{N-2}. Si cette seconde suite est convergente on dira abusivement que $(\Upsilon_i)_i$ converge. Dans ce contexte, la méthode de Newton est définie par la formule de récurrence

$$\Upsilon_{i+1} = \Upsilon_i - {\Gamma'_{\Upsilon_i}}^{-1} \Gamma(\Upsilon_i) \tag{1.8}$$

On note que Γ'_{Υ_i} n'est pas inversible. Ainsi ${\Gamma'_{\Upsilon_i}}^{-1}\Gamma(\Upsilon_i)$ est défini à un élément du noyau près. On choisi pour ${\Gamma'_{\Upsilon_i}}^{-1}\Gamma(\Upsilon_i)$ le vecteur orthogonal au noyau; autrement dit, on se déplace selon la ligne de plus grande pente.

Ici la forme quadratique à utiliser peut être définie à partir de

- la dérivée seconde de Γ en Υ_i.
- une métrique à définir sur P_{N-2}.

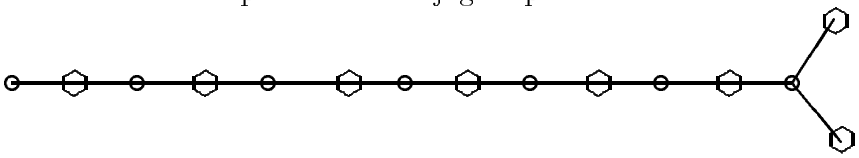
Pour le calcul numérique, il faut choisir un représentant convenable de Υ_i dans C^N, afin d'éviter une divergence artificielle due à un glissement le long des lignes de niveaux de Γ. Il reste maintenant à décrire une heuristique pour le calcul d'une approximation Υ_0 propre à faire converger la méthode.

On remarque d'une part que dans les dessins calculés explicitement jusqu'à présent, les segments sont presque rectilignes. Par ailleurs, les angles formés par les arêtes autour des sommets doivent être égaux. Il ne manque plus à cette description schématique qu'une évaluation de la longueur des segments. Celle-ci peut être obtenue par l'observation de dessins voisins mais plus simples. Ainsi le système (1.7) varie peu lorsqu'on "éclate" un point, c'est-à-dire lorsqu' on remplace un point de multiplicité $\bar{\nu}$ par deux points de couleurs opposées et de multiplicités $\bar{\nu}_1$ et $\bar{\nu}_2$ telles que $\bar{\nu}_1 + \bar{\nu}_2 = \bar{\nu}$. Cela revient à greffer un nouveau segment sur le dessin qui pousse alors d'étape en étape comme un arbre. Si l'on appelle Υ^t la solution du premier arbre à N sommets, on peut par exemple obtenir un vecteur Υ_0^g de dimension $N+1$ en dupliquant la valeur correspondant au sommet éclaté. Ce vecteur peut être pris comme valeur de départ dans la méthode itérative pour le calcul de l'arbre greffé à $N+1$ sommets. En effet, sur les $N-1$ équations (1.7) correspondantes, les $N-2$ premières sont déjà satisfaites parce que ce sont les équations (1.7) de l'arbre précédent. On peut ainsi utiliser les longueurs de l'arbre précédent comme des approximations à celles de l'arbre greffé.

Une fois obtenue une bonne approximation de la limite Υ_∞ on a donc un élément de P_{N-2} que l'on cherche à relever dans C^N en un point défini sur un corps raisonnable. Pour cela il convient de définir une normalisation habile qui assure à priori que ce point est défini sur un domaine de rationalité aussi petit que possible. Si les approximations calculées sont assez fines, on pourra alors retrouver les diverses dépendances algébriques à l'aide de l'algorithme LLL de Lenstra, Lenstra et Lovász ([32] et [25]). On obtiendra alors une solution formelle au problème (1.1).

Exemple

L'arbre en T à 15 points a 21 conjugués possibles.



Le calcul montre qu'il est en effet de degré 21. Les 21 sous-corps de $\bar{Q}$ correspondants sont engendrés par les racines du polynôme

$$
\begin{aligned}
&2^{12}3^5 5^2 x^{21} + 1158312960\,x^{20} + 25502867712\,x^{19} + 341618429376\,x^{18} \\
&+3209936201344\,x^{17} + 20392715344064\,x^{16} + 99638796203968\,x^{15} \\
&+370504764844224\,x^{14} + 1062741483903680\,x^{13} + 2370640833511888\,x^{12} \\
&+4128644196255936\,x^{11} + 5614827771514976\,x^{10} + 5942714032340512\,x^9 \\
&+4860315116093808\,x^8 + 3036961695710128\,x^7 + 1425822458726372\,x^6 \\
&+491072052205560\,x^5 + 119836481716252\,x^4 + 19663328827436\,x^3 \\
&+1993132055040\,x^2 + 106550236828\,x + 2000024111
\end{aligned}
$$

Le discriminant de ces corps, calculé avec Pari par Henri Cohen est

$$-2^{588}3^{382}5^{386}7^{61}11^{20}$$

Pour la méthode de Newton, les calculs numériques ont été menés sous Pari. Pour la recherche de dépendances algébriques avec LLL, j'ai eu recours aux conseils et aux programmes d'Antoine Joux.

1.4 Problèmes de rationalité

Dans cette section, nous définissons le corps des modules d'un dessin et montrons que dans le cas où le dessin est un arbre propre, il admet toujours une fonction de Belyi (un polynôme même) définie sur son corps des modules. On rappelle qu'une fonction de Belyi de genre 0, $\Pi : P_1 \to P_1$, est définie à composition à droite par une homographie près. Puisque une telle fonction peut être choisie définie sur $\bar{Q}$, on peut faire agir le groupe $\sigma \in Gal(\bar{Q}/Q)$ sur les coefficients de la fonction de Belyi (qui n'est autre qu'une fraction rationnelle). On obtient alors une fonction de Belyi associée à un dessin non-nécessairement égal au précédent. Cela définit une action de $Gal(\bar{Q}/Q)$ sur les dessins (on vérifie aisément que la définition donnée ne dépend pas de la fonction de Belyi choisie).

On appelle groupe des modules du dessin, le groupe des $\sigma \in Gal(\bar{Q}/Q)$ tels qu'il existe une homographie H_σ satisfaisant

$$^{\sigma}\Pi = \Pi \circ H_\sigma$$

C'est le stabilisateur du dessin dans $Gal(\bar{Q}/Q)$ selon l'action décrite plus haut.

On appelle corps des modules K d'un dessin, le corps fixé par le groupe G des modules du dessin. Pour une définition plus intrinsèque voir [18].

Nous cherchons maintenant une fonction de Belyi définie sur une extension aussi petite que possible du corps K (Par définition, le corps de définition d'une fonction de Belyi est le corps engendré par les fonctions symétriques des racines de son numérateur et de son dénominateur.) Pour cela on veut ajouter deux conditions appropriées au système (1.1). On va voir que dans le cas des arbres, il existe toujours une fonction de Belyi définie sur K et qu'elle peut être caractérisée par les deux conditions

$$\sigma_1 = 0 \qquad \text{et} \qquad \Sigma_u = 1 \tag{1.9}$$

où σ_1 et Σ_u sont, à peu de choses près, deux fonctions symétriques bien choisies.

La première spécification est que l'unique pôle soit à l'infini. On a alors un polynôme. Deux fonctions de Belyi satisfaisant à cette condition se correspondent, on l'a vu, par une application affine (homographie fixant l'infini).

On demande ensuite que la somme σ_1 des racines de ce polynôme soit nulle, ce qui peut toujours être obtenu en composant par une translation. Deux fonctions de Belyi satisfaisant aussi à cette deuxième condition se correspondent par une application linéaire (homographie fixant l'infini et zéro):

$$z \mapsto Az$$

Considérons $\Pi(X) = \pi_P X^P + \pi_{P-2}X^{P-2} + \pi_{P-3}X^{P-3} + ... + \pi_0$ l'une d'entre elles et appelons e le pgcd de l'ensemble des entiers l strictement positifs tels que π_l soit non nulle.

Il existe donc une combinaison multiplicative

$$\Sigma_u = \prod_k \pi_k^{\lambda_k}$$

des coefficients de Π, qui soit homogène en A de degré e (Identité de Bezout).

On pose comme troisième condition que $\Sigma_u = 1$. Comme Σ_u est une fonction homogène de degré e de A, il existe une et une seule fonction de Belyi satisfaisant aux trois conditions. En effet, pour qu'une application linéaire $z \mapsto Az$ laisse Σ_u invariant on doit avoir $A^e = 1$, mais justement tous les coefficients non nuls de Π sont de degré un multiple de e et donc notre fonction de Belyi est elle aussi invariante si on la compose par l'application linéaire $z \mapsto Az$.

La fonction Π_0 ainsi construite est définie sur K, cela découle de son unicité.

Notons en particulier qu'il est possible de construire Π_0 à partir de n'importe quelle fonction de Belyi Π de la façon suivante:

- Si la fonction a un dénominateur, alors ce dénominateur n'a qu'une racine correspondant à l'unique pôle p. On s'en débarrasse en composant par une homographie

$$H_1(X) = \frac{pX}{X+1}$$

– Maintenant on peut annuler la somme des racines en composant par la translation

$$H_2(X) = X - \frac{\sigma}{P}$$

où σ est la valeur initiale de cette somme.

– Pour finir on ramène à un la combinaison de fonctions symétriques Σ_u. Le degré de Σ_u est e. Soit Σ la valeur initiale de Σ_u et $\Sigma^{1/e}$ une de ses racines e-ième. On compose alors par

$$H_3(X) = \frac{X}{\Sigma^{1/e}}$$

On peut remarquer que e est le plus grand entier positif tel que $\Pi_0(X) = \widetilde{\Pi}_0(X^e)$ où $\widetilde{\Pi}$ est un polynôme. C'est aussi l'ordre de la symétrie de centre 0 qui laisse stable le dessin, ou mieux, l'ordre du groupe de symétrie du dessin.

En pratique, on peut utiliser d'autres fonctions symétriques que les π_k. Par exemple, on définit les polynômes Θ_k pour $k \in Z$ où

$$\Theta_k = \prod_{i \in I \text{ et } \bar{\nu}_i = k} (X - \alpha_i) \quad \text{et} \quad \Pi^+ = \prod_{k>0} \Theta_k^k \quad \text{et} \quad \Pi^- = \prod_{k<0} \Theta_k^{-k} \tag{1.10}$$

Donc Θ_k a pour racines les sommets d'une couleur et multiplicité données. Les polynômes $\widehat{\Theta}_k = \Theta_k \Theta_{-k}$ sont définis sur le même corps que Π. Leurs coefficients constituent une famille de fonctions symétriques plus riche, que l'on prend comme nouvelles inconnues du problème. On choisit alors deux telles fonctions, de degré un, et on demande que l'une soit nulle et l'autre égale à un. Il y a au plus une fonction de Belyi satisfaisant ces conditions. Elle est alors définie sur le corps des modules du dessin. Ces deux conditions ajoutées peuvent simplifier grandement les calculs car elles permettent d'éliminer deux inconnues. On remarque aussi que seules les multiplicités des points singuliers apparaissent dans les equations (1.1) ce qui ne suffit pas à caractériser le dessin, loin de là. Cependant, il n'y a qu'un nombre fini de dessins avec des multiplicités données. Ainsi le système (1.1) n'a qu'un nombre fini de solutions.

Remarques

– L'existence d'une fonction de Belyi sur le corps K est assurée dès qu'il existe un célibataire dans le dessin, c'est-à-dire un sommet ou un pôle qui soit unique par sa valence. Pour construire la fonction Π_0, il suffit alors d'envoyer ce célibataire à l'infini et de finir comme ci-dessus. Cette observation reste valable si la fonction de Belyi n'est pas propre. A vrai dire, elle l'est encore pour tout revêtement de genre 0 de la sphère moins un ensemble rationnel, et muni d'un célibataire.

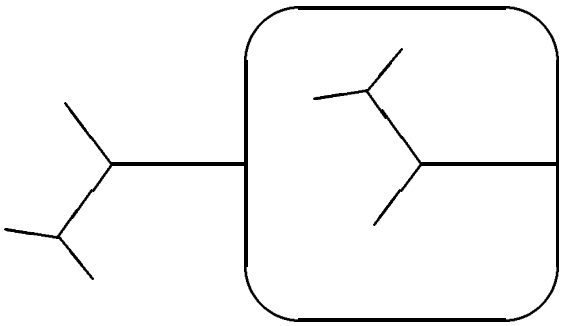
– La question qui se pose alors est de savoir s'il existe toujours une fonction de Belyi sur le corps K des modules du dessin, même en l'absence de célibataire. La réponse est non comme on le verra ci-dessous. Cependant, l'extension nécessaire est au plus quadratique.

1.5 Contre-exemple

Nous donnons maintenant un exemple de dessin dont le corps des modules est Q et pour lequel il n'existe pas de fonction de Belyi de P_1 dans P_1, définie sur Q.

Le dessin proposé ne doit comporter aucun célibataire, on choisit donc un dessin à deux faces. Pour simplifier, les deux faces n'ont que deux cotés en commun. On trace donc un cercle et deux points sur ce cercle. A partir de chacun de ces deux points on dessine deux arbres "conjugués" c'est-à-dire ayant la même liste de valences. Et voilà une famille de candidats contre-exemples.

Après quelques essais infructueux (certains dessins étaient trop complexes pour être explicitement calculés, d'autres, trop simples pour conduire à une obstruction) j'ai mené à leur terme les calculs correspondant au dessin suivant.



On remarque que ce dessin admet une bicoloration. Il comporte 6 sommets de valence 3, 6 sommets de valence 1 et deux faces de valence 12.

Pour les calculs, les deux pôles sont envoyés en zéro et l'infini. On exige en outre que la somme de tous les sommets de multiplicité 3 soit égale à 1.

On appelle $\widehat{\Theta}_1$ et $\widehat{\Theta}_3$ les polynômes de degré 6 définis par $\widehat{\Theta}_1 = \Theta_1\Theta_{-1}$ et $\widehat{\Theta}_3 = \Theta_3\Theta_{-3}$ avec les notations de (1.10). L'équation (1.1) est alors

$$\widehat{\Theta}_1\widehat{\Theta}_3^3 + \lambda X^{12} = Q^2(X) \tag{1.11}$$

Les calculs sont menés formellement comme décrits au paragraphe 1.10. On obtient comme attendu, deux fonctions de Belyi distinctes et conjuguées par l'action de Galois. Ces fonctions sont décrites dans la section 10. Il se trouve qu'elles sont définies sur $Q(i)$ et conjuguées. Appelons les $\mathrm{II} = -\lambda^{-1}X^{-12}\widehat{\Theta}_1\widehat{\Theta}_3^3$ et $\bar{\mathrm{II}}$ où l'on note en surlignant la conjugaison dans $Q(i)$. On trouve que

$$\bar{\mathrm{II}} = \mathrm{II} \circ H \text{ où } H(X) = \frac{A}{X} \text{ et } A = \frac{-1}{4100}$$

Cela prouve que le corps des modules du dessin est Q. Une homographie H peut être définie (à multiplication par une constante près) par une matrice 2×2 que nous notons $\mathcal{H}$. Nous choisissons ici de poser

$$\mathcal{H} = \begin{bmatrix} 0 & A \\ 1 & 0 \end{bmatrix}$$

Notons aussi que le groupe des automorphismes de II, i.e. l'ensemble des homographies H telles que

$$\Pi \circ H = \Pi$$

est trivial. En effet une telle homographie devrait soit fixer les pôles soit les inverser. Si elle les fixe alors c'est une application linéaire et donc triviale à cause de la normalisation adoptée. Si elle permute les pôles elle est de la forme $X \mapsto C/X$ et c'est une inversion de centre 0. Mais une telle inversion ne respecte pas le dessin. Graphiquement on voit que les petites fourchettes ont bougé. Celle qui s'élevait est abaissée et celle qui s'abaissait est relevée (selon les paroles de l'Évangile...)

Supposons maintenant qu'il existe une fonction de Belyi Π_Q définie sur le corps Q. Soit H_Q l'homographie telle que

$$\Pi_Q = \Pi \circ H_Q \tag{1.12}$$

On va montrer que H_Q peut être représentée par une matrice définie sur $Q(i)$.

On représente d'abord H_Q par une matrice quelconque de $\bar{Q}$. Ainsi on peut faire agir $Gal(\bar{Q}/Q)$ sur $\mathcal{H}_Q$ par action sur les coefficients.

Soit donc $\sigma \in Gal(\bar{Q}/Q(i))$. L'action de σ sur (1.12) donne

$$\Pi_Q = \Pi \circ H_Q^\sigma$$

puisque Π_Q et Π sont définies sur $Q(i)$. On en déduit que

$$\Pi = \Pi \circ H_Q^\sigma \circ H_Q^{-1}$$

et donc $H_Q^\sigma \circ H_Q^{-1}$ est l'identité. Toute matrice associée est constante, en particulier

$$\mathcal{H}_Q^\sigma = \mathcal{H}_Q \delta(\sigma).$$

On voit, en faisant à nouveau agir $Gal(\bar{Q}/Q(i))$ sur cette dernière équation que δ satisfait à la condition de cocycle.

$$\delta(\tau\sigma) = \delta(\tau)^\tau \delta(\sigma)$$

Le théorème 90 de Hilbert assure alors que l'on peut définir $\mathcal{H}_Q$ sur $Q(i)$ en divisant par une constante Δ appropriée (celle telle que $\delta(\sigma) = \Delta^{-1\sigma}\Delta$).

Il reste maintenant à faire agir sur (1.12) la conjugaison ordinaire de $Q(i)/Q$.

$$\Pi_Q = \bar{\Pi} \circ \bar{H}_Q = \Pi \circ H \circ \bar{H}_Q$$

Parce que le groupe d'automorphismes de Π est trivial, on en déduit l'existence d'une constante $\beta \in Q(i)$ telle que

$$\mathcal{H}_Q = \beta\mathcal{H} \circ \bar{\mathcal{H}}_Q$$

En conjuguant cette égalité on obtient

$$\bar{\mathcal{H}}_Q = \bar{\beta}\bar{\mathcal{H}} \circ \mathcal{H}_Q$$

puis

$$\bar{\mathcal{H}}_Q = \bar{\beta}\beta\bar{\mathcal{H}} \circ \mathcal{H} \circ \bar{\mathcal{H}}_Q$$

et donc

$$\beta\bar{\beta} = \frac{1}{A} = -4100$$

Or toutes les normes sont positives dans $Q(i)$. Contradiction.
On a donc prouvé le

Fait 1.1 *Le dessin défini par la fonction* II *n'admet pas de fonction de Belyi définie sur* $\mathbb{Q}$ *sur* $P_{1/Q}$.

On peut même reprendre le raisonnement précédent avec un corps quelconque K_0. Une fonction de Belyi pour le dessin considéré ici peut être définie sur un tel corps si et seulement s'il existe deux éléments x et y dans K_0 tels que $x^2+y^2 = (x+iy)(x-iy) = \frac{1}{A}$. Dans le cas où de tels x et y existent, ou bien $i \in K_0$ et on peut prendre la fonction de Belyi donnée plus haut, ou bien $i \notin K_0$ et on peut prendre pour matrice de passage

$$\mathcal{H}_Q = \begin{bmatrix} a & b \\ \beta\bar{a} & \beta\bar{b} \end{bmatrix}$$

où $\beta = x + iy$, $a = a_1 + a_2 i$ et $b = b_1 + b_2 i$ sont dans $K_0(i)$ et $\bar{a} = a_1 - a_2 i$, $\bar{b} = b_1 - b_2 i$ avec $a_1, a_2, b_1, b_2 \in K_0$. En remarquant que $4100 = 50^2 + 40^2$ est une norme dans $Q(i)$ on trouve

Fait 1.2 *Le dessin défini par la fonction* II *admet une fonction de Belyi sur la sphère de Riemann, définie sur un corps* K_0 *si et seulement s'il existe deux éléments* x *et* y *dans* K_0 *tels que* $x^2 + y^2 = (x + iy)(x - iy) = -1$

Cependant, puisque le dessin n'a pas d'automorphisme, le critère de descente de Weil, que l'on examinera plus en détail au paragraphe 1.7.2, implique l'existence d'un modèle défini sur Q pour ce dessin, c'est à dire, une courbe de genre 0 définie sur Q et une fonction de Belyi de cette courbe dans le plan projectif, définie sur Q elle aussi. Or, toute courbe sur Q, de genre zéro est isomorphe sur Q à une conique plane. On cherche donc une fonction de Belyi définie sur $\mathbb{Q}$, sur une conique définie sur $\mathbb{Q}$ et satisfaisant aux conditions de ramifications du dessin proposé.

Dans la suite de cette section, on utilisera des coordonnées projectives. Soit donc une conique $\mathcal{C}$ de P_2 d'équation en $[U, V, W]$

$$E(U, V, W) = aU^2 + 2bUV + cV^2 + dUW + eVW + fW^2 = 0$$

où $a, b, c, d, e, f \in Q$.

Tout isomorphisme de $\mathcal{C}$ sur P_1 peut se mettre sous la forme suivante où $[X, Y]$ sont les coordonnées projectives sur P_1

$$[X, Y] = [N(U, V, W), D(U, V, W)] = [n_1U + n_2V + n_3W, d_1U + d_2V + d_3W]$$

où $n_1, n_2, n_3, d_1, d_2, d_3 \in \bar{Q}$.

Supposons que N et D sont définis sur $Q(i)$ et que l'équation de $\mathcal{C}$ est

$$E(U, V, W) = N\bar{N} - AD\bar{D} \tag{1.13}$$

où $A = \frac{-1}{4100}$

On appelle $\Pi(X, Y)$, la version homogène de la fonction de Belyi Π déjà calculée. Alors,

$$\bar{\Pi}[X, Y] = \Pi[AY, X]$$

Si on compose Π et l'isomorphisme défini plus haut on obtient une fonction de Belyi Π_0 sur la conique

$$\Pi_0(U, V, W) = \Pi[N(U, V, W), D(U, V, W)]$$

On voit alors que Π_0 est définie sur $\mathbb{Q}$. En effet

$$\begin{aligned} \bar{\Pi}_0(U, V, W) &= \bar{\Pi}[\bar{N}(U, V, W), \bar{D}(U, V, W)] = \Pi[A\bar{D}, \bar{N}] = \Pi[AD\bar{D}, \bar{N}D] \\ &= \Pi[\bar{N}N, \bar{N}D] = \Pi[N, D] \end{aligned}$$

et on a utilisé l'équation de la courbe pour substituer $N\bar{N}$ à $AD\bar{D}$.

Il est donc possible d'obtenir des fonctions de Belyi définie sur $\mathbb{Q}$ sur toutes les coniques de la forme donnée en (1.13). Ces coniques sont deux à deux Q-isomorphes et le procédé de construction adopté n'est autre que celui décrit dans [45].

1.6 Contre-exemple, suite...

Comme on vient de le voir, le dessin précédent admet une fonction de Belyi définie sur $\mathbb{Q}$ sur une conique. On remarque que A intervient dans l'équation de cette conique. Or A est dans Q, ce qui est lié à la trivialité du groupe d'automorphismes du dessin.

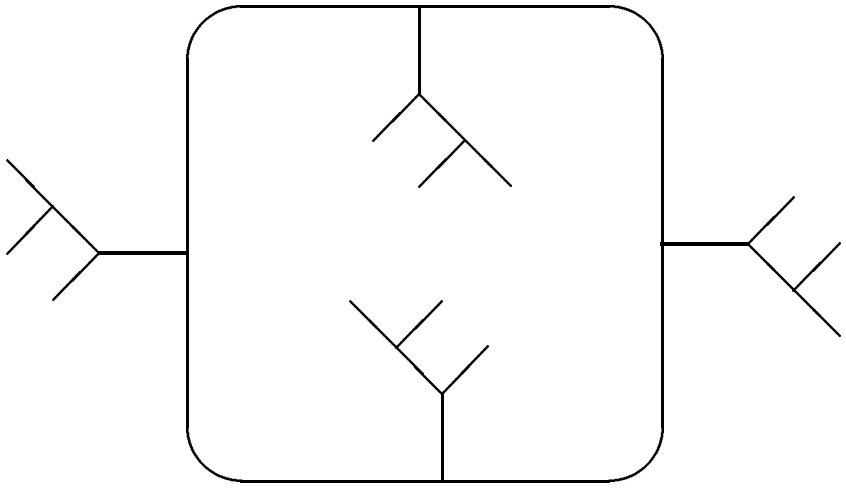
En effet, considérons la fonction de Belyi $\Psi(X) = \Pi(X^2)$ obtenue en composant Π avec un morphismes de degré 2 au dessus de la sphère, ramifié au dessus des deux faces 0 et l'infini

$$X \mapsto X^2$$

Le dessin correspondant admet un automorphisme non trivial

$$X \mapsto -X$$

Voici ce dessin



On remarque tout de suite que Ψ est définie sur $Q(i)$ et que

$$\bar{\Psi}(X) = \Psi(\frac{\sqrt{A}}{X}) = \Psi \circ K$$

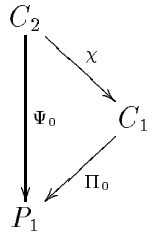
où on a posé

$$K = \begin{bmatrix} 0 & \sqrt{A} \\ 1 & 0 \end{bmatrix}$$

Donc le dessin est rationnel, son corps des modules est Q. Cependant on notera que $\sqrt{A}$ n'est pas rationnel, si bien que le procédé de descente présenté au paragraphe précédent ne fonctionne plus. On devine alors que ce dessin n'admet aucun modèle défini sur $\mathbb{Q}$.

En voici une preuve.

Supposons qu'il existe une courbe C_2 de genre 0 et une fonction de Belyi Ψ_0 sur C_2, toutes deux définies sur Q. Soit C_1 le quotient de C_2 par le groupe d'automorphismes de Psi_0 et χ l'application quotient. On appelle Π_0 l'unique application qui fasse commuter le diagramme suivant.



Alors C_1, χ et Π_0 peuvent être définies sur Q. Ainsi la paire (C_1, Π_0) est un modèle défini sur Q pour le dessin sans automorphismes étudié dans la section précédente. Donc C_1 est isomorphe sur Q à la conique d'équation $x^2 + y^2 + 1 = 0$. On en déduit l'existence d'un revêtement galoisien de degré deux, de cette dernière conique par la courbe C_2, défini sur Q et ramifié au dessus de deux points. La contradiction vient alors du théorème suivant, que l'on démontrera au paragraphe 1.7.1.

Théorème 1.1 *Soient C_1 et C_2 deux courbes de genre 0 et χ un revêtement de C_1 moins deux points par C_2, topologiquement isomorphe à l'application de P_1 dans P_1*

définie par le polynôme $X \to X^e$ où e est un entier naturel. On suppose que C_1, C_2 et χ sont définis sur un corps de nombres K. Alors:

- *Si e est pair, C_1 est isomorphe sur K à P_1.*
- *Si e est impair, C_1 est isomorphe sur K à C_2.*

Dans notre cas, C_1 ne peut être Q-isomorphe à P_1, comme on l'a vu au précédent paragraphe.

On a donc montré le

Fait 1.3 *Le dessin représenté plus haut n'admet pas de modèle défini sur $\mathbb{Q}$.*

On peut finir en énonçant le

Fait 1.4 *Pour tout corps de nombre K_0, les deux conditions suivantes sont équivalentes*

- *Il existe, définie sur K_0, une fonction de Belyi pour le dessin correspondant à Ψ.*
- *L'équation*

$$x^2 + y^2 = -1$$

admet une solution sur K_0 .

1.7 Descente de Weil et courbes de genre 0

Dans cette section on s'intéresse aux dessins de genre 0 et sans automorphismes. Nous verrons le résultat suivant

Fait 1.5 *Un dessin de genre 0 et sans automorphismes admet une fonction de Belyi sur la sphère de Riemann, définie sur une extension au plus quadratique de son corps des modules. Une telle fonction peut être calculée par de simples manipulations polynômiales.*

Ensuite, pour savoir s'il existe une fonction de Belyi à coefficients dans le corps des modules, il suffit de calculer un symbole de Hilbert global. Dans le cas où une telle fonction existe, son calcul se réduit à la résolution d'une équation aux normes de degré 2 sur le corps des modules du dessin.

On a vu que la trivialité du groupe d'automorphismes implique l'existence d'une fonction de Belyi sur une conique. Puisque toute conique est isomorphe à la P_1 sur une extension au plus quadratique de son corps de définition, on en déduit qu'il existe pour ce dessin une fraction rationnelle définie sur une telle extension.

Nous donnons ici une construction explicite de cette fonction de Belyi. D'autre part, cette approche ne nous laisse pas tout a fait sans recours lorsque le dessin admet des automorphismes, comme on le verra dans la section suivante.

On s'intéresse ici exclusivement au problème de descente et donc on suppose connue une fonction de Belyi associée au dessin, ainsi que le corps des modules de ce dessin. On verra comment obtenir tout cela en 1.8.

La suite de cette section consiste en trois parties. Dans la première, nous rappelons quelques faits élémentaires classiques sur les courbes de genre 0. Dans la seconde partie, nous nous intéressons au calcul explicite de bons modèles pour un dessin donné, sans automorphismes. Dans la troisième, nous décrivons quelques techniques utiles à la recherche de points rationnels dans les corps de genre 0.

1.7.1 Une famille rationnelle de coniques à deux points marqués

Soit K un corps de nombres, C une courbe de genre 0 définie sur K et $\{\alpha, \beta\}$ une paire de points, définie sur K. On appelle $K(\sqrt{D})$ l'extension au plus quadratique de K sur laquelle α et β sont des points rationnels. Soit I_1 un isomorphisme de C sur P_1 qui envoie α sur 0 et β sur ∞. Deux tels isomorphismes sont égaux à composition près par une application de la forme $X \to \mathcal{A}X$ où $\mathcal{A} \in \bar{Q}$. On en déduit, à l'aide du théorème 90 de Hilbert, que I_1 peut être définie sur $K(\sqrt{D})$.

Supposons que D n'est pas un carré parfait et faisons agir sur I_1 l'unique automorphisme non trivial de $K(\sqrt{D})/K$. Il existe $A \in K$ tel que

$$\overline{I_1} = A/I_1$$

Soit maintenant $\mathcal{C}$ la conique plane d'équation homogène

$$x^2 - Dy^2 - Az^2 = 0$$

et J_2 l'application de P_1 dans $\mathcal{C}$ définie par

$$J_2([U,V]) = [\sqrt{D}(U^2 + AV^2), AV^2 - U^2, 2UV\sqrt{D}]$$

Alors, si l'on pose $J_2^{(-1)} = I_2$ on a $I_2([x,y,z]) = [x - y\sqrt{D}, z] = [Az, x + y\sqrt{D}]$ et $\overline{I_2} = A/I_2$ si bien que $J = J_2 \circ I_1$ est définie sur K.

De plus, J envoie la paire $\{\alpha, \beta\}$ sur la paire de points à l'infini de $\mathcal{C}$.

On en déduit le

Théorème 1.2 *Toute conique privée de deux points est isomorphe sur son corps de définition K à une courbe affine d'équation $x^2 - Dy^2 - A = 0$.*

De plus, si $D, A_1, A_2 \in K$ la courbe projective d'équation $x^2 - Dy^2 - z^2 = 0$ est isomorphe à P_1 sur K, et si le quotient A_1/A_2 est une norme dans $K(\sqrt{D})$, alors les courbes affines d'équations $x^2 - Dy^2 - A_1 = 0$ et $x^2 - Dy^2 - A_2 = 0$ sont isomorphes sur K.

Une première conséquence de ceci est que tout dessin de genre 0, sans automorphisme, admet sur son corps des modules K, une fonction de Belyi définie sur une conique d'équation $x^2 - Dy^2 - Az^2 = 0$ ou bien encore une fonction de Belyi φ de P_1 dans P_1 définie sur $K(\sqrt{D})$ et satisfaisant $\overline{\varphi} = A/\varphi$, avec $A, D \in K$.

Nous donnons maintenant une preuve du théorème 1.1.

On peut supposer que les deux courbes C_1 et C_2 ont pour équations respectives $x^2 - D_1y^2 - A_1z^2 = 0$ et $x^2 - D_2y^2 - A_2z^2 = 0$ que les points singuliers de χ sont les points à l'infini de C_2; et qu'ils sont envoyés par χ sur les points à l'infini de C_1.

Appelons I_1 l'application de C_1 dans P_1 définie par $I_1([x,y,z]) = [x - y\sqrt{D_1}, z] = [A_1 z, x + y\sqrt{D_1}]$ et de même I_2. Notons que l' application I_1 (respectivement I_2) est définie sur K ou sur une extension quadratique de K. Dans ce dernier cas, elle a pour conjuguée A_1/I_1 (respectivement A_2/I_2). Soit alors ζ l'unique application qui fait commuter le diagramme suivant

$$\begin{array}{ccc} C_2 & \xrightarrow{I_2} & P_1 \\ {\scriptstyle \chi}\downarrow & & \downarrow{\scriptstyle \zeta} \\ C_1 & \xrightarrow{I_1} & P_1 \end{array}$$

On voit que ζ est ramifiée au dessus de 0 et ∞ elle est donc de la forme $\zeta(X) = \theta X^e$ ou $\zeta(X) = \theta / X^e$ avec $e \neq 0$ et $\theta \neq 0$. Notons que si C_1 et C_2 sont K-isomorphes à P_1, alors le théorème est démontré. On peut donc supposer que l'une au moins des deux applications I_1 et I_2 n'est pas définie sur K. Ainsi, quitte à remplacer I_1 ou I_2 par sa conjuguée, on peut toujours supposer que ζ est de la forme $\zeta(X) = \theta X^e$.

On en déduit que $\sqrt{D_1}$ et $\sqrt{D_2}$ engendrent le même corps. En effet, dans le cas contraire, considérons σ l'automorphisme tel que ${}^\sigma\sqrt{D_1} = \sqrt{D_1}$ et ${}^\sigma\sqrt{D_2} = -\sqrt{D_2}$. On trouve alors, en faisant agir σ sur le diagramme commutatif ci-dessus que ${}^\sigma\zeta(X) = {}^\sigma\theta X^e = \theta A_2^e / X^e$, ce qui n'est pas possible.

Ainsi, $\sqrt{D_1}$ et $\sqrt{D_2}$ engendrent le même corps. Soit donc σ l'automorphisme non trivial de $K(\sqrt{D_1})/K$. En faisant agir σ sur le diagramme commutatif on obtient la relation

$${}^\sigma\theta\theta = \frac{A_1}{A_2^e}$$

Si e est pair, on obtient que A_1 est une norme sur $K(\sqrt{D_1})$ et donc que C_1 est K-isomorphe à P_1.

Si e est impair, on obtient que A_1/A_2 est une norme sur $K(\sqrt{D_1})$ et donc que C_1 est K-isomorphe à C_2. CQFD.

1.7.2 Descente de Weil pour les fonctions de Belyi

Venons en à la deuxième partie de notre exposition. Nous voulons, pour tout dessin $\mathcal{D}$ sans automorphismes, trouver une fonction de Belyi sur la sphère de Riemann à coefficients sur le corps des modules K de $\mathcal{D}$, ou bien une fonction de Belyi sur la sphère de Riemann à coefficients sur une extension quadratique de K.

Supposons connus le corps des modules K du dessin et une famille de fonctions de Belyi conjuguées φ_i pour $1 \leq i \leq e$ définies sur des extensions L_i de degré e de K.

Nous verrons en 1.8 comment les obtenir.

Pour i et j compris entre 1 et e, φ_i et φ_j définissent le même dessin et il existe donc une homographie $T_{j,i}$ telle que

$$\varphi_i = \varphi_j \circ T_{j,i}$$

Comme le dessin n'admet pas d'automorphismes, les $T_{j,i}$ sont uniques et doivent donc vérifier les deux familles de conditions :

$$\begin{aligned} T_{k,j}T_{j,i} &= T_{k,i} \\ T_{j,i}^{\sigma} &= T_{\sigma(j),\sigma(i)} \text{ pour tout } \sigma \text{ dans } Gal(\bar{L}/K) \end{aligned}$$

On utilise alors le critère de Weil et la construction donnée dans [45] pour construire un modèle rationnel associé à ce dessin.

Théorème 1.3 ***(Critère de Weil)*** *Soit K un corps de nombres et L une extension algébrique de K. Soit $\bar{K}$ une clôture algébrique de K, et Θ l'ensemble des injections de L dans $\bar{K}$ qui fixent K.*

Soit V une variété projective (resp. affine) définie sur L. Pour tout $\sigma \in \Theta$ on note ${}^{\sigma}V$ la variété obtenue par action de σ sur V. On suppose qu'il existe, pour tout $\sigma, \tau \in \Theta$ un isomorphisme $T_{\tau,\sigma}$ de ${}^{\sigma}V$ dans ${}^{\tau}V$ et que ces divers isomorphismes satisfont les deux familles de conditions suivantes

$$\begin{aligned} T_{\nu,\tau}T_{\tau,\sigma} &= T_{\nu,\sigma} \\ T_{\tau,\sigma}^{\nu} &= T_{\nu\tau,\nu\sigma} \textit{ pour tout } \sigma,\tau,\nu \textit{ dans } Gal(\bar{L}/K) \end{aligned}$$

Alors, il existe une variété projective (resp. affine) V_0 définie sur K et un isomorphisme T de V_0 dans V tels que $T_{\tau,\sigma} = {}^{\tau}T^{\sigma}T^{-1}$.

On reprend ici la construction de Weil dans le cas particulier d'une courbe de genre 0.

Soit $B_1 = (\alpha_{1,k})_k$ une base de L_1 sur K. Les conjuguées de B_1 sont appelées B_i et sont des bases des L_i pour $1 \leq i \leq e$. On note $B_i = (\alpha_{i,k})_k$. Soient maintenant $(\delta_i)_{1\leq i\leq e}$ les fonctions coordonnées de l'espace affine A_e de dimension e.

Si l'homographie $T_{j,i}$ est donnée par la matrice

$$T_{j,i} = \begin{bmatrix} a_{j,i} & b_{j,i} \\ c_{j,i} & d_{j,i} \end{bmatrix}$$

on considère dans A_e la variété définie par le système d'équations $(E_{i,j})_{1\leq i<j\leq e}$

$$c_{j,i}\sum_k \alpha_{i,k}\delta_k \sum_k \alpha_{j,k}\delta_k + d_{j,i}\sum_k \alpha_{j,k}\delta_k - a_{j,i}\sum_k \alpha_{i,k}\delta_k - b_{j,i} = 0$$

L'ensemble des équations $E_{i,j}$ forme un système qui définit une courbe $\mathcal{C}_0$ définie sur K et $\bar{K}$-isomorphe à P_1 par l'application ζ telle que

$$X_1 = \zeta(\delta_1, ..., \delta_e) = \sum_k \alpha_{1,k}\delta_k$$

L'application réciproque se construit en inversant la matrice B formée de tous les B_i. En effet B est inversible par indépendance des automorphismes.

Il est clair alors que la fonction de Belyi $\varphi_0 = \varphi_1 \circ \zeta$ est définie sur K.

On voit en outre que $\mathcal{C}_0$ se présente comme une intersection de quadriques *définies sur* K (penser à décomposer les équations $E_{i,j}$ comme sommes d'équations définies sur K). Il reste à construire un K-isomorphisme entre $\mathcal{C}_0$ et une conique plane définie sur K. Une telle conique est alors isomorphe à P_1 sur une extension au plus quadratique de K.

1.7.3 Trivialisation des cocycles de $PGL(2,\bar{Q})$

Le modèle rationnel construit au paragraphe précédent présente l'inconvénient d'être plongé dans un espace affine de dimension élevée. On sait bien que toute courbe de genre 0 est isomorphe à une conique sur son corps de définition, mais la construction d'un tel isomorphisme n'est pas des plus aisées. De plus, dans le cas particulier où le dessin admet une famille de ramification de cardinalité impaire (par exemple, un nombre impair de points au dessus de 0 avec un ordre de ramification donné), on sait que le dessin admet un modèle sur P_1 car toute conique admettant un diviseur de degré impair est isomorphe à P_1 sur son corps de définition. On aimerait alors construire ce modèle rationnel sur la droite.

Soit donc $\varphi : P_1 \to P_1$ une fonction de Belyi définie sur une extension L du corps des modules K. Soit G le groupe de Galois de $\bar{L}/K$. Pour tout $\sigma \in G$ il existe H_σ une homographie unique telle que ${}^\sigma\varphi = \varphi H_\sigma$, et les H_σ forment un cocycle.

On suppose que $\varphi(\infty) \notin \{0, 1, \infty\}$. On appelle $P_i(X)$ pour $i \geq 1$ le polynôme unitaire dont les racines sont les points au dessus de 0 où la ramification est i. On définit de même $Q_i(X)$ et $R_i(X)$ avec les points au dessus de 1 et ∞ de ramification i.

Tous ces polynômes sont définis sur L. On cherche une fraction rationnelle définie comme combinaison multiplicative de ces polynômes et de degré négatif aussi grand que possible. D'après le théorème de Riemann-Hurwitz, il existe une telle fonction de degré -2. Dans le cas où il existe une famille (un polynôme parmi les P_i, Q_i, R_i) de cardinalité impaire, alors il existe une telle fonction de degré -1.

Appelons ψ une telle fonction, et $\mathcal{K}$ le diviseur associé. Le diviseur $\mathcal{K}$ vérifie

$$ {}^\sigma\mathcal{K} = H_\sigma^{-1}(\mathcal{K}) $$

On peut donc identifier les espaces linéaires correspondant aux différents conjugués en composant par les H_σ.

$$ \mathcal{L}(\mathcal{K}) \xrightarrow{T_\sigma} \mathcal{L}({}^\sigma\mathcal{K}) $$

$$ f \longmapsto f \circ H_\sigma $$

Le cocycle H_σ se relève alors en un cocycle $\tilde{H}_\sigma$ à valeurs dans $GL(\mathcal{L}(\mathcal{K}))$ défini de la façon suivante.

Soit $\mathcal{B} = (\psi, X\psi, X^2\psi)$ (respectivement $\mathcal{B} = (\psi, X\psi)$) une base de $\mathcal{L}(\mathcal{K})$. Pour $v = (v_1, v_2, v_3)$ (respectivement $v = (v_1, v_2)$) un vecteur à coordonnées dans $\bar{Q}$, on note f_v la fonction définie par $f_v = (v_1 + v_2X + v_3X^2)\psi$ (respectivement $f_v = (v_1 + v_2X)\psi$).

Pour $\sigma \in G$ on pose

${}^\sigma f_v = ({}^\sigma v_1 + {}^\sigma v_2 X + {}^\sigma v_3 X^2){}^\sigma\psi$, ce qui définit une autre application

$$ \mathcal{L}(\mathcal{K}) \xrightarrow{U_\sigma} \mathcal{L}({}^\sigma\mathcal{K}) $$

$$ f \longmapsto {}^\sigma f $$

On s'intéresse à la composée $T_\sigma^{-1}U_\sigma$. Il existe un élément unique $\tilde{H}_\sigma$ de $GL(\mathcal{L}(\mathcal{K}))$ tel que

$$f_{\tilde{H}_\sigma({}^\sigma v)} \circ H_\sigma = {}^\sigma f_v$$

soit encore

$$\mathcal{L}(\mathcal{K}) \xrightarrow{T_\sigma^{-1} U_\sigma} \mathcal{L}(\mathcal{K})$$

$$f_v \longmapsto f_{\tilde{H}_\sigma({}^\sigma v)}$$

Les $\tilde{H}_\sigma$ forment un cocycle à valeurs dans $GL(\mathcal{L}(\mathcal{K}))$.

Par exemple, si le degré de ψ est -2 et si H_σ est représentée par la matrice

$$H_\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

alors $\tilde{H}_\sigma$ est donné par

$$\tilde{H}_\sigma^{-1} = \begin{bmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{bmatrix} \psi(\frac{a}{c}).\frac{1}{c^2}$$

Puisque le $H^1(Gal(\bar{Q}/K), GL(\mathcal{L}(\mathcal{K})))$ est trivial, il existe $M \in \mathcal{L}(\mathcal{K})$ tel que $\tilde{H}_\sigma = M {}^\sigma M^{-1}$. Ce M se calcule explicitement comme série de Poincaré ([41] page 159, par exemple). On a alors pour tout v à coefficients rationnels

$${}^\sigma(f_{Mv}) = f_{Mv} H_\sigma$$

Soit maintenant v un vecteur à coefficients dans Q et $w = (w_1, w_2, w_3) = Mv$. On demande que $w_2^2 - 4w_1w_3 \neq 0$, ce qui est vérifié pour presque tout v.

Appelons α et β les racines de $w_1 + w_2X + w_3X^2$. Alors, l'ensemble $\{\alpha, \beta\}$ formé de ces deux racines vérifie

$${}^\sigma\{\alpha, \beta\} = H_\sigma^{-1}\{\alpha, \beta\}$$

En particulier, il existe une extension de K au plus quadratique telle que pour tout $\sigma \in Gal(\bar{Q}/K(\sqrt{D}))$

$${}^\sigma\alpha = H_\sigma^{-1}\alpha \text{ et } {}^\sigma\beta = H_\sigma^{-1}\beta$$

Soit alors S une homographie telle que $S(\infty) = \alpha$ et $S(0) = \beta$. Si nous posons $\varphi_1 = \varphi S$, on a ${}^\sigma\varphi_1 = \varphi_1 T_\sigma$ avec $T_\sigma = S^{-1} H_\sigma {}^\sigma S$. Et T_σ vérifie $T_\sigma(0) = 0$ et $T_\sigma(\infty) = \infty$. Ainsi $T_\sigma(X) = t_\sigma X$ où t_σ est un 1-cocycle scalaire et donc par le théorème 90 de Hilbert $t_\sigma = \lambda {}^\sigma\lambda^{-1}$. On pose alors $\varphi_2(X) = \varphi_1(\lambda X)$ et on obtient une fonction de Belyi définie sur $K(\sqrt{D})$ telle que ${}^\tau\varphi_2 = A/\varphi_2$ avec A une constante dans K et τ l'unique automorphisme non trivial de $K(\sqrt{D})/K$. Nous avons de aussi calculé une extension quadratique sur laquelle le cocycle H_σ se trivialise :

$$H_\sigma = {}^\sigma(\lambda S)(\lambda S)^{-1}$$

pour $\sigma \in Gal(\bar{Q}/K(\sqrt{D}))$.

On se trouve alors dans la situation de la section 1.5 et l'on sait construire un modèle rationnel sur la conique d'équation $x^2 - Dy^2 - Az^2 = 0$. On peut chercher à savoir si cette conique est isomorphe sur K à P_1. L'existence sur un corps K d'une solution à l'équation $x^2 - Dy^2 - Az^2 = 0$ s'exprime avec le symbole de Hilbert global sur K noté $(D, A)_K$. Ce symbole est la conjonction des symboles locaux en les places finies qui divisent $2AD$ et en les places à l'infini. Il est donc très facile à calculer. Il est plus difficile de trouver une solution explicite à l'équation $x^2 - Dy^2 - Az^2 = 0$ (voir [31]).

Remarquons que dans le cas où le degré de ψ est -1, le calcul décrit plus haut conduit non pas à des paires rationnelles de points mais à des points rationnels, parce que la dimension de $\mathcal{L}(\mathcal{K})$ est 2. Le cocycle se trivialise alors directement sur le corps K lui même.

Remarque

Il n'est pas nécessaire de calculer la clôture de Galois du corps L pour mener tous ces calculs. Le plus simple est de travailler en notation flottante. En effet, on connaît les conjuguées de toutes les grandeurs qui apparaissent, puisqu'elles proviennent de la famille initiale de fonctions de Belyi conjuguées, c'est à dire des H_σ.

1.8 Dessins dont le groupe d'automorphismes est quelconque

1.8.1 Monodromie d'un dessin et calcul du groupe d'automorphismes, dessin réduit

Si $\varphi : \mathcal{C} \to P_1$ est une fonction de Belyi de genre quelconque associée au dessin $\mathcal{D}$, on appelle "drapeaux" les composantes connexes de l'image réciproque par φ du segment ouvert $(0, 1)$. On définit trois permutations de ces drapeaux σ_0, σ_1, σ_∞ de la façon suivante : σ_0 fait tourner les drapeaux autour des sommets, dans le sens positif. De même σ_1 fait tourner les drapeaux autour des cotés, et σ_∞ autour des faces. On a alors $\sigma_\infty\sigma_1\sigma_0 = 1$ et le groupe engendré par ces trois permutations est isomorphe au groupe de Galois $\mathcal{G}$ de la clôture galoisienne de l'extension associée au morphisme φ. Appelons $\mathcal{H}$ le stabilisateur d'un drapeau f arbitraire dans $\mathcal{G}$, alors le groupe d'automorphismes du revêtement est le quotient par $\mathcal{H}$ de son normalisateur dans $\mathcal{G}$

$$\mathfrak{A} = \mathcal{N}_\mathcal{G}(\mathcal{H})/\mathcal{H}$$

et ce dernier groupe est isomorphe au centralisateur de $\mathcal{G}$ dans le groupe complet de permutations S_N où N est le degré du dessin :

$$\mathfrak{A} = \mathcal{Z}_{S_N}(\mathcal{G})$$

En effet, à chaque élément a de $\mathcal{N}_\mathcal{G}(\mathcal{H})/\mathcal{H}$ on associe l'unique élément $\tilde{a}$ de $\mathcal{Z}_{S_N}(\mathcal{G})$ tel que $\tilde{a}(f) = a(f)$.

Cela donne une description combinatoire de ce groupe d'automorphismes ainsi qu'un moyen de le calculer. En particulier, si $\tilde{a} \in \mathcal{Z}_{S_N}(\mathcal{G})$, alors $\tilde{a}$ commute aux σ_i et donc il induit une permutation de leurs cycles qui décrit l'action de l'automorphisme correspondant sur les points de ramification.

Par ailleurs si $(\mathcal{C}, \varphi)$ est définie sur un corps de nombres L , alors il existe une courbe $\mathcal{C}_0$, une application rationnelle $\varphi_0 : \mathcal{C}_0 \to P_1$ et un revêtement géométriquement galoisien de groupe $\mathfrak{A}$, $\chi : \mathcal{C} \to \mathcal{C}_0 - \varphi_0^{-1}(\{0, 1, \infty\})$ tous définis sur L et tels que $\varphi = \varphi_0 \circ \chi$.

Remarque: nous disons qu'un revêtement de courbe algébrique est géométriquement Galoisien si l'extension de corps de fonctions associée est Galoisienne moyennant une extension algébrique du corps des scalaires.

Le dessin $\mathcal{D}_0$ associé à φ_0 est appelé dessin réduit du dessin initial. On voit que tout corps de définition du dessin initial est aussi corps de définition du dessin réduit.

En fait, le corps des modules du dessin réduit est inclus dans le corps des modules du dessin initial. En effet, si K est le corps des modules du dessin initial, soit $\sigma \in Gal(\bar{Q}/K)$. Alors, il existe un isomorphisme $H_\sigma : {}^\sigma\mathcal{C} \to \mathcal{C}$ défini sur $\bar{Q}$ tel que ${}^\sigma\varphi = \varphi H_\sigma$. Il existe donc un unique morphisme $h_\sigma : {}^\sigma\mathcal{C}_0 \to \mathcal{C}_0$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} \mathcal{C} & \xleftarrow{H_\sigma} & {}^\sigma\mathcal{C} \\ {\scriptstyle\chi}\downarrow & & \downarrow{\scriptstyle{}^\sigma\chi} \\ \mathcal{C}_0 & \xleftarrow{h_\sigma} & {}^\sigma\mathcal{C}_0 \end{array}$$

Ceci prouve que le corps des modules du dessin réduit est un sous-corps du corps des modules du dessin initial. En fait on a mieux.

Puisque chaque h_σ est unique et ne depend que de H_σ, la famille des h_σ vérifie la condition de cocycle sur $Gal(\bar{Q}/K)$. Ainsi, le dessin réduit $\mathcal{D}_0$ admet un modèle sur K. La classe de K-isomorphisme de ce modèle est uniquement déterminée par le dessin $\mathcal{D}$. On la note $\mathcal{D}_0^{\mathcal{D}}$ et on l'appelle modèle réduit de $\mathcal{D}$. Noter que le dessin $\mathcal{D}_0$ peut avoir lui même des automorphismes, si bien qu'il peut admettre plusieurs K-modèles non K-isomorphes. Néanmoins, vu comme dessin réduit de $\mathcal{D}$, le dessin $\mathcal{D}_0$ admet un modèle canonique sur K.

Pour toute extension M de K, on dit que le modèle réduit $\mathcal{D}_0^{\mathcal{D}}$ a un point non singulier rationnel sur M si et seulement s'il existe une valeur non singulière de χ, $\alpha \in \mathcal{C}_0$ telle que $h_\sigma({}^\sigma\alpha) = \alpha$ pour tout $\sigma \in Gal(\bar{Q}/M)$.

Soit alors un point β sur $\mathcal{C}$ tel que $\chi(\beta) = \alpha$ et "ajustons" les H_σ de telle sorte que

$$H_\sigma({}^\sigma\beta) = \beta$$

pour $\sigma \in Gal(\bar{Q}/M)$.

Cela est toujours possible de manière unique parce que le morphisme χ est géométriquement galoisien. Les H_σ ainsi obtenus forment un cocycle, qui admet lui aussi un point rationnel. Donc, le dessin $\mathcal{D}$ admet un modèle sur le corps M, muni lui aussi d'un point rationnel β.

Théorème 1.4 *Le corps des modules K d'un dessin $\mathcal{D}$ est un corps de définition de son dessin réduit $\mathcal{D}_0$. Si le modèle réduit correspondant $\mathcal{D}_0^{\mathcal{D}} = (\mathcal{C}_0, h_\sigma)$ a un point non singulier rationnel sur une extension M de K, alors M est un corps de définition de $\mathcal{D}$ et il existe un modèle M-rationnel pour $\mathcal{D}$ avec un point régulier M-rationnel.*

Corollaire 1.1 – *Tout corps de définition d'un dessin est corps de définition de son dessin réduit.*

– *Le corps des modules du dessin réduit est inclus dans le corps des modules du dessin lui même.*

Examinons maintenant le cas d'un dessin de genre 0. Soit $K(\sqrt{D})$ une extension au plus quadratique de K sur laquelle le cocycle h_σ se trivialise.

$\mathcal{D}_0^{\mathcal{D}}$ a alors une infinité de points $K(\sqrt{D})$-rationnels, la plupart non singuliers. Appliquant la troisième partie du théorème 1.4 on en déduit le

Théorème 1.5 *Tout dessin de genre* 0 *admet un modèle* $\phi : P_1 \to P_1$ *défini sur une extension au plus quadratique de son corps des modules.*

On a mieux encore. Soit $\mathcal{S}$ l'ensemble des valeurs singulières de χ. Cet ensemble vérifie la condition

$$h_\sigma({}^\sigma\mathcal{S}) = S$$

et donc si sa cardinalité est impaire, le cocycle formé par les h_σ est dans la classe triviale (sur K) et admet donc une infinité de points K-rationnels. Or, on va voir que tout revêtement fini géométriquement galoisien de genre 0 de la sphère, non cyclique, a 3 valeurs singulières (i.e. est ramifié au dessus de 3 points exactement). On en déduit le

Théorème 1.6 *Tout dessin de genre* 0 *et de groupe d'automorphismes non cyclique et non trivial, admet un modèle* $\phi : P_1 \to P_1$ *défini sur son corps des modules.*

Il nous reste seulement à énoncer le résultat classique suivant (voir [2] page 106)

Théorème 1.7 *Tout revêtement géométriquement galoisien de genre* 0 *de la sphère a pour groupe de Galois géométrique un groupe cyclique, dièdral ou bien l'un des trois groupes suivants:*

– A_4 *le groupe de symétrie du tetraèdre.*

– S_4 *le groupe de symétrie de l'octaèdre.*

– A_5 *le groupe de symétrie de l'icosaèdre.*

Le nombre de valeurs singulières est 2 *si le groupe de Galois est cyclique, et* 3 *sinon.*

Par exemple les applications $X \to X^n$ et $X \to X^n + X^{-n}$ ont pour groupes de Galois C_n et D_n respectivement.

Dans la section suivante nous allons examiner comment obtenir les modèles rationnels ci-dessus.

1.8.2 Normalisation de fractions rationnelles

Nous généralisons le procédé de normalisation déjà utilisé pour les arbres.

Soit

$$\varphi(X) = \frac{N(X)}{D(X)} = \frac{X^F + f_1 X^{F-1} + f_2 X^{F-2} + ... + f_F}{g_0 X^G + g_1 X^{G-1} + g_2 X^{G-2} + ... + g_G}$$

une fraction rationnelle. On suppose que $G \geq 1$ et $g_0 \neq 0$. Si l'on remplace X par AX pour $A \in C$ et que l'on met la fraction obtenue sous la forme ci-dessus, alors f_1 est multipliée par A^{-1}. On dit que f_1 est homogène de degré -1. De même f_i est de degré $-i$ et g_i est degré $G - F - i$.

Soit e l'ordre du groupe des automorphismes de φ qui fixent 0 et ∞. Alors $F - G$ est un multiple de e car c'est la ramification en l'infini. En fait, e est le pgcd de tous les entiers k tels qu'il existe une fonction de degré k non nulle parmi les f_i et les g_i.

En particulier, il existe une combinaison non nulle et de degré e de la forme

$$\mathcal{S} = \prod_{i \geq 0} {f_i}^{\mu_i} {g_i}^{\nu_i}$$

où les $(\mu_i)_i$ et les $(\nu_i)_i$ sont à valeurs dans Z et à supports finis.

Si une fonction de Belyi φ satisfait les trois conditions suivantes:

- $\varphi(\infty) \in \{0, 1, \infty\}$
- $g_1 = 0$
- $\mathcal{S} = 1$ pour un $\mathcal{S}$ donné comme ci-dessus.

alors on dira qu'elle est normalisée.

Il est clair que si σ est dans le groupe des modules du dessin, alors ${}^{\sigma}\varphi$ est encore une fonction de Belyi normalisée pour ce dessin. La normalisation est conservée.

On a mieux:

Définition 1.1 *Soit φ une fonction de Belyi et α un point de ramification de φ. Le type de α est le triplet $\mathcal{T}(\alpha) = (\varphi(\alpha), r, e)$ où r est le degré de ramification de φ en α et e est l'ordre du sous groupe des automorphismes du dessin qui fixent α.*

Si φ est une fonction de Belyi normalisée, on définit son type comme celui de son point à l'infini.

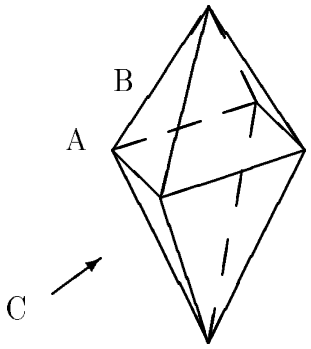
Il est clair que le type est invariant par action de Galois.

Soient maintenant φ_1 et φ_2 deux fonctions de Belyi normalisées par les mêmes conditions et associées à un dessin donné. Il existe donc une homographie H telle que $\varphi_2 = \varphi_1 H$. Supposons de plus que les points à l'infini de ces deux fonctions se correspondent par un automorphisme du dessin. Alors H peut être choisie telle que $H(\infty) = \infty$. On voit alors que les conditions $g_1 = 0$ et $\mathcal{S} = 1$ implique que H est l'identité.

Ainsi, le nombre de fonctions de Belyi d'un type donné et normalisées par un ensemble donné de conditions, est borné par le nombre de points du type considéré, dans le dessin, *à automorphisme près*. En particulier, une telle fonction de Belyi est définie sur une extension du corps des modules, de degré inférieur à ce nombre.

Exemple

L'octaèdre



Ce dessin admet 3 fonctions de Belyi normalisées correspondant aux points A, B, C. Elles sont toutes définies sur son corps des modules car le groupe d'automorphismes agit transitivement sur les sommets, sur les arêtes et sur les faces.

Application: calcul du corps des modules d'un dessin

La donnée d'une famille de fonctions de Belyi normalisées permet de calculer le corps des modules du dessin. En effet, si les $(\varphi_i)_{1\leq i\leq I}$ sont l'ensemble des fonctions de Belyi conjuguées par action de Galois à φ_1, alors le corps K des modules du dessin est l'intersection des corps de définition K_i de ces fonctions.

Soit $(c_{1,j})_{1\leq j\leq J}$ un vecteur formé de l'ensemble des coefficients de φ_1, et de même, soient $(c_{i,j})_{1\leq j\leq J}$ pour $1 \leq i \leq I$ les vecteurs formés des coefficients des

$$(\varphi_i)_{1\leq i\leq I}$$

Ces vecteurs sont conjugués au dessus de K.

Appelons $\sigma_{i,j}$ la i-ème fonction symétrique de la famille $(c_{1,j}, c_{2,j}, ..., c_{I,j})$. Les $\sigma_{i,j}$ sont dans K. Soit maintenant M un polynôme en J variables tel que M appliqué à $(c_{1,j})_{1\leq j\leq J}$ donne un générateur M_1 du corps de définition L_1 de φ_1. Définissons alors les M_i comme les valeurs de M appliqué aux $(c_{i,j})_{1\leq j\leq J}$ pour $1 \leq i \leq I$. Alors les fonctions symétriques des M_i engendrent K.

Soit maintenant $\mathfrak{A}$ le groupe d'automorphismes du dessin. C'est l'un des groupes énumérés au théorème 1.7. Soit X l'ensemble des points fixés par un élément non trivial de $\mathfrak{A}$ et faisons agir $\mathfrak{A}$ sur X. Il est bien connu (voir [2] page 106) que le nombre d'orbites est 3 si $\mathfrak{A}$ n'est pas cyclique. Soient $\mathcal{O}_1$, $\mathcal{O}_2$, $\mathcal{O}_3$ ces orbites. Si x_i est un élément de $\mathcal{O}_i$ alors l'ordre du stabilisateur de x_i dans $\mathfrak{A}$ ne dépend que de i. On obtient ainsi trois entiers caractéristiques du groupe $\mathfrak{A}$ et dont les valeurs sont données dans la table suivante:

- 2,2,n pour $n \geq 2$ si le groupe est D_n.
- 2,3,3 si le groupe est A_4.
- 2,3,4 si le groupe est S_4.
- 2,3,5 si le groupe est A_5.

On voit que dans tous les cas, sauf pour D_2, il existe une orbite d'ordre différent des autres. Alors, une fonction de Belyi normalisée obtenue en envoyant à l'infini un point de cette orbite, sera définie sur le corps des modules du dessin.

Reste alors le cas où le groupe d'automorphismes est le groupe de Klein. On obtient trois fonctions de Belyi normalisées correspondant aux trois orbites, et définies sur des extensions du corps des modules de degré au plus trois. En fait, ou bien l'une d'elles au moins est définie sur le corps des modules, ou bien elles sont toutes les trois conjuguées. Dans ce dernier cas, appelons φ_1, φ_2 et φ_3 ces fonctions. Le groupe d'automorphismes de φ_1 est engendré par les deux automorphismes $X \to -X$ et $X \to \alpha^2/X$ où $\alpha \in C$. Ainsi, φ_1 se décompose comme

$$\varphi_1(X) = \Phi_1(\frac{X^2}{\alpha^2} + \frac{\alpha^2}{X^2})$$

On procède alors comme au paragraphe 1.8.1 en calculant un cocycle h_σ pour les Φ_i puis en le relevant en un cocycle pour les φ_i. Ces cocycles se trivialisent alors sur le corps de définition par la méthode exposée en 1.7.3. Ici, le diviseur fixé par le cocycle h_σ est l'ensemble $\{-2, 2, \infty\}$ des valeurs singulières du revêtement défini par $X \mapsto \frac{X^2}{\alpha^2} + \frac{\alpha^2}{X^2}$.

Cela résout la question de la recherche des fonctions de Belyi dans le cas où le groupe d'automorphismes est non cyclique.

1.8.3 Groupes cycliques d'automorphismes

On note que dans le cas cyclique d'ordre e, il n'y a que deux points fixes d'automorphismes et la normalisation décrite plus haut conduit à envoyer l'un en 0 et l'autre à l'infini. Si les types de ces orbites sont distincts, alors les deux fonctions de Belyi normalisées correspondantes sont définies sur le corps des modules du dessin. Si les deux types sont égaux, alors au pire, les deux fonctions de Belyi sont définies sur la même extension quadratique du corps des modules du dessin et elles sont conjuguées.

Regardons plus en détail comment se pose alors le problème de la descente.

On vient de calculer deux fonctions de Belyi Ψ et $\bar{\Psi}$ définies sur une extension $K(\sqrt{D})$ du corps des modules du dessin. On voit sans peine qu'il existe deux nombres A et B tels que $B^e = A \in K$ et

$$\bar{\Psi}(X) = \Psi(B/X)$$

De plus, $\Psi(X) = \Pi(X^e)$ où Π est une fraction rationnelle définie sur $K(\sqrt{D})$.

Si $e = 2f + 1$ est impair, alors posons $\Psi_0(X) = \Psi(B^{f+1}X)$. On voit alors que $\bar{\Psi}_0(X) = \Psi_0(A^{-1}/X)$. Ainsi, le dessin admet un modèle rationnel sur la courbe d'équation $x^2 - Dy^2 - A^{-1}z^2 = 0$. On le construit comme au paragraphe 1.7.1.

Théorème 1.8 *Un dessin de genre zéro dont le groupe d'automorphismes est cyclique d'ordre impair admet un modèle sur son corps des modules.*

Si $e = 2f$, il peut y avoir une obstruction à l'existence d'un modèle rationnel pour le dessin. Dans le cas particulier du paragraphe 1.6, le dessin "réduit" défini par Π n'a pas d'automorphisme. Alors, l'obstruction est mesurée par un symbole de Hilbert : le dessin a un modèle rationnel si et seulement si la classe d'isomorphisme de coniques associée à son dessin réduit est triviale.

1.9 Conclusion

Nous venons de voir que tout dessin de genre 0 admet un modèle sur son corps des modules pourvu que son groupe d'automorphismes ne soit pas cyclique d'ordre pair. En fait, si le groupe d'automorphismes n'est pas cyclique, le modèle peut être choisi sur P_1. Si le groupe d'automorphismes est cyclique d'ordre impair, et en particulier s'il est trivial, le dessin admet un modèle sur une conique. Nous en avons donné des exemples.

Tous ces résultats demeurent valables pour un revêtement connexe, fini, de genre 0 de la sphère, ramifié au dessus d'un ensemble rationnel. Les preuves et les procédés de construction sont les mêmes.

1.10 Calculs et résultats

Nous décrivons maintenant la conduite des calculs sous Maple pour la fonction de Belyi de la formule (1.11).

On note

$$Q(X) = X^{12} + q_{11}X^{11} + ... + q_1X + q_0$$

$$\Theta_1 = x^3 + r_{1,2}x^2 + r_{1,1}x + r_{1,0} \text{ et } \Theta_{-1} = x^3 + b_{-1,2}x^2 + b_{-1,1}x + b_{-1,0}$$

$$\Theta_3 = x^3 + r_{3,2}x^2 + r_{3,1}x + r_{3,0} \text{ et } \Theta_{-3} = x^3 + b_{-3,2}x^2 + b_{-3,1}x + b_{-3,0}$$

On obtient un premier ensemble d'équations en divisant (1.11) par X^{12} et en dérivant. Les considérations ordinaires de divisibilité donnent alors

$$\widehat{\Theta}_3^2 = XQ' - 6Q$$

Cette relation permet d'éliminer tous les coefficients de Q sauf q_6. En compensation elle donne une équation sur les coefficients de Θ_3 que l'on appelle E_6.

Une conséquence de la bicoloration est que si l'on note $\lambda = \Lambda^2$ alors

$$\Theta_1\Theta_3^3 = Q - \Lambda X^6 \text{ et } \Theta_{-1}\Theta_{-3}^3 = Q + \Lambda X^6$$

On en déduit que le résidu de Q modulo Θ_3^3 est proportionnel à X^6. Ceci donne 8 équations en les coefficients de Θ_3 que l'on appelle $R_0, R_1, R_2, R_3, R_4, R_5, R_7, R_8$. Même chose pour Θ_{-3} et on obtient $B_0, B_1, B_2, B_3, B_4, B_5, B_7, B_8$.

On prend comme dernière condition de normalisation que

$$r_{3,2} + b_{-3,2} = 1$$

Ceci permet d'éliminer $b_{-3,2}$.

Il reste donc 5 inconnues (les coefficients de Θ_3 et Θ_{-3} sauf $b_{-3,2}$.)

On prend donc les 5 équations les moins grosses parmi celles dont on dispose à savoir E_6,R_0,R_8,B_0,B_8.

Malheureusement toutes les tentatives de résolution de ce système par la méthode de Grobner ont échoué.

Mais en factorisant la différence $R_8 - B_8$ j'ai isolé le facteur

$$b_{-3,1} + r_{3,1} = \frac{1}{50}$$

On choisit donc d'adjoindre cette relation au système ce qui permet d'éliminer $r_{3,1}$. Maintenant il ne reste plus que 4 inconnues et Maple ne fait plus de difficultés.

On remarquera que Θ_1, Θ_{-1}, Θ_3, Θ_{-3} ne sont pas définis sur $Q(i)$ mais sur une extension quadratique $Q(i,\sqrt{11})$. Ceci parce que les rouges et les bleus sont exactement symétriques (même répartition des valences). Si on appelle τ l'automorphisme de $Q(i,\sqrt{11})$ tel que $\tau(i) = i$ et $\tau(\sqrt{11}) = -\sqrt{11}$ alors

$$\Theta_{-1} = \Theta_1^\tau \quad \text{et} \quad \Theta_{-3} = \Theta_3^\tau$$

Si l'on note par une étoile la transformation d'une fraction rationnelle à coefficients sur $Q(i)$, telle que

$$F^*(X) = \bar{F}(\frac{A}{X})$$

alors

$$\left(\widehat{\frac{\Theta_1}{x^3}}\right)^* = \zeta\frac{\widehat{\Theta}_1}{x^3} \quad \text{et} \quad \left(\widehat{\frac{\Theta_3}{x^3}}\right)^* = \zeta\frac{\widehat{\Theta}_3}{x^3}$$

où

$$\zeta = \frac{54280 - 42471i}{68921}$$

Comme prévu, la norme de ζ est 1. Et donc $\zeta = \varepsilon/\bar{\varepsilon}$
où

$$\varepsilon = \frac{121i}{275684} - \frac{351}{275684}$$

Donc $\left(\varepsilon x^{-3}\widehat{\Theta}_1\right)^* = \varepsilon x^{-3}\widehat{\Theta}_1$ et $\left(\varepsilon x^{-3}\widehat{\Theta}_3\right)^* = \varepsilon x^{-3}\widehat{\Theta}_3$.
De plus, on remarque que

$$\lambda\zeta^4 = \frac{3^6 11^{11}}{2^{16}5^{12}41^{12}}$$

Et encore

$$\frac{\bar{\lambda}}{\lambda} = \left(\frac{40 - 9i}{41}\right)^{12}$$

Voici les valeurs obtenues pour Θ_1, Θ_3, $\widehat{\Theta}_1$, $\widehat{\Theta}_3$, λ.
On a posé $r = \sqrt{11}$.

$$\begin{aligned}\Theta_1 \;=\; & x^3 + \left(\frac{33\,ir}{410} - \frac{36\,r}{205} + \frac{9}{10}\right)x^2 + \left(\frac{5247\,ir}{168100} - \frac{6831\,r}{84050} + \frac{45273}{168100} - \frac{4356\,i}{42025}\right)x \\ & - \frac{7623\,i}{137842000} + \frac{6669\,r}{137842000} - \frac{22113}{137842000} + \frac{2299\,ir}{137842000}\end{aligned}$$

$$\begin{aligned}
\Theta_3 &= x^3 + \left(\frac{12\,r}{205} - \frac{11\,ir}{410} + 1/2\right)x^2 + \left(\frac{11\,ir}{33620} + \frac{1}{100} + \frac{309\,r}{84050}\right)x \\
&\quad - \frac{351\,r}{137842000} - \frac{1053}{137842000} - \frac{121\,ir}{137842000} - \frac{363\,i}{137842000}
\end{aligned}$$

$$\begin{aligned}
\varepsilon x^{-3}\widehat{\Theta}_1 &= \left(\frac{121\,i}{275684} - \frac{351}{275684}\right)x^3 + \left(\frac{1089\,i}{1378420} - \frac{3159}{1378420}\right)x^2 \\
&\quad + \left(\frac{4719\,i}{13784200} - \frac{19593}{13784200}\right)x \\
&\quad - \frac{1773}{5513680} + \left(\frac{4719\,i}{56515220000} + \frac{19593}{56515220000}\right)x^{-1} \\
&\quad + \left(-\frac{1089\,i}{23171240200000} - \frac{3159}{23171240200000}\right)x^{-2} \\
&\quad + \left(\frac{351}{19000416964000000} + \frac{121\,i}{19000416964000000}\right)x^{-3}
\end{aligned}$$

$$\begin{aligned}
\varepsilon x^{-3}\widehat{\Theta}_3 &= \left(\frac{121\,i}{275684} - \frac{351}{275684}\right)x^3 + \left(\frac{121\,i}{275684} - \frac{351}{275684}\right)x^2 \\
&\quad + \left(\frac{847\,i}{13784200} - \frac{177}{551368}\right)x - \frac{993}{137842000} \\
&\quad + \left(\frac{177}{2260608800} + \frac{847\,i}{56515220000}\right)x^{-1} \\
&\quad + \left(-\frac{351}{4634248040000} - \frac{121\,i}{4634248040000}\right)x^{-2} \\
&\quad + \left(\frac{121\,i}{19000416964000000} + \frac{351}{19000416964000000}\right)x^{-3}
\end{aligned}$$

$$\lambda = \frac{3^9 \cdot 11^{13} \cdot 13 \cdot 23 \cdot 59\,i}{2^6 \cdot 5^{11} \cdot 41^{12}} + \frac{3^6 \cdot 7^2 \cdot 11^{11} \cdot 31 \cdot 241 \cdot 3121}{2^{10} \cdot 5^{12} \cdot 41^{12}}$$

On entreprend maintenant de dessiner sur la conique d'équation affine

$$u^2 + v^2 + \frac{1}{4100} = 0$$

Le morphisme est donc $x = u + iv$, on obtient alors

$$\begin{aligned}
-2^2 41^3 \varepsilon x^{-3}\widehat{\Theta}_1 &= \left(968\,u^2 + \frac{4356\,u}{5} + \frac{387079}{2050}\right)v \\
&\quad + 2808\,u^3 + \frac{12636\,u^2}{5} + \frac{1607679\,u}{2050} + \frac{1823643}{20500}
\end{aligned}$$

$$\begin{aligned}
-2^2 41^3 \varepsilon x^{-3}\widehat{\Theta}_3 &= \left(968\,u^2 + 484\,u + \frac{2783}{82}\right)v \\
&\quad + 2808\,u^3 + 1404\,u^2 + \frac{363903\,u}{2050} + \frac{44223}{20500}
\end{aligned}$$

Chapitre 2

Dessins d'enfants de Grothendieck

Ce chapitre resulte d'une collaboration avec Louis Granboulan et doit beaucoup à son ingéniosité. Bien qu'il fasse l'objet d'une publication commune [13], j'ai pris la liberté de le retranscrire intégralement. Je ne saurais trop remercier Leila Schneps pour le soin qu'elle à mis a relire et corriger ce texte.

In this chapter we study the topological aspects of dessins (via analytic description) with two distinct goals. Firstly we are interested in fields of definition and fields of moduli. We give a topological proof that there exist some dessins with no model defined over their field of moduli. This answers explicitly a question asked in [23]. Our second motivation is to collect practical and theoretical data for the explicit computation of covers given by some topological description, following ideas of Atkin [5] Oesterlé and ourselves. This leads to a method for the computation of the linear space associated to a divisor on a given dessin.

2.1 Introduction

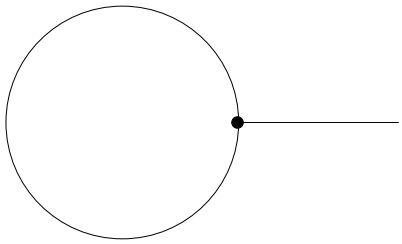
This chapter develops some practical applications of the archimedean analytic description of coverings through Puiseux series. In the second section, we recall a classical result due to Klein concerning the classification of genus zero geometric Galois coverings, and related to the classification of regular polytopes. In the third section we give a review of many possible definitions of what a moduli field is. We do not claim to exhaust the list of various contradictory notions denoted by these words, but simply to avoid the frequent confusion about it. The fourth section is an illustration of what knowledge can be provided by local considerations at infinity. We show that such a study leads to interesting examples of coverings with strange rationality properties, which we can state by mere combinatorial considerations. In the fifth section we recall quite classical results related to the Legendre form of elliptic curves, which are useful in the next section. The sixth section consists in the analytic description of the linear systems associated with some divisors on the curve corresponding to a given dessin. This provides us with an algorithmic correspondance between abstract dessins and explicit Belyi functions. We give quite general techniques. In the case where the genus of the dessin is small, the equations have a simple general form which helps beautifying

the method. We detail that in the seventh section.

We wish to thank Leila Schneps for many useful discussions and for the organization of the Luminy conference in April 1993, where we found the motivation for this work (specially the four talks given by Joseph Oesterlé).

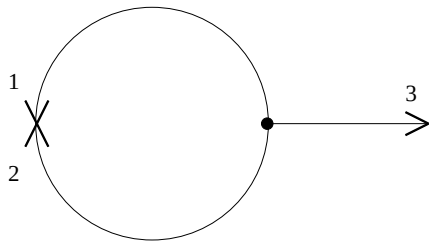
Throughout this chapter we represent the coverings as dessins. For definitions and motivations, the reader should read the article by Leila Schneps in [18], and of course the introduction to this book. There are many possible combinatorial descriptions with such dessins. Let us illustrate this on a small example which we will consider throughout this chapter every time we need to be more explicit. In our drawings, the points over 0 are denoted by a black bullet and the points over 1 correspond to the middles of the segments and to the extremities without bullets (unramified points over 1). This corresponds to Grothendieck's normalization. We ask that the ramification above 1 be equal to 1 or 2.

Let us consider the following genus zero and degree 3 dessin:



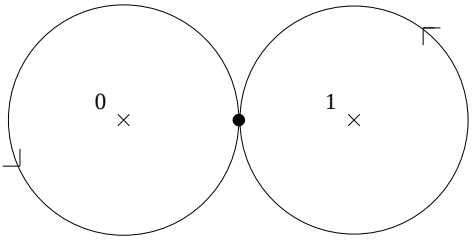
It has one vertex of multiplicity 3, corresponding to the totally ramified point over 0. There is one circular edge, corresponding to a point over 1 with ramification degree equal to 2, and one half-edge the extremity of which is an unramified point over 1. To finish, there are two faces. The inner one is unramified and the outer one is ramified of order 2.

Since the dessin is of degree 3, there are 3 flags that we draw on the following picture



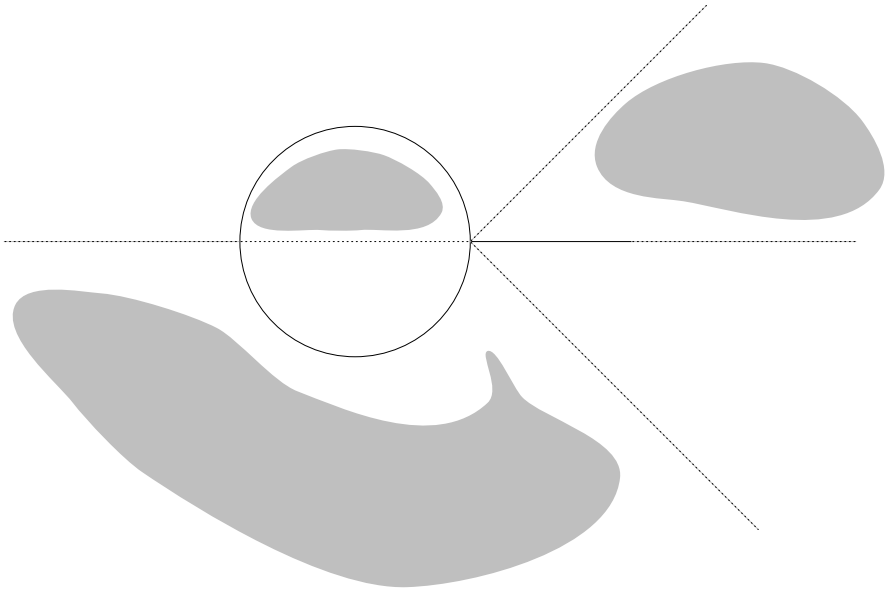
The monodromy of the dessin is given by the following three permutations of the

flags which correspond to the elementary loops around 0, 1 and ∞.



$$\sigma_0 = (1,2,3),\ \ \sigma_1 = (1,2),\ \ \sigma_\infty = (2,3).$$

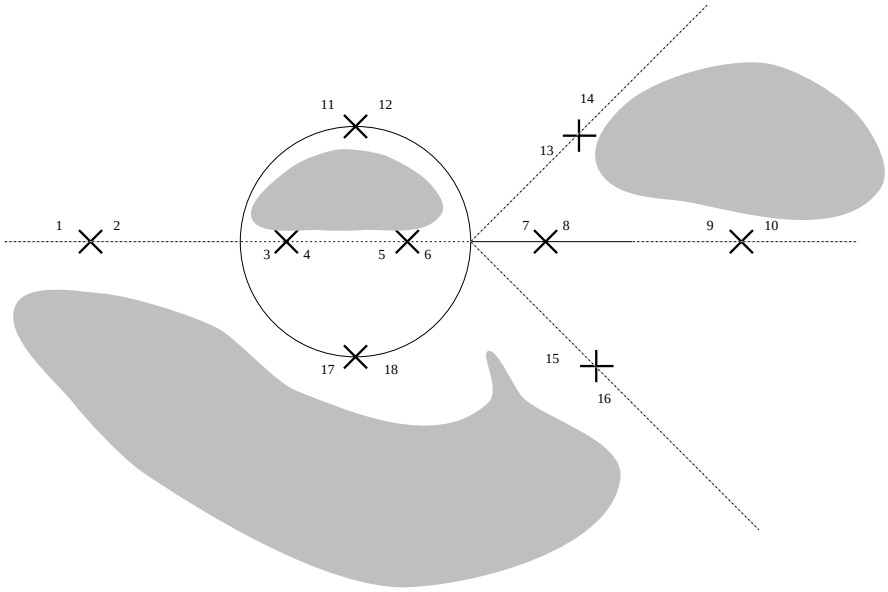
The dessin itself is the preimage of the segment $[0,1]$ under the Belyi function. If we consider rather the preimage of the full real axis, we get a coloured triangulation of the sphere, consisting of three (grey) triangles oriented in the positive direction and sent by the Belyi function onto the upper half plane, and three (white) triangles, oriented in the inverse direction and lying above the lower half plane. This way, the dessin can be considered as a combinatorial covering of coloured triangulations.



We now consider the elementary triangle $0, 1, \infty$ on the Riemann sphere. The middles of the three edges are -1, $1/2$ and 2. This splits the real axis into six open segments plus three points. The six open segments are called *standards* and we give each of them a name which will become clearer later. The segment $(0, 1/2)$ is denoted by $0\vec{1}$; the segment $(1/2, 1)$ is denoted by $1\vec{0}$, the segment $(1, 2)$ is denoted by $1\vec{\infty}$, the segment $(2, \infty)$ is denoted by $\infty\vec{1}$, the segment $(\infty, -1)$ is denoted by $\infty\vec{0}$ and the segment $(-1, 0)$ is denoted by $0\vec{\infty}$.

The preimages of these six standards under the Belyi function give 3×6 standards on the dessin. We draw these standards as little arrows and give an arbitrary number

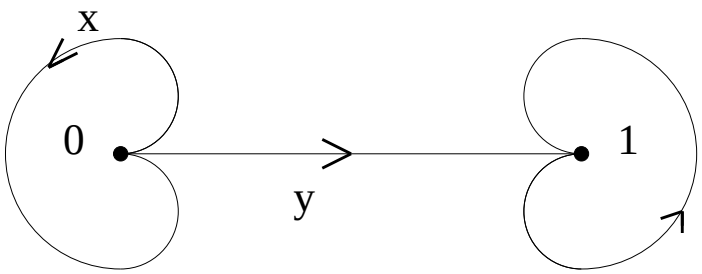
to each of them.



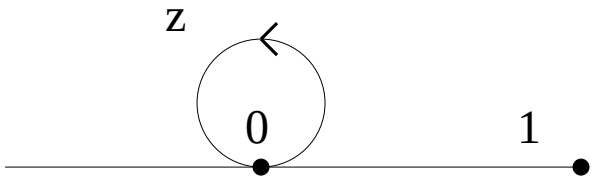
The standards above $0\vec{1}$ are $\{7, 12, 18\}$, the standards above $1\vec{0}$ are $\{11, 17, 8\}$ and so on. There is, on those standards, an action of the fundamental groupoid with "tangential base points"

$$\mathcal{B} = \{0\vec{1}, 1\vec{0}, 1\vec{\infty}, \infty\vec{1}, \infty\vec{0}, 0\vec{\infty}\}$$

as defined by Deligne in [17] (see the aricle by Lochak and Emsalem in [18]). This groupoid is generated by the paths $x_{\vec{v}}$ and $y_{\vec{v}}$ and $z_{\vec{v}}$ where $\vec{v}$ runs through the six standards. The paths $x_{0\vec{1}} = x$, $y_{0\vec{1}} = y$ and $x_{1\vec{0}}$ are shown in the following drawing (we let the reader imagine what the other ones could be.)



We also show $z_{0\vec{1}} = z$ below:



This action is given by the following maps:

$$x_{\vec{01}} = (12, 18, 7),\ y_{\vec{01}} = (7 \mapsto 8, 12 \mapsto 11, 18 \mapsto 17),\ y_{\vec{10}} = y_{\vec{01}}^{-1} ...$$

2.2 Topological classification of genus zero covers

In this section, we recall a quite classical result first stated by Klein in its modern formulation [26]. We need to introduce a certain number of Galois genus zero coverings of the sphere, corresponding to well-known dessins.

The first family corresponds to the dessins consisting of a star with e rays where e is a positive integer. A corresponding Belyi function is

$$y = f(x) = x^e$$

where e is the degree of the covering, totally ramified over 0 and ∞ and unramified elsewhere. We call these dessins $\mathfrak{C}_e$. Their topological Galois group is the cyclic group with e elements, C_e.

The second family corresponds to the polygon with $2e$ edges and admits the following Belyi function

$$-4y = x^e + x^{-e} - 2.$$

We call these dessins $\mathfrak{D}_{2e}$. Their topological Galois group is the dihedral group with $2e$ elements, D_{2e}.

We then have three coverings consisting of

- The tetrahedron which we call $\mathfrak{T}$ of degree 12 and with geometric Galois group the alternating permutation group on 4 letters A_4. A corresponding Belyi function is given by

$$yx^3(x^3 + 8)^3 = 2^6(x^3 - 1)^3.$$

- The octahedron $\mathfrak{O}$, of degree 24 with geometric Galois group the full symmetric group on 4 letters S_4. A corresponding Belyi function is given by

$$y(x^8 + 14x^4 + 1)^3 = 2^2.3^3.x^4(x^4 - 1)^4.$$

- The icosahedron $\mathfrak{I}$, of degree 60 with geometric Galois group the alternating permutation group on 5 letters A_5. A corresponding Belyi function is given by

$$y(x^{20} + 228x^{15} + 494x^{10} - 228x^5 + 1)^3 = x^5(x^{10} - 11x^5 - 1)^5.$$

We can now state Klein's theorem ([26]), in which two coverings $\chi : \mathcal{C} \to \mathcal{D}$ and $\chi' : \mathcal{C}' \to \mathcal{D}'$ are said to be weakly isomorphic if there exist two isomorphisms c and d such that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{c} & \mathcal{C}' \\ \downarrow{\scriptstyle \chi} & & \downarrow{\scriptstyle \chi} \\ \mathcal{D} & \xrightarrow{d} & \mathcal{D}' \end{array}$$

They are *strongly* isomorphic if $\mathcal{D} = \mathcal{D}'$ and d can be chosen to be the identity.

Theorem 2.1 *Any genus zero geometric Galois covering of the sphere is weakly isomorphic over* $\mathbb{C}$ *to one of the following:* $\mathfrak{C}_e$ *or* $\mathfrak{D}_{2e}$ *with* $e \geq 1$, *or* $\mathfrak{T}$, $\mathfrak{O}$, *or* $\mathfrak{I}$. *In particular, it is ramified over* 2 *or* 3 *points.*

Proof

We first note that the Galois group G of such a covering $\mathfrak{G}$ is a finite subgroup of $\mathbf{PGL}_2(\mathbb{C})$. Such subgroups are known to be isomorphic to one of the following: C_e, D_{2e} with $e \geq 2$, A_4, S_4, or A_5. The proof is quite elementary and uses the fact that a non-trivial element of finite order in $\mathbf{PGL}_2(\mathbb{C})$ has two fixed points ([2] p. 104). If we call X the set of such fixed points, then G acts on X. One of the consequences of the proof is that there are 2 orbits if G is cyclic and 3 otherwise. The order of the stabilizer of a point in X just depends on its orbit. For each orbit $\mathcal{O}$ we denote by $(o_\mathcal{O}, s_\mathcal{O})$ the couple consisting of its cardinality and the order of the stabilizer of some element in $\mathcal{O}$. We list the values we obtain in each case:

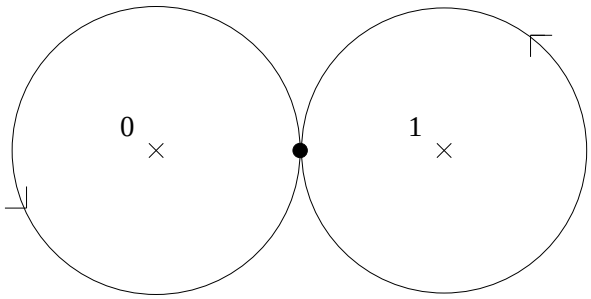
- $(1, e), (1, e)$ for C_e.
- $(e, 2), (e, 2), (2, e)$ for D_{2e}.
- $(4, 3), (6, 2), (4, 3)$ for A_4.
- $(6, 4), (12, 2), (8, 3)$ for S_4.
- $(12, 5), (30, 2), (20, 3)$ for A_5.

It is clear that these fixed points are the ramification points of the covering with orders of ramification the orders of their stabilizer. This proves that either the covering is cyclic or there are exactly three singular values.

If the covering is cyclic, one can suppose that it is totally ramified over 0 and ∞ and that the single point above 0 is 0 and the single point above ∞ is ∞. We then get a function of the form $y = Ax^e$ which is clearly equivalent to the one we gave.

If there are three ramification values we can send them on 0, 1 and ∞ using the 3-transitivity of $\mathbf{PGL}_2(\mathbb{C})$. Note that we have put those three ramification values in some definite order in the above table. We respect this order in that we send the first one to 0, the second one to 1 and the third one to ∞.

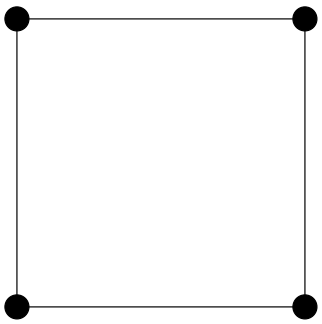
Then, a strong isomorphism class of finite coverings is given by a subgroup of finite index of $\pi_1(\mathbb{P}_1 - \{0, 1, \infty\}, b)$ where $b = 1/2$ is the base point. We choose the following basis of $\pi_1(\mathbb{P}_1 - \{0, 1, \infty\}, b)$ that induces an isomorphism to the free group with two generators (σ_0, σ_1):



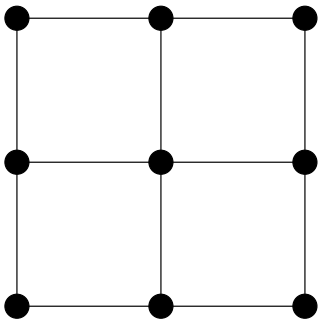
We write $\sigma_\infty^{-1} = \sigma_1\sigma_0$. Now we can associate to $\mathfrak{G}$ a subgroup $\mathfrak{g}$ of π_1. Let us write $\mathfrak{G}_0$ for the covering in the list given above which has G as Galois group, and let $\mathfrak{g}_0$ be the corresponding subgroup. We prove that $\mathfrak{g} = \mathfrak{g}_0$.

Suppose for example that $G = A_4$. Both $\mathfrak{g}_0$ and $\mathfrak{g}$ have index 12. They both contain σ_0^3, σ_1^2 and σ_∞^3 because of the ramification orders. The point now is that the subgroup generated by σ_0^3, σ_1^2 and σ_∞^3 is of finite index 12 (trivial from the classical presentation of A_4) so that $\mathfrak{g} = \mathfrak{g}_0 = \langle \sigma_0^3, \sigma_1^2, \sigma_\infty^3 \rangle$. The remaining cases are similar and reduce to the classical presentations of rotation groups.

Remark: Such a method no longer works for arbitrary genus. For example the following genus one dessin (where the opposite sides are identified) is Galois and the corresponding subgroup contains σ_0^4, σ_1^2 and σ_∞^4.



But the following dessin has the same property, and yet it is different. Indeed the subgroup generated by σ_0^4, σ_1^2 and σ_∞^4 is not of finite index.



2.3 Fields of definition, fields of moduli

In this section we simply recall a certain number of definitions in order to clarify our terminology for the rest of the chapter.

Let $\mathcal{D}$ be a dessin, that is, an isomorphism class over $\bar{\mathbb{Q}}$ of Belyi pairs. We recall that a Belyi pair is made of a curve $\mathcal{C}$ defined over $\bar{\mathbb{Q}}$ and a function $\chi : \mathcal{C} \to \mathbb{P}_{1/\bar{\mathbb{Q}}}$ defined over $\bar{\mathbb{Q}}$ and unramified outside $\{0, 1, \infty\}$. Two Belyi pairs are said to be equivalent if the corresponding coverings are strongly isomorphic.

Let $\mathbb{K}$ be a number field and $\mathcal{C}$ a projective curve and ϕ a function on $\mathcal{C}$, defined over $\mathbb{K}$. If the Belyi pair $(\mathcal{C}, \phi)$ belongs to $\mathcal{D}$, we say that $\mathbb{K}$ is *a field of definition* of $\mathcal{D}$.

There is an action of $\mathbf{\Gamma}$ on the set of dessins. This action can be seen as the naive

action on the coefficients of the equations of any Belyi pair. We call $\mathbf{\Gamma}_{\mathcal{D}}$ the stabilizer of $\mathcal{D}$ and $\mathbb{K}_{\mathcal{D}}$ its fixed field. We call $\mathbb{K}_{\mathcal{D}}$ the moduli field of $\mathcal{D}$.

The moduli field is contained in any field of definition and is actually the intersection of all the possible fields of definition ([12]). It need not be a field of definition itself as we will show in section 2.4.

Note that we do not ask that the automorphisms of the covering (if any) be defined over the field of definition, which could have the effect of augmenting it. On the other hand, the field of moduli of $\mathcal{C}$ itself might be strictly smaller than the one of the dessin. For genus zero dessins, $\mathbb{P}_{1/\mathbb{C}}$ has $\mathbb{Q}$ as field of moduli but Lenstra proved that there exist genus zero dessins with arbitrary field of moduli (see the article by L. Schneps in [18]). To finish with the *distinguo* we should warn the reader that people studying modular forms over possibly non-congruence subgroups, usually consider structures that are somewhat richer than dessins. Following Birch (see his contribution in [18]), we define marked dessins to be dessins plus a fixed marked point over infinity. In this case, of course, the field of moduli might become bigger but it is more likely to be a field of definition (for example, it will always be one in genus zero).

In the case where the dessin has no automorphisms, it must admit a model over its field of moduli $\mathbb{K}_{\mathcal{D}}$ by Weil's criterion ([45]). In this case we note that the corresponding $\mathbb{K}_{\mathcal{D}}$-isomorphism class of curves is characteristic of the dessin. We will see an example of this in the next section.

2.4 Galois action. Descending from $\mathbb{C}$ to $\mathbb{R}$

In this section we illustrate the problems of fields of definition and descent on the toy example of descending from $\mathbb{C}$ to $\mathbb{R}$. This is particularly interesting because we can give topological criteria for the descent. Further results on this subject can be found in [20]. Here, we are only interested in descent with extensions ramified over three points which thus can be chosen to be real, and which we take to be our favourite ones.

Let us denote by $\mathbf{S}_3$ the sphere minus three points $\mathbb{P}_{1/\mathbb{C}} - \{0, 1, \infty\}$ with base point $b = 1/2$ and the same basis as above for the π_1. A covering is thus given by two permutations a_0 and a_1 of the fibre over b, corresponding to the paths σ_0 and σ_1.

We write $\mathbb{M}_{0,1,\infty}$ for the maximal extension of $\mathbb{R}(t)$ unramified outside $\{0, 1, \infty\}$. We consider the following tower of extensions

$$\begin{array}{c} \mathbb{M}_{0,1,\infty} \\ \Big| \hat{\pi}_1 \\ \mathbb{C}(t) \\ \Big| \mathbb{Z}/2\mathbb{Z} \\ \mathbb{R}(t) \end{array}$$

and the corresponding exact sequence of groups

$$1 \to \hat{\pi}_1 \to \mathcal{G} \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

We recall that there exist two $\mathbb{R}$-isomorphism classes of genus zero curves, the class of the straight line $\mathbb{P}_{1/\mathbb{R}}$ and the class of the plane curve given by the equation

$$x^2 + y^2 + z^2 = 0,$$

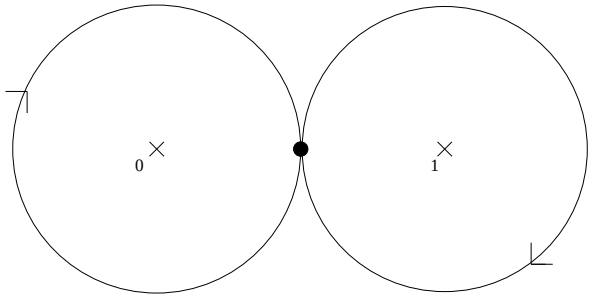
which we call $\tilde{\mathbb{P}}_{1/\mathbb{R}}$.

Given a dessin $\mathcal{D}$ by its monodromy (a_0, a_1), or equivalently, a triangulation of a surface, we ask three questions:

- Is the moduli field of $\mathcal{D}$ equal to $\mathbb{C}$ or $\mathbb{R}$?
- If the moduli field is $\mathbb{R}$, does the dessin admit a model over $\mathbb{R}$?
- If a real genus zero dessin has no automorphisms, it admits a real model. Then can we say whether the underlying curve is $\mathbb{P}_1$ or $\tilde{\mathbb{P}}_1$?

We will give examples of all the possible situations and finish with an example of a real dessin (i.e. a dessin with real moduli field) with no real model.

To answer the first question we note that the outer action of $\mathbb{Z}/2\mathbb{Z}$ on $\hat{\pi}_1$ comes from an action on π_1 itself. Let τ denote the reflection of the plane induced by the unique non-trivial element $\tau \in Gal(\mathbb{C}/\mathbb{R}) \approx \mathbb{Z}/2\mathbb{Z}$. This reflection is continuous and thus induces an involution of π_1. The images of σ_0, σ_1, σ_∞ are given by ${}^\tau\sigma_0 = \sigma_0^{-1}$, ${}^\tau\sigma_1 = \sigma_1^{-1}$, and ${}^\tau\sigma_\infty = \sigma_1\sigma_0$.



Let now $\chi : \mathcal{C} \to \mathbf{S}_3$ be an algebraic covering of degree d and ${}^\tau\chi : {}^\tau\mathcal{C} \to \mathbf{S}_3$ its conjugate under τ. There is a bijection induced by τ between the fibre of χ above b and the fibre of ${}^\tau\chi$ above b. Let $\{b_1, b_2, ..., b_d\}$ denote the points above b and $\{{}^\tau b_1, {}^\tau b_2, ..., {}^\tau b_d\}$ their images under τ. If σ is a closed path in π_1 and b_i a point above b on $\mathcal{C}$, then $\sigma(b_i)$ denotes the extremity of the lifted path on $\mathcal{C}$, with origin b_i. On the other hand, we can lift ${}^\tau\sigma$ onto ${}^\tau\mathcal{C}$, with origin ${}^\tau b_i$, so ${}^\tau\sigma({}^\tau b_i)$ is the extremity of the lifted path. Then ${}^\tau\sigma({}^\tau b_i) = {}^\tau(\sigma(b_i))$.

This means that the action of σ on the fibre $\chi^{-1}(b)$ is conjugated by τ to the action of ${}^\tau\sigma$ on the fibre ${}^\tau\chi^{-1}(b)$. Therefore, if χ was given by its monodromy (a_0, a_1), the monodromy of ${}^\tau\chi$ is (a_0^{-1}, a_1^{-1}) where a_0^{-1} and a_1^{-1} can be seen as permutations of $\{{}^\tau b_1, {}^\tau b_2, ..., {}^\tau b_d\}$ through the bijection with $\{b_1, b_2, ..., b_d\}$ induced by τ. This gives an explicit description of the outer action of $Gal(\mathbb{C}/\mathbb{R})$ in the above exact sequence.

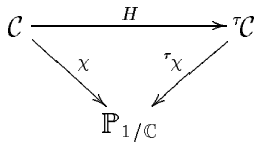
Now, a dessin of degree d will be said to be real if and only if its field of moduli is $\mathbb{R}$. If (a_0, a_1) is its monodromy, this is just saying that there exists a permutation $\omega \in \mathcal{S}_{\{b_1, b_2, ..., b_d\}}$ such that

$${}^\tau(a_0, a_1) = (a_0^{-1}, a_1^{-1}) = {}^\omega(a_0, a_1) = (\omega^{-1} a_0 \omega, \omega^{-1} a_1 \omega)$$

If this is the case, we note that ω belongs to the normalizer of $G = \langle a_0, a_1 \rangle$ in $\mathcal{S}_{\{b_1,b_2,\ldots,b_d\}}$, and is defined up to an automorphism of $\mathcal{D}$ (we recall that the automorphism group of $\mathcal{D}$ is $\mathfrak{a} = \mathcal{Z}_{\mathcal{S}_{\{b_1,b_2,\ldots,b_d\}}}(G)$, the centralizer of G in the full permutation group). Furthermore, since τ is an involution, we have $\omega^2 \in \mathfrak{a}$. Now, the dessin $\mathcal{D}$ admits a model over $\mathbb{R}$ if and only if ω can be chosen to satisfy Weil's cocycle condition

$$\omega^2 = 1.$$

Indeed, associated to ω, there is a morphism $H : \mathcal{C} \to {}^{\tau}\mathcal{C}$ such that the following diagram commutes



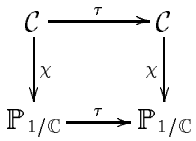
and H and ω are linked by the following identity

$$H(b_i) = {}^{\tau}(\omega(b_i)).$$

The cocycle condition on H for the existence of a real model is ${}^{\tau}H H = I$ which is immediately translated on ω as $\omega^2 = 1$.

We now come to the situation where the dessin $\mathcal{D}$ has no automorphisms. In this case ω is unique and ω^2 can only be equal to 1 and we have a model over $\mathbb{R}$ (here H is nothing but the identity)

and the action of τ extends to the real curve $\mathcal{C}$ in a way that makes the following diagram commute:



The action of τ on the fibre above b is thus given by the formula

$${}^{\tau}b_i = \omega(b_i)$$

and since ω conjugates a_0 and a_0^{-1}, it induces a permutation of the cycles of a_0 which gives the action of τ on the fibre $\chi^{-1}(0)$. In the same way we describe the Galois action on $\chi^{-1}(1)$ and $\chi^{-1}(\infty)$.

Suppose that among the cycles of σ_0 and σ_1 there is one which is fixed under the action of ω. Then, the corresponding point on $\mathcal{C}$ is real and thus $\mathcal{C}$ is isomorphic over $\mathbb{R}$ to the projective line $\mathbb{P}_{1/\mathbb{R}}$.

To state the reciprocal assertion, we need to work a bit more. Suppose that χ is a real rational fraction: $\chi : \mathbb{P}_{1/\mathbb{R}} \to \mathbb{P}_{1/\mathbb{R}}$ associated to the dessin $\mathcal{D}$. Let c be some

connected component of the preimage of the open segment $(0,1)$. Because χ is real and unramified over $(0,1)$, c is either contained in $\mathbb{R}$, or does not intersect it. If there exists such a c contained in $\mathbb{R}$ then its extremities are real thus proving the assertion that at least one point over $\{0,1\}$ is real, and so the corresponding cycle must be fixed by ω. On the other hand, suppose that $\chi^{-1}((0,1)) \cap \mathbb{R}$ is empty. We note that $\chi^{-1}([0,1]) \cap \mathbb{R}$ cannot be empty because $\chi^{-1}([0,1])$ is a connected non-empty subset of the plane which is invariant under the reflection τ. This again proves the desired statement.

We finish by stating

Theorem 2.2 *Let $\mathcal{D}$ be a dessin, given by its monodromy (a_0, a_1, a_∞).*

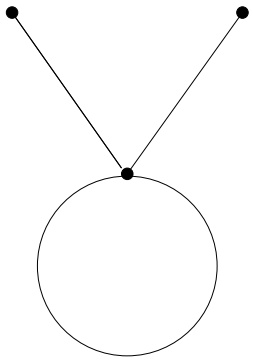
The field of moduli of $\mathcal{D}$ is $\mathbb{R}$ if and only if there exists some ω such that $a_0^{-1} = {}^{\omega}a_0$ and $a_1^{-1} = {}^{\omega}a_1$.

In the latter case, the dessin admits a real model if and only if ω can be chosen so that $\omega^2 = 1$.

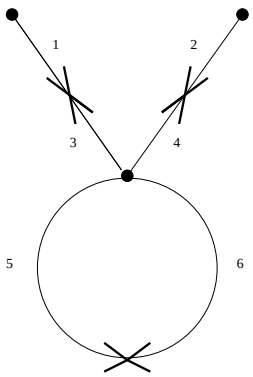
If $\mathcal{D}$ is of genus zero and its automorphism group (the centralizer of $\langle a_0, a_1 \rangle$) is trivial, then the dessin admits a rational model over some real genus 0 curve. This curve is $\mathbb{R}$-isomorphic to $\mathbb{P}_{1/\mathbb{R}}$ if and only if the action of ω over the cycles of a_0 and a_1 has at least one fixed point.

Examples

The rabbit is a real dessin with no automorphisms and admits a real model on the projective line.



To see this, we give numbers to the flags and compute the monodromy.



$$a_0 = (3,5,6,4),\ a_1 = (1,3)(2,4)(5,6),\ a_\infty = (4,2,6,3,1).$$

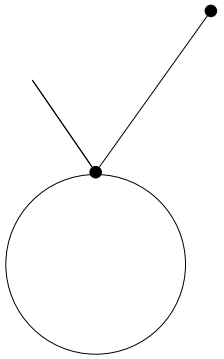
It is clear that there are no automorphisms. If a is a permutation which commutes with a_∞, it must fix 5. But since it commutes with a_1 as well, it must fix 6 as well. Now, coming back to a_∞ we see that a must be the identity. Furthermore we have

$$\omega = (3,4)(1,2)(5,6),$$

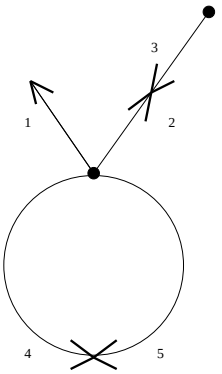
and check that the dessin is real.

The action of ω on the cycles of a_0 and a_1 fixes the cycle $(3,5,6,4)$ in a_0 and the cycle $(5,6)$ in a_1. This is more than enough to prove that the dessin has a real model on $\mathbb{P}_{1/\mathbb{R}}$.

The rabbit with a lopped off left ear is a non-real dessin.



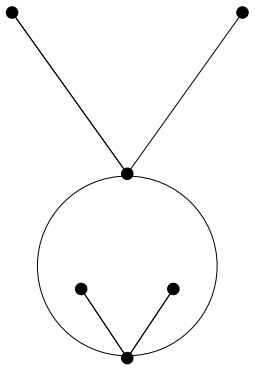
The monodromy is given by:



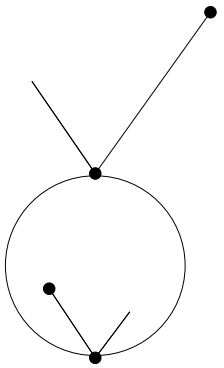
$$a_0 = (1,4,5,2),\ a_1 = (2,3)(4,5),\ a_\infty = (5,1,2,3).$$

Here there is no hope of finding an ω since such a permutation should fix 3 (from a_0) and 4 (from a_∞) and thus 2 and 5 as well (from a_1). This does not work.

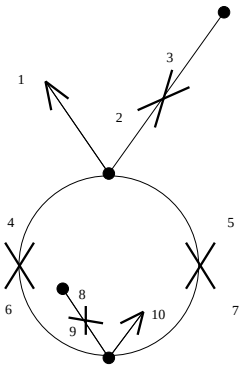
The smiling rabbit evidently has an automorphism group of order 2.



The rabbit with a lopped off left ear and a sidelong smirk on the right hand side is a real dessin with no non-trivial automorphisms and real model on the real curve $\tilde{\mathbb{P}}_1$ with equation $x^2 + y^2 + z^2 = 0$.



Its monodromy is:



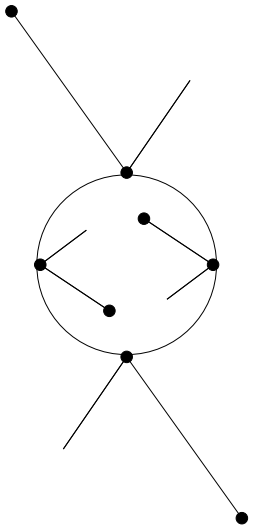
$$a_0 = (1,4,5,2)(9,6,7,10),\ a_1 = (2,3)(4,6)(8,9)(7,5),$$
$$a_\infty = (4,9,8,10,7)(3,5,6,1,2).$$

There are no non-trivial automorphisms (exercise) and there is a unique ω defined as

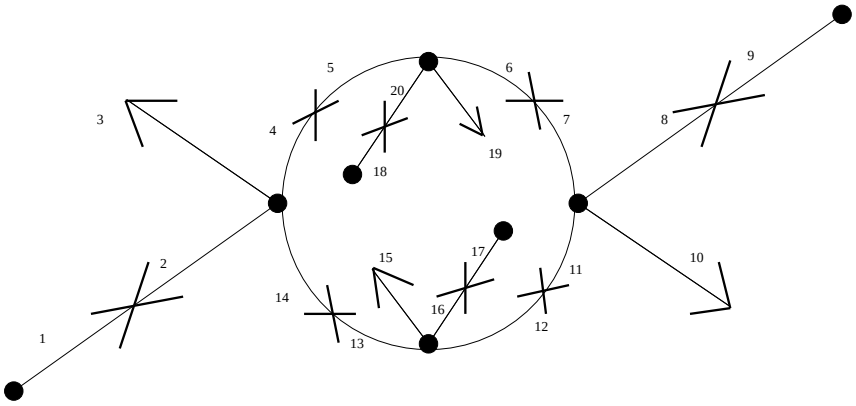
$$\omega = (1,10)(3,8)(9,2)(6,5)(4,7),$$

and none of the cycles of a_0 and a_1 are fixed by ω.

The double rabbit is a real dessin with no real model.



Its monodromy is:



$$a_0 = (3,2,14,4)(5,20,19,6)(7,11,10,8)(15,13,12,16),$$

$$a_1 = (1,2)(4,5)(6,7)(11,12)(13,14)(16,17)(8,9)(18,20),$$

$$a_\infty = (18,5,14,15,16,17,12,7,19,20)(4,6,8,9,10,11,13,2,1,3).$$

There is an automorphism group of order 2 generated by

$$\mathfrak{a} = (3,10)(8,2)(9,1)(14,7)(6,13)(5,12)(11,4)(20,16)(15,19)(17,18).$$

The dessin is real for we can choose ω to be

$$\omega = (15,3,19,10)(16,2,20,8)(17,1,18,9)(13,4,6,11)(12,14,5,7).$$

We could have chosen $\mathfrak{a}\omega$ instead. But $(\mathfrak{a}\omega)^2 = \omega^2$ is *not* the identity. This proves that our dessin although real, has no real model.

2.5 Spheres minus four points

In this section we recall the basics about the Legendre form for elliptic curves. We are interested in building moduli spaces for spheres minus four points. To begin with, we define two different kinds of spheres minus four points. A non-coloured sphere minus four points is defined as a set of four distinct points $\{a,b,c,d\}$ on the complex projective line. A coloured sphere is a quadruplet of distinct points in $\mathbb{P}_{1/\mathbb{C}}$.

There are actions of $\mathbf{PGL}_2(\mathbb{C})$ on both sets. Defined by

$$H\{a,b,c,d\} = \{Ha, Hb, Hc, Hd\},\ H(a,b,c,d) = (Ha, Hb, Hc, Hd).$$

The set of coloured spheres is $\mathcal{C} = \mathbb{P}^4_1 - \mathcal{D}$ where $\mathcal{D}$ is the discriminant variety defined as $(a-b)(a-c)(a-d)(b-c)(b-d)(c-d) = 0$. The group $\mathcal{S}_4$ acts naturally on $\mathcal{C}$. The set of non-coloured spheres is the quotient $\mathcal{N}$ of $\mathcal{C}$ by $\mathcal{S}_4$.

We thus have a decolouration covering s_4 which is Galois with Galois group $\mathcal{S}_4$.

$$\begin{array}{c} \mathcal{C} \\ \downarrow{\scriptstyle s_4} \\ \mathcal{D} \end{array}$$

We define the classical function cross-ratio on $\mathcal{C}$

$$[a,b,c,d] = \lambda(a,b,c,d) = \frac{b-c}{b-a} \cdot \frac{d-a}{d-c}.$$

It is well known that two elements in $\mathcal{C}$ belong to the same $\mathbf{PGL}_2(\mathbb{C})$-orbit if and only if λ takes the same value at those points .

We note that λ is invariant under the Klein group, seen as the subgroup V of $\mathcal{S}_4$ generated by the permutations of type $(2,2)$. This subgroup is normal so that the covering splits in two. We note $\mathcal{H} = \mathcal{C}/V$, v the corresponding V-covering, and s_3 the $\mathcal{S}_3$-covering of the lower part:

$$\begin{array}{ccc} \mathcal{C} & & \\ \downarrow{\scriptstyle v} & & \\ \mathcal{H} & \xrightarrow{\lambda} & \mathbb{P}_1 \\ \downarrow{\scriptstyle s_3} & & \\ \mathcal{D} & & \end{array}$$

and we have the exact sequence

$$1 \to V \to \mathcal{S}_4 \to \mathcal{S}_3 \to 1.$$

It is tempting (although not particularly original...) to look at the action of $\mathcal{S}_3$ on λ. It is given in the following list:

$$\begin{array}{lll} [[1,2]] & \lambda \mapsto & 1-\lambda \\ [[1,3]] & \lambda \mapsto & 1/\lambda \\ [[2,3]] & \lambda \mapsto & \lambda/\lambda - 1 \\ [[1,2,3]] & \lambda \mapsto & (\lambda-1)/\lambda \\ [[1,3,2]] & \lambda \mapsto & 1/(1-\lambda) \end{array}$$

This action is killed by the function

$$J(\lambda) \stackrel{\text{def}}{=} 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

which defines a Galois covering with (strong) automorphism group $\mathcal{S}_3$. Note the following amusing fact: J also admits a weak automorphism, namely

$$J(\frac{\lambda-2}{2\lambda-1}) = \frac{1728J}{J-1728} \tag{2.1}$$

The linear fraction

$$\delta(\lambda) = \frac{\lambda-2}{2\lambda-1}$$

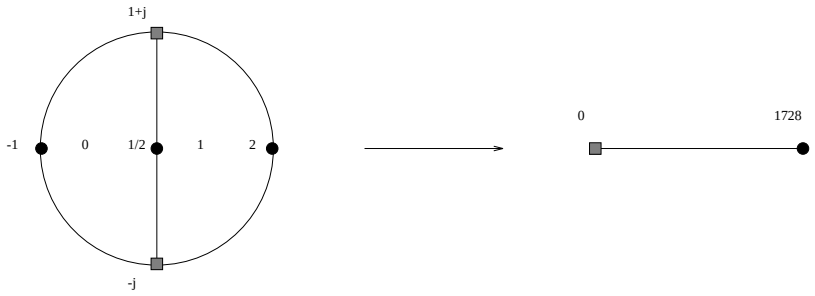
sends the triangle $(0,1,\infty)$ to the triangle $(2,-1,1/2)$. It is of order two. The linear fraction

$$\rho(J) = \frac{1728J}{J-1728}$$

is of order two and permutes the ramification locus of J. We have

$$\rho J = J\delta.$$

This will appear later on. We can draw the reciprocal image of $[0,1728]$ under J and find the dessin below:



We note $J(a,b,c,d) = J(\lambda(a,b,c,d))$ and get a symmetric function of (a,b,c,d) defined over $\mathcal{D}$:

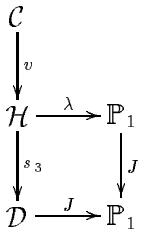
$$J(a,b,c,d) = 2^8 \cdot \frac{E_4^3}{disc(a,b,c,d)} \tag{2.2}$$

and

$$J - 1728 = 2^6 \cdot \frac{E_6^2}{disc(a,b,c,d)},$$

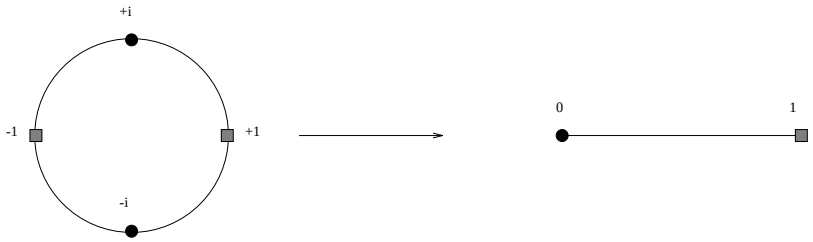
where $E_4 = 12\sigma_4 + \sigma_2^2 - 3\sigma_1\sigma_3$ and $E_6 = 72\sigma_2\sigma_4 - 2\sigma_2^3 + 9\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2 - 27\sigma_4\sigma_1^2$, and $disc(a,b,c,d) = \Delta$ denotes the discriminant. Those polynomials satisfy the expected invariance relations. For example, if $H(z) = (uz+v)/(wz+k)$ then we have

$$\frac{\Delta(H(a),H(b),H(c),H(d))}{\Delta(a,b,c,d)} = \frac{(uk-vw)^{12}}{(u^4 - \sigma_1 u^3 w + \sigma_2 u^2 w^2 - \sigma_3 u w^3 + \sigma_4 w^4)^6}$$



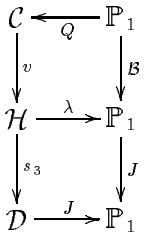
We note that the above commutative diagram is compatible with the Galois actions of $\mathcal{S}_3$ on each side. It seems as well that the right hand side of this is incomplete (one level is lacking). In the sequel we try to see what can be done to complete this construction. We first remember of the existence of a Galois genus 0 covering of the sphere with group $\mathcal{S}_4$. We build such a covering in the following way. Let $\mathcal{B}(x) = 1/4(x + 1/x)^2 = 1 + 1/4(x - 1/x)^2$ be the Galois function with automorphism group V, ramified over 0, 1, ∞.

We draw the corresponding dessin:



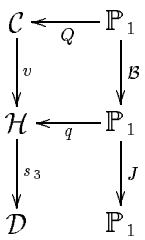
The composition $J \circ \mathcal{B}$ is a function ramified over 0, 1728, ∞ which defines the only genus zero $\mathcal{S}_4$-extension of $\mathbb{P}_1$ ramified at those places (in *that* order).

To each value of x we associate the quadruplet $Q(x) = (x, -x, 1/x, -1/x)$ such that $\lambda(Q(x)) = [x, -x, 1/x, -1/x] = \mathcal{B}(x)$ and get the following commutative diagram:



Note also that we can define $q(\lambda) = v(Q(x)) = v(x, -x, 1/x, -1/x)$ where x is any point such that $\mathcal{B}(x) = \lambda$. Such a point $q(\lambda)$ on $\mathcal{H}$ can be defined by its V-symmetric functions $\sigma_1 = 0$, $\sigma_2 = 2 - 4\lambda$, $\sigma_3 = 0$, $\sigma_4 = 1$, and $[x, -x, 1/x, -1/x] = \lambda$.

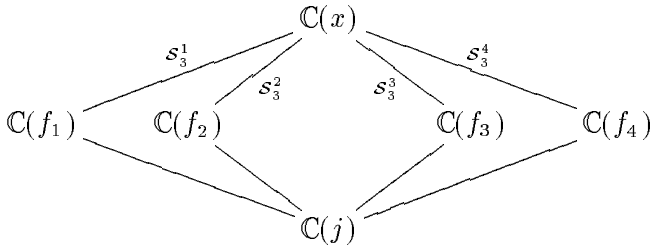
This way we get the following commutative diagram



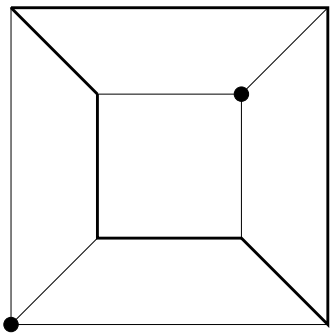
We would like to build four algebraic functions $f_1(x)$, $f_2(x)$, $f_3(x)$ and $f_4(x)$ with the following properties:

- The set $\{f_1, f_2, f_3, f_4\}$ is invariant under the automorphism group of $J \circ \mathcal{B}$, and this group $\mathcal{G}$ acts on $\{f_1, f_2, f_3, f_4\}$ like $\mathcal{S}_4$.
- The cross-ratio $[f_1, f_2, f_3, f_4]$ is (something like) $\lambda = [x, -x, 1/x, -1/x] = \mathcal{B}(x)$.

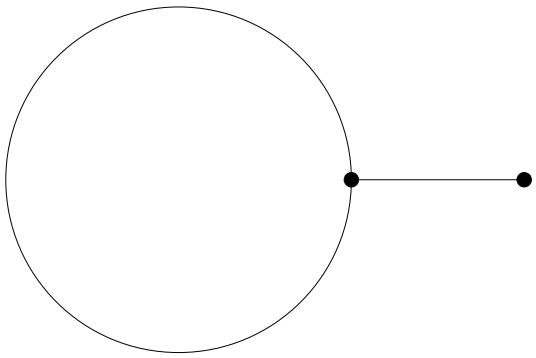
To do this, we write $\mathcal{S}_3^i$ for the stabilizer of i in $\mathcal{S}_4$ for $i \in \{1, 2, 3, 4\}$. The corresponding subextensions of $\mathbb{C}(x)/\mathbb{C}(j)$ are genus zero fields. We choose f_1 to be a generator of $\mathbb{C}(x)^{\mathcal{S}_3^1}$. We then can choose $f_2(x) = f_1(-x)$, $f_3(x) = f_1(1/x)$ and $f_4(x) = f_1(-1/x)$. Note that the f_i are defined up to a linear transform on the left.



We can be more precise if we look for the minimal polynomial of f_1 with coefficients in $\mathbb{C}(j)$. To compute it, we just quotient the dessin corresponding to a cube by the group $\mathcal{S}_3^1$ which can be seen as the stabilizer of one of the four diagonals of the cube.



We thus get the following dessin.



If we send the vertex of order three to zero and the one of order one to one, the corresponding Belyi function will be $X \mapsto Y$ such that

$$Y + 2^{14} \cdot X^3(X-1) = 0.$$

In other words, we choose for f_i the four roots of the equation

$$j + 2^{14} \cdot f^3(f-1) = 0. \tag{2.3}$$

On the other hand, the map $x \mapsto f_1$ is a Galois covering with group $\mathcal{S}_3$. As we saw in the second section, such a covering must be equal to the classical J covering up to linear transforms L and R on both sides:

$$f_1(x) = L(J(R(x))).$$

We don't worry too much about L since it does not change the cross-ratio $[f_1, f_2, f_3, f_4]$. As for R, it can be defined as follows. Let r be the primitive 8-th root of unity given by

$$r = \sqrt{2} \cdot \frac{1+i}{2}$$

and let R be the linear transform defined by the matrix

$$R = \begin{bmatrix} 3 - r - 2r^2 + 4r^3 & 1 - r + 2r^2 \\ 3 - 2r - r^2 + 2r^3 & 2 + r - 2r^2 + 3r^3 \end{bmatrix}$$

We set $f_1(x) = L(J(R(x)))$ and $f_2(x) = f_1(-x)$, $f_3(x) = f_1(1/x)$ and $f_4(x) = f_1(-1/x)$. Then it can be easily shown that the cross-ratio $[f_1, f_2, f_3, f_4]$ satisfies

$$[f_1(x), f_2(x), f_3(x), f_4(x)] = \delta(\mathcal{B}(x))$$

We also get the j-invariant thanks to (2.2)

$$\begin{aligned} J(f_1(x), f_2(x), f_3(x), f_4(x)) &= J(f_1(x), f_1(-x), f_1(1/x), f_1(-1/x)) \\ &= \rho(J(x, -x, 1/x, -1/x)) \\ &= \rho(j) \\ &= \frac{1728j}{j - 1728} \end{aligned}$$

The symmetric functions of the f_i are given by (2.3):

$$\sigma_1 = 1,\ \sigma_2 = 0,\ \sigma_3 = 0,\ \sigma_4 = 2^{-14}j.$$

It is important not to confuse j, the invariant of $[x, -x, 1/x, -1/x]$, with $\rho(j)$, the invariant of the f_i.

We now define three maps. The first one, called D, from the j-space $\mathbb{P}_{1/\mathbb{C}}$ to the non-coloured space $\mathcal{D}$, is such that $D(j)$ is the point of $\mathcal{D}$ defined by its symmetric functions

$$\sigma_1 = 1, \sigma_2 = 0, \sigma_3 = 0, \sigma_4 = 2^{-14}j.$$

The second map, called H, from the λ-space $\mathbb{P}_{1/\mathbb{C}}$ to the half-coloured space $\mathcal{H}$, is such that $H(\lambda)$ is defined by its V-symmetric functions

$$\sigma_1 = 1, \sigma_2 = 0, \sigma_3 = 0, \sigma_4 = 2^{-14} J(\lambda) = 2^{-6} \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (\lambda - 1)^2},$$

and the cross-ratio defined as

$$\delta(\lambda) = \frac{\lambda - 2}{2\lambda - 1}.$$

The third map, called C, from the x-space $\mathbb{P}_{1/\mathbb{C}}$ to the coloured space $\mathcal{C}$, is such that $C(x)$ is defined by the quadruplet $(f_1(x), f_2(x), f_3(x), f_4(x))$ as above.

We then get the following commutative diagram in which the actions of $\mathcal{S}_4$ as a Galois group on both sides are compatible with the arrows.

$$\begin{array}{ccc}
\mathcal{C} & \xleftarrow{C} & \mathbb{P}_1 \\
\downarrow{\scriptstyle v} & & \downarrow{\scriptstyle \mathcal{B}} \\
\mathcal{H} & \xleftarrow{H} & \mathbb{P}_1 \\
\downarrow{\scriptstyle s_3} & & \downarrow{\scriptstyle J} \\
\mathcal{D} & \xleftarrow{D} & \mathbb{P}_1
\end{array}$$

We have thus realized the covering of moduli spaces as a restriction of the covering of naive spaces. We finish by noting that $\lambda H = \delta$ and $JD = \rho$ which stresses the importance of (2.1). The functions (H, D) define something which is almost but not quite a section of (λ, J).

2.6 Approximating dessins from Puiseux series

In this section we now come to the problem of computing explicitely some algebraic model for a given abstract dessin. In fact, we will do better: we will compute the linear space associated with any given divisor on the dessin. The result is given as Puiseux series. Of course, we must truncate the series and consider floating point coefficients if we want to work with finite memory and time. We show in the next section how to obtain some exact solution from such approximations.

We consider the subgroup of $\mathbf{PGL}_2(\mathbb{C})$ consisting of six linear transforms permuting 0, 1, and ∞. We describe it explicitly as follows:

$$H_{\vec{01}}(\lambda) = \lambda = \lambda_{\vec{01}}, \quad H_{0\vec{\infty}}(\lambda) = \frac{\lambda}{\lambda - 1} = \lambda_{0\vec{\infty}},$$

$$H_{\vec{10}}(\lambda) = 1 - \lambda = \lambda_{\vec{10}}, \quad H_{1\vec{\infty}}(\lambda) = \frac{\lambda - 1}{\lambda} = \lambda_{1\vec{\infty}},$$

$$H_{\vec{\infty}0}(\lambda) = \frac{1}{1 - \lambda} = \lambda_{\vec{\infty}0}, \quad H_{\vec{\infty}1}(\lambda) = \frac{1}{\lambda} = \lambda_{\vec{\infty}1}.$$

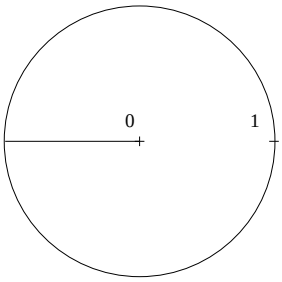
We note that for any standard $\vec{v}$ we have $H_{\vec{v}}(\vec{v}) = \vec{01} = (0, 1/2)$. Now let e be a positive integer. We build an e-th root of $\lambda_{\vec{v}}$ as follows. First let $\Lambda_{\vec{01},e}$ be defined for $\lambda_{\vec{01}} \in \mathbb{C} - (-\infty, 0]$ as

$$\Lambda_{\vec{01},e}(\lambda_{\vec{01}}) = \lambda_{\vec{01}}^{1/e} = exp(2i\pi \, Log(\lambda_{\vec{01}}) e^{-1})$$

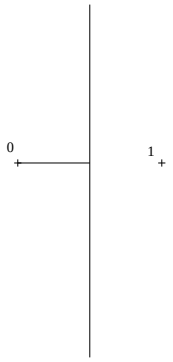
where *Log* is the principal determination of the logarithm. We then define the $\Lambda_{\vec{v},e}$ as

$$\Lambda_{\vec{v},e}(\lambda_{0\vec{1}}) = \Lambda_{0\vec{1},e}(H_{\vec{v}}(\lambda_{0\vec{1}})) = \Lambda_{0\vec{1},e}(\lambda_{\vec{v}}).$$

Now we define the domain $\mathcal{K}_{0\vec{1}}$ to be the open circle of center 0 and radius 1 minus the segment $(-1, 0)$,



and similarly, $\mathcal{K}_{\vec{v}}$ is such that $H_{\vec{v}}(\mathcal{K}_{\vec{v}}) = \mathcal{K}_{0\vec{1}}$. For example $\mathcal{K}_{0\vec{\infty}}$ is the half-plane $\Re(z) < 1/2$ minus the segment $(0, 1/2)$.



Note that there are two uniformizing parameters at any given point. For example, $\Lambda_{0\vec{1},e}$ will be useful for analytic continuation from 0 to 1 and $\Lambda_{0\vec{\infty},e}$ will be useful for analytic continuation from 0 to ∞. The six domains of convergence form a covering of $\mathbb{P}_1 - \{\rho, \bar{\rho}\}$ where $\rho = \exp(\frac{2i\pi}{6})$.

We consider a dessin $\mathcal{D}$ together with a Belyi function $\chi : \mathcal{C} \to \mathbb{P}_1 - \{0, 1, \infty\}$ for some algebraic curve $\mathcal{C}$, and a divisor D over $\mathcal{D}$, i.e. a divisor over the underlying curve $\mathcal{C}$ whose points all lie over $\{0, 1, \infty\}$. We write

$$D = \sum_i o_i P_i$$

and we write $\mathcal{L}(D)$ for the corresponding linear space. We will characterize it as the kernel of a certain operator built from some universal hermitian blocks. Let f be some function in $\mathcal{L}(D)$. Associated to each standard $\vec{v}$ above $0\vec{1}$ there is a connected component of $\chi^{-1}(\mathcal{K}_{0\vec{1}})$, and also an expansion of f as a series in $\Lambda_{0\vec{1},e_i}$, where e_i is the ramification at the associated point P_i over 0.

$$f = \sum_{k \geq -o_i} a_{\vec{v},k} \Lambda^k_{0\vec{1},e_i}.$$

Similarly, we define uniformizing parameters and expansions of f at any standard of the dessin. We call $\mathbf{S}$ the set of all standards in the dessin. To a function $f \in \mathcal{L}(D)$ we associate the list of sequences of coefficients of its expansions at all standards

$$((a_{\vec{v},k})_k)_{\vec{v}\in\mathbf{S}}.$$

The sequence $(a_{\vec{v},k})_k$ is such that the associated entire series

$$\sum_k a_{\vec{v},k} X^k$$

is convergent on the open disk of radius one and is bounded outside any neighbourhood of $\{0,1\}$ in the disk. Such sequences form a linear space which we call $\mathbf{J}$. To each function $f \in \mathcal{L}(D)$ we associate a vector in $\mathbf{J}^{\mathbf{S}}$. This clearly induces an injection of linear spaces. We want to characterize its image as the kernel of a certain linear operator.

We now study the relations between the various expansions. The relations will be of three types. The first two types involve expansions at various standards related to the same point. The third one relates the expansions at two standards facing each other.

Let P_i be a point above 0 with ramification order e_i and $\vec{v}$ a standard at P_i. Let's say that $\vec{v}$ is over $\vec{01}$. We call $\vec{w} = x_{\vec{01}}(\vec{v})$ the next standard over $\vec{01}$ at P_i reached when turning counterclockwise.

A typical situation of that is in our example from the introduction, the standards 7 and 12. We write the two corresponding expansions

$$f = \sum_{k\geq -o_i} a_{\vec{v},k} \Lambda^k_{\vec{01},e_i},$$

$$f = \sum_{k\geq -o_i} a_{\vec{w},k} \Lambda^k_{\vec{01},e_i},$$

where the coefficients are related by the obvious relations

$$a_{\vec{w},k} = \zeta^k_{e_i} \cdot a_{\vec{v},k} \tag{2.4}$$

where $\zeta_{e_i} = exp(2i\pi e_i^{-1})$ is the smallest primitive e_i-th root of unity. This relation simply expresses the monodromy of the logarithm.

We may think now of relating the expansion at $\vec{v}$ and the expansion at $\vec{u} = z_{\vec{01}}(\vec{v})$, which is the first flag over $0\vec{\infty}$ met when turning counterclockwise. For example the standards 7 and 13.

$$f = \sum_{k\geq -o_i} a_{\vec{v},k} \Lambda^k_{\vec{01},e_i},$$

$$f = \sum_{k\geq -o_i} a_{\vec{u},k} \Lambda^k_{0\vec{\infty},e_i}.$$

This requires no more than expressing $\Lambda_{0\vec{\infty},e_i}$ from $\Lambda_{\vec{01},e_i}$. Let $\xi_{e_i} = exp(i\pi e_i^{-1})$ be the smallest e_i-th root of -1; we find that

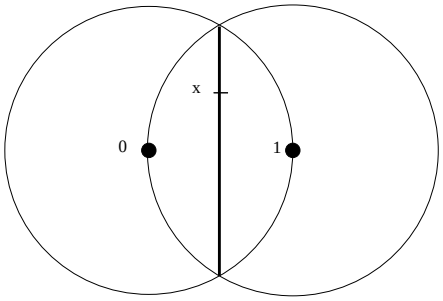
$$\Lambda_{0\vec{\infty},e_i} = \xi_{e_i} \cdot \frac{\Lambda_{\vec{01},e_i}}{(1-\lambda_{\vec{01}})^{1/e_i}} = \xi_{e_i} \cdot \Lambda_{\vec{01},e_i} \sum_{k\geq 0} \binom{e_i^{-1}}{k} \lambda^k_{\vec{01}} \tag{2.5}$$

Now comes the only non-trivial type of relation. For example the standards 7 and 8. This time the two expansions are not over the same point since when $\vec{v}$ is over $0\vec{1}$ and concerns a point P_i over 0, on the contrary $\vec{t}$ is over $1\vec{0}$ and is attached to some point P_j above 1. We have the two corresponding expansions

$$f = \sum_{k \geq -o_i} a_{\vec{v},k} \Lambda^k_{0\vec{1},e_i},$$

$$f = \sum_{k \geq -o_j} a_{\vec{t},k} \Lambda^k_{1\vec{0},e_j}.$$

Following Atkin [5], we now equate these two expansions at some point x on the open segment $(\rho, \bar{\rho})$ where $\rho = exp(2i\pi/6)$ is a sixth root of unity. It is to be noted that for such an x, $1 - x = \bar{x}$.



For convenience we adopt the following notation. Let $|a_{\vec{v},k}\rangle$ denote the infinite column vector of all coefficients in the expansion at $\vec{v}$, namely

$$|a_{\vec{v},k}\rangle = (a_{\vec{v},-o_i}, a_{\vec{v},-o_i+1}, a_{\vec{v},-o_i+2}, ...)\tilde{}$$

where the tilde stands for transposition.

We also write $\langle x, -o_i, e_i|$ for the infinite line vector

$$\langle x, -o_i, e_i| = (\Lambda^{-o_i}_{\vec{01},e_i}(x), \Lambda^{-o_i+1}_{\vec{01},e_i}(x), \Lambda^{-o_i+2}_{\vec{01},e_i}(x), ...)$$

Then the value taken by f at x is given by

$$f(x) = \langle x, -o_i, e_i||a_{\vec{v},k}\rangle$$

and the relation between the two expansions can be expressed for all x in the segment $(\rho, \bar{\rho})$ as

$$\langle x, -o_i, e_i||a_{\vec{v},k}\rangle = \langle 1 - x, -o_j, e_j||a_{\vec{t},k}\rangle = \langle \bar{x}, -o_j, e_j||a_{\vec{t},k}\rangle \tag{2.6}$$

We write $|\bar{x}, -o_i, e_i\rangle$ for the adjoint of $\langle x, -o_i, e_i|$ and similarly, $|\bar{x}, -o_j, e_j\rangle$ for the adjoint of $\langle x, -o_j, e_j|$. We also define the operators $\mathfrak{v}_{x,-o_i,e_i}$, $\mathfrak{v}_{x,-o_j,e_j}$ and $\mathfrak{c}_{x,-o_i,e_i,-o_j,e_j}$ by

$$\begin{aligned}
\mathfrak{v}_{x,-o_i,e_i} &= |\bar{x}, -o_i, e_i\rangle\langle x, -o_i, e_i| \\
\mathfrak{v}_{x,-o_j,e_j} &= |\bar{x}, -o_j, e_j\rangle\langle x, -o_j, e_j| \\
\mathfrak{c}_{x,-o_i,e_i,-o_j,e_j} &= |\bar{x}, -o_i, e_i\rangle\langle \bar{x}, -o_j, e_j|
\end{aligned}$$

We deduce from (2.6) that

$$\begin{bmatrix} \mathfrak{v}_{x,-o_i,e_i} & -\mathfrak{c}_{x,-o_i,e_i,-o_j,e_j} \\ -\mathfrak{c}^*_{x,-o_i,e_i,-o_j,e_j} & \bar{\mathfrak{v}}_{x,-o_j,e_j} \end{bmatrix} |a_{\vec{v},k}\rangle \oplus |a_{\vec{t},k}\rangle = 0 \tag{2.7}$$

where $\bar{\mathfrak{v}}_{x,-o_j,e_j}$ is the conjugate of $\mathfrak{v}_{x,-o_j,e_j}$.

This proves that the direct sum $|a_{\vec{v},k}\rangle \oplus |a_{\vec{t},k}\rangle$, obtained as concatenation of the two column-vectors, is in the kernel of a given hermitian positive operator which we call

$$\mathfrak{j}_{x,-o_i,e_i,-o_j,e_j} = \begin{bmatrix} \mathfrak{v}_{x,-o_i,e_i} & -\mathfrak{c}_{x,-o_i,e_i,-o_j,e_j} \\ -\mathfrak{c}^*_{x,-o_i,e_i,-o_j,e_j} & \bar{\mathfrak{v}}_{x,-o_j,e_j} \end{bmatrix}.$$

We now choose a positive measure μ with non-finite support on $(\rho, \bar{\rho})$, such that μ is small enough around ρ and $\bar{\rho}$. For example we can choose it with non-finite compact support in $(\rho, \bar{\rho})$. This is safe enough but it may be even better to take $\mu(x)dx$, where $\mu(x)$ is a suitable power of $1 - |x|^2 = 1 - x + x^2$ or equivalently $J(x) = (1 - x + x^2)^3 x^{-2}(x-1)^{-2}$. Then we integrate (2.7) over $(\rho, \bar{\rho})$. We define the integrals of the above operators:

$$\begin{aligned} \mathfrak{V}_{-o_i,e_i} &= \int \mathfrak{v}_{x,-o_i,e_i} d\mu \\ \mathfrak{V}_{-o_j,e_j} &= \int \mathfrak{v}_{x,-o_j,e_j} d\mu \\ \mathfrak{C}_{-o_i,e_i,-o_j,e_j} &= \int \mathfrak{c}_{x,-o_i,e_i,-o_j,e_j} d\mu \\ \mathfrak{J}_{-o_i,e_i,-o_j,e_j} &= \int \mathfrak{j}_{x,-o_i,e_i,-o_j,e_j} d\mu, \end{aligned}$$

and we obtain

$$\mathfrak{J}_{-o_i,e_i,-o_j,e_j} |a_{\vec{v},k}\rangle \oplus |a_{\vec{t},k}\rangle = 0. \tag{2.8}$$

This finishes the characterization of $\mathcal{L}(D)$. Indeed, the expansions in $\mathbf{J}$ associated to any function in $\mathcal{L}(D)$ must satisfy the above conditions. Reciprocaly, to any vector in $\mathbf{J}^{\mathbf{S}}$ satisfying those condition one associates $\mathbf{S}$ analytic functions defined on the unit disk. Because of the positiveness of the junction operators, we get compatibility relations between those functions at infinitely many points (the support of the distribution we chosed is infinite). Thus our functions can be patched together to form an analytic multivalued function with the expected monodromy. Because of the regularity imposed on the series in $\mathbf{J}$, we see that there are no other poles than the ones allowed by the divisor D.

We can now collect all the relations in a blockwise matrix. The blocks are universal junction matrices, and the disposition of all the blocks reflects the topology of the dessin since it comes from the action of the fundamental groupoid on the standards. We note that all the entries of the junction operators are of the form

$$\int x^a (1-x)^b d\mu$$

where a and b are rationals. We can think of expressing them with the beta function plus some hypergeometric functions.

Now, for the actual computation of a dessin we first choose a divisor on the dessin. For example, the Riemann-Hurwitz formula gives us a divisor which is in the canonical class, made up of ramification points. Indeed, if $\mathcal{D}$ is our dessin, we call P_i, Q_j, R_k the points above 0, 1, ∞ respectively, and p_i, q_j, r_k their multiplicities. If the dessin is clean, $q_j = 2$. We call $\mathcal{K}$ the following divisor, which is well known to be in the canonical class:

$$\mathcal{K} = -\sum_i (P_i) + \sum_j (q_j - 1)(Q_j) - \sum_k (R_k).$$

If the genus is greater than or equal to 2 then the divisor $2\mathcal{K}$ is very ample. We compute the associated linear space $\mathcal{L}(2\mathcal{K})$ with enough accuracy as the kernel of the operator introduced above. To achieve that, we choose a given precision P and write down the junction matrices, truncated at rank P. We then build a blockwise matrix corresponding to the above divisor, from the truncated junction matrices, and compute its kernel. Actually, this matrix, being no more than an approximation, is not very likely to have a kernel. We just look for vectors with small images under this matrix, using the least-squares method. This provides us with an explicit, though approximate, description of the linear space $\mathcal{L}(2\mathcal{K})$ given by some base $(f_1, .., f_{\ell(2\mathcal{K})})$ where the f_i are Puiseux series with P terms. This linear space defines an embedding of the curve in a projective space. By looking for algebraic dependancies between the f_i, we build an algebraic regular model $\mathcal{C}$ for the curve provide the genus is greater than or equal to 2 (if the genus is 0, a model of the curve is $\mathbb{P}_1$; if the genus is 1, we have some elliptic curve which can be determinated by looking at any ample divisor, although there exist simpler techniques).

Now it remains to compute the Belyi function $\varphi(f_1, .., f_{\ell(2\mathcal{K})})$ from $\mathcal{C}$ to $\mathbb{P}_1$. We first compute the linear space associated to the divisor $-(\varphi) = \sum_k r_k(R_k) - \sum_i p_i(P_i)$ just in the same way as above. It is of dimension 1, and we take a generator that we normalize with the conditions $\varphi(Q_j) = 1$. From all the Puiseux series expansions we have (both for φ and the f_i), we can express φ as an algebraic function of $(f_1, .., f_{\ell(2\mathcal{K})})$.

Of course, all that is quite tedious, and we must develop sharper techniques depending on the genus of the curve as we will see in the next section for genus 0.

Thanks to some *a priori* description, we can refine the approximation with an iterative method such as the one detailed below, which leads us to an algebraic exact solution over $\bar{\mathbb{Q}}$.

2.7 Iterative *ad hoc* methods

In this section we describe iterative methods to compute genus zero dessins as rational functions from $\mathbb{P}_{1/\mathbb{C}}$ to $\mathbb{P}_{1/\mathbb{C}}$. We compute the positions α_i, β_i and γ_i of the points over 0, 1 and ∞. Algebraic methods are feasible in the case of relatively small dessins of low degree; numerous examples are given in the articles by Shabat, Malle, Birch in [18]. However it is possible to do the calculations much more efficiently via approximation and iteration.

Our method consists of three stages:

- Computing approximations of the positions of the points with ad hoc methods.
- Use an iterative algorithm to obtain the numeric convergence and compute the positions with hundreds of digits. We obtain a very good approximation of the Belyi function.
- Find the number field where the coefficients of the Belyi function are. We use a lattice reduction.

We work all the way with the geometrical definition of the dessins: we try to compute some *canonical* positions of the vertices of a coloured triangulation of the curve. Thanks to this intuitive approach, we can occasionally help the computer with human intervention, if part of the solution seems obvious.

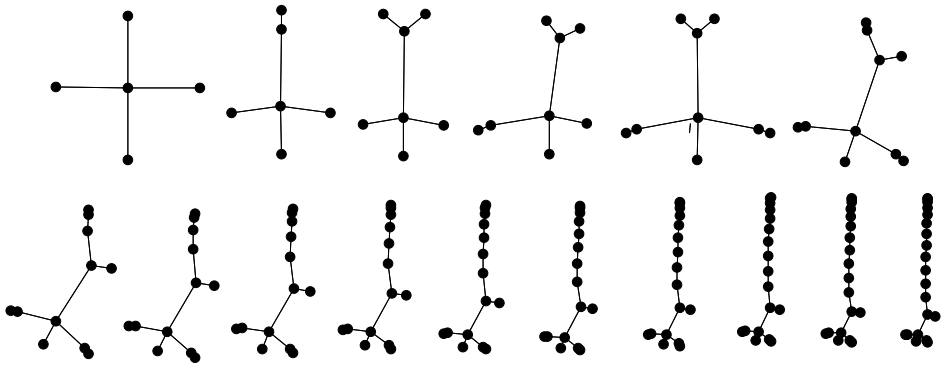
Finding the first approximation

The more general method uses Puiseux series, as stated in section 2.6, but this method needs memory and time, and cannot be used to analyse families of dessins.

In genus 0, we can use visual intuition and very quickly build an approximation of the Belyi function.

We can say that two dessins are close if their combinatorial structure is close. For example, if we add one vertex to a dessin, the resulting dessin has a similar shape. This leads to a method of *growing families of dessins* where we add branches to an initial seed.

Here is for example a family of dessins, with the vertices in their correct positions. We see that the deformation caused by adding a point is small, so each time we can build an approximation of the positions of the vertices from the previous dessin.



This stage needs our intuition, so we can place the new point near its future position with visual considerations such as the regularity of the graph $\phi^{-1}([0,1])$ and the local symmetry around a vertex.

Numeric convergence

The second stage consists in solving some equations to find the position of the vertices with arbitrary precision.

We want to have a good system of equations, so as to really be able to compute the solutions with our computer. This system must be as simple and as small as

possible and it must be stable, so we can converge to the exact solution even with rough approximations.

The case of trees

A dessin is called a "tree" if it is clean, of genus 0 and totally ramified over ∞.

If the dessin is a tree, there is a system of polynomial equations in the coordinates of the vertices, that is easy to compute and easy to solve.

We write A the set of the N vertices of the dessin and B the set of the edges. We write ϕ a Belyi function of degree d, it is a rational function with ramification points $(\alpha_i)_{i\in A}$ of degree ν_i over 0, ramification points $(\beta_j)_{j\in B}$ of degree 2 over 1 and totally ramified over ∞. Hence we can write, if we put ∞ over ∞:

$$\phi = \frac{-1}{\lambda}\prod_{i\in A}(X-\alpha_i)^{\nu_i} = \frac{-1}{\lambda}\left(\prod_{i\in B}(X-\beta_i)\right)^2 + 1$$

Since we fixed ∞ over ∞, the positions of the vertices are defined up to an affine transformation: we have 2 degrees of liberty.

Now we have an equation in the positions of the vertices (α_i) and the segments (β_i):

$$\prod_{i\in A}(X-\alpha_i)^{\nu_i} = \left(\prod_{i\in B}(X-\beta_i)\right)^2 - \lambda \qquad \text{which we write as:} \quad \Pi = Q^2 - \lambda \qquad (2.9)$$

This is the equation used by Atkin in [5] and Shabat and Birch in [18]. This system could be solved with a Gröbner basis reduction algorithm, but the dessin should not be too large.

We want to build a better system of equations. We want to reduce the number of unknowns and obtain a system of equations independent of the (β_i).

We can factor the right-hand part of the equation (2.9): $Q^2 - \lambda = \left(Q-\sqrt{\lambda}\right)\left(Q+\sqrt{\lambda}\right)$, so we can split the set of vertices A in two subsets A^+ and A^- – the blue and the red vertices – such that $i \in A^+$ if and only if $Q(\alpha_i) = +\sqrt{\lambda}$. We factor the left-hand part of equation (2.9):

$$\Pi^+ = \prod_{i\in A^+}(X-\alpha_i)^{\nu_i} = \left(Q+\sqrt{\lambda}\right)$$

$$\Pi^- = \prod_{i\in A^-}(X-\alpha_i)^{\nu_i} = \left(Q-\sqrt{\lambda}\right)$$

We use the notation:

$$\Theta = \prod_{i\in A}(X-\alpha_i)$$

$$\Sigma = \sum_{i\in A}\frac{\nu_i}{X-\alpha_i} \qquad \Sigma^+ = \sum_{i\in A^+}\frac{\nu_i}{X-\alpha_i} \qquad \Sigma^- = \sum_{i\in A^-}\frac{\nu_i}{X-\alpha_i}$$

$$\sigma = \Theta\Sigma \qquad \sigma^+ = \Theta\Sigma^+ \qquad \sigma^- = \Theta\Sigma^-$$

to differentiate equation (2.9):

$$\Pi\Sigma = 2QQ' \quad \text{i.e.} \quad \frac{\Pi}{\Theta}\sigma = 2QQ'$$

but since Q is prime to Π and to $\frac{\Pi}{\Theta}$, we deduce

$$\sigma = dQ \text{ i.e. } \sigma^+ + \sigma^- = dQ \tag{2.10}$$

Now, we can compute $\sigma^+ - \sigma^-$, and we obtain an equation with the (α_i) and λ but without the (β_i).

$$\sigma^+ - \sigma^- = d\sqrt{\lambda} \tag{2.11}$$

because $(\sigma^+ - \sigma^-) - d\sqrt{\lambda}$ is a polynomial of degree less than $N-1$ with N distinct roots:
for i in A^+, $(\sigma^+ - \sigma^-)(\alpha_i) = \sigma^+(\alpha_i) = dQ(\alpha_i) = d\sqrt{\lambda}$
for i in A^-, $(\sigma^+ - \sigma^-)(\alpha_i) = -\sigma^-(\alpha_i) = -dQ(\alpha_i) = d\sqrt{\lambda}$.

If we add and substract equations (2.10) and (2.11), we obtain a system in the (α_i) that respects the coloration of the vertices:

$$2\sigma^+ = d\Pi^- \text{ and } 2\sigma^- = d\Pi^+.$$

Let us define $\bar{\nu}_i = \nu_i$ for $i \in A^+$ and $\bar{\nu}_i = -\nu_i$ for $i \in A^-$. Equation (2.11) divided by Θ and with $U = 1/X$ is

$$\frac{d\sqrt{\lambda}U^{N-1}}{\prod_{i\in A}(1-U\alpha_i)} = \sum_{i\in A^+}\frac{\nu_i}{1-U\alpha_i} - \sum_{i\in A^-}\frac{\nu_i}{1-U\alpha_i} = \sum_{i\in A}\frac{\bar{\nu}_i}{1-U\alpha_i}.$$

Now, λ does not interfere with the terms of degree less than N; to eliminate λ, we write down the $N-1$ first terms of the Taylor expansion of this equation:

$$\forall\, 0 \le k \le N-2, \qquad \sum_{i\in A}\bar{\nu}_i\alpha_i^k = 0 \tag{2.12}$$

The equation for $k=0$ is trivial, so we have $N-2$ equations for N indeterminates. The set of solutions is invariant under affine transformations $(\alpha_i)_i \mapsto (A\alpha_i + B)_i$.

We add a few inequalities to the system, namely $\alpha_i \neq \alpha_j$ if $i \neq j$. This defines a smooth variety of dimension 2 in the space of dimension N. If we quotient this by the action of the group of affine transformations, we get a variety of dimension 0 in $\mathbb{P}_{N-2/\mathbb{C}}$. It is not necessarily a single point, not even necessarily irreducible over $\mathbb{Q}$, but one point must correspond to our Belyi function.

That proves that our system has a unique solution near our first approximation: the dessin we want to compute.

The case of dessins with all ramification orders even

If all the ramification orders of the dessin are even, we obtain equations similar to (2.12).

Let α_i, of ramification $2\nu_i$, denote the vertices and γ_i of ramification $2\mu_i$ the faces. Since all ramification indices are even, we can colour the vertices and the faces. We denote $\bar{\nu}_i$ and $\bar{\mu}_i$ the algebraic ramifications.

Then we have the system:

$$\forall\, i, \quad \forall\, 0 \le k \le \nu_i - 1, \qquad \sum_j \frac{\bar{\mu}_j}{(\gamma_j - \alpha_i)^k} = 0$$

$$\forall\, j, \quad \forall\, 0 \leq k \leq \mu_j - 1, \qquad \sum_i \frac{\bar{\nu}_i}{(\alpha_i - \gamma_j)^k} = 0.$$

Solving the system

The system (2.12) is a Vandermonde-like system. Let $\mathcal{A} = (\alpha_1, ..., \alpha_N)$ and the function $\mathcal{F}(\mathcal{A}) = (\sum_{i \in A} \bar{\nu}_i \alpha_i^k)_{k=1...N-2}$ be such that our system is $\mathcal{F}(\mathcal{A}) = 0$.

Newton's algorithm for solving such equations begins with an approximation of the solution $\mathcal{A}_0$ and iterates the formula: $\mathcal{A}_{n+1} = \mathcal{A}_n - {\mathcal{F}'_{\mathcal{A}_n}}^{-1} \mathcal{F}(\mathcal{A}_n)$.

But $\mathcal{F}'_{\mathcal{A}_n}$ is not invertible and ${\mathcal{F}'_{\mathcal{A}_n}}^{-1}$ is defined up to an element of the kernel. We choose a vector orthogonal to the kernel.

Now we have a method to solve $\mathcal{F}(\mathcal{A}) = 0$, but we must be careful: the numeric representation forces us to work with $\mathcal{A}_n \in \mathbb{C}^N$, but we must be aware that $\mathcal{A}_n$ is defined up to some affine transformation.

We must normalize the $\mathcal{A}_n$ to avoid a shift to infinity. We fix the center of the dessin at 0, and the scale of the dessin to a diameter of 1. The sum of the coordinates of the vertices is 0 and the maximal distance between two vertices is 1.

To handle large numbers, we use the PARI library.

Back to the algebraic point of view

The third stage uses the powerful lattice reduction tools to go from the geometrical point of view to the algebraic description: given very precise complex approximations of algebraic complex numbers, we build a lattice such that the shortest vector of this lattice gives the minimal polynomial. We use the method described in [32].

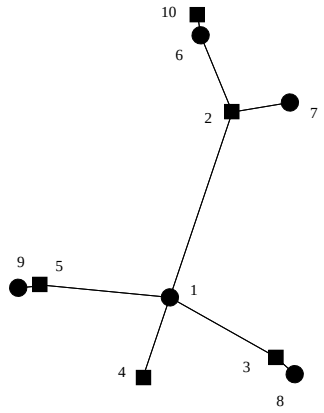
The problem of finding a short vector in an integer lattice is hard, but efficient algorithms have been published in [32], [37] and [38]. We use the efficient implementation of Antoine Joux ([25]) on a SparcStation 10.

The previous stage allows us to compute these numbers to any desired precision. However, a priori we do not know what precision is necessary to find the exact solution with the lattice reduction method. We compute upper bounds for the degree and we guess the size of the coefficients of the polynomial.

The degree is lower than the number of "combinatorial" conjugates of the dessin i.e. the cardinal of the variety of dimension 0 in $\mathbb{P}_{N-2/\mathbb{C}}$, solution of our system. This number can be approximated by character formulae, see [42].

Application to an example

Consider the dessin given by this graph, a tree with 10 vertices:



It is the 6th of the family of dessins shown above. We make the tree grow step by step, and then we compute the solution to 2000 digits. We normalise the sum of vertices to 0.

Then the minimal polynomial of α_1/α_2 is the polynomial given here, of degree 24 and of discriminant $-1.2^{799}.3^{270}.5^{90}.7^{54}.N^2$ (N is a large number with no smaller factor than 127):

$$
\begin{aligned}
&1216396531470080000\,x^{24} + 15167128532892096000\,x^{23}\\
&+88567164003405619200\,x^{22} + 320465331330548463040\,x^{21}\\
&+801926461469806116168\,x^{20} + 1468854325860309911334\,x^{19}\\
&+2037128673503852027315\,x^{18} + 2189254042743982149456\,x^{17}\\
&+1858352449953325455855\,x^{16} + 1271096908385844699688\,x^{15}\\
&+717291487653207390204\,x^{14} + 342482003051130999024\,x^{13}\\
&+140622333198259937516\,x^{12} + 49205805780202178532\,x^{11}\\
&+13997991682162739850\,x^{10} + 2897517763455570160\,x^{9}\\
&+284441186456050050\,x^{8} - 67794459856593624\,x^{7}\\
&-41017353384312340\,x^{6} - 10862737575891504\,x^{5}\\
&-1796582490031788\,x^{4} - 178029020920154\,x^{3}\\
&-7529198821413\,x^{2} + 14589968448\,x - 34245281017
\end{aligned}
$$

Note that the leading coefficient $1216396531470080000 = 2^{11}.5^4.950309790211$.

Chapitre 3

Racines carrées et factorisation d'entiers

Ce chapitre doit beaucoup à l'obligeance d'Hendrik Lenstra qui a bien voulu le relire pour en corriger tant la langue que le contenu. Il a été publié dans le volume "The development of the number field sieve" édité par A.K. et H.W. Lenstra [15].

The number field sieve is a method proposed by Lenstra, Lenstra, Manasse and Pollard for integer factorization in [33]. A heuristic analysis indicates that this method is asymptotically faster than any other existing one. It has had spectacular successes in factoring numbers of a special form. New technical difficulties arise when the method is adapted for general numbers ([10]). Among these is the need for computing the square root of a huge algebraic integer given as a product of hundreds of thousands of small ones. We present a method for computing such a square root that avoids excessively large numbers. It works only if the degree of the number field that is used is odd. The method is based on a careful use of the Chinese remainder theorem.

3.1 Introduction

We begin by recalling the basic scheme of the number field sieve, cf. [33]. Let n be a positive integer that is not a power of a prime number. In order to factor n, we first find many congruences modulo n involving a given set of numbers called the *basis*. This is done by means of a suitable ring of algebraic integers. To construct this ring, one chooses a positive integer d, which is the degree of the ring to be constructed; if n has between 110 and 160 decimal digits then $d = 5$ is a good choice. Next one chooses a monic polynomial $f \in \mathbb{Z}[X]$ of degree d that represents n, i. e., $f(m) = n$ for some integer m. We want both m and the coefficients of f to be as small as possible. Indeed, we can easily make them smaller than $n^{1/d}$. Now, if f is reducible, then a non-trivial factor h of f should give a non-trivial factor $h(m)$ of n. Otherwise, we consider the number field $K = \mathbb{Q}[X]/(f)$ together with the morphism φ from the order $\mathbb{Z}[\alpha]$ to $\mathbb{Z}/n\mathbb{Z}$ for which $\varphi(\alpha) = m$, where we write $\alpha = (X \bmod f)$. We then look for algebraic numbers of the form $a + b\alpha$ such that both $a + bm$ and $a + b\alpha$ are *smooth*. This means that, for a suitable positive integer y chosen at the beginning, both $a + bm$ and the norm $\mathbb{N}(a + b\alpha)$ of $a + b\alpha$ are integers divisible only by prime numbers not exceeding y. With each prime number $p \leq y$ we associate a function $\nu_p : \mathbb{Z} - \{0\} \to \mathbb{Z}/2\mathbb{Z}$, which

assigns to any non-zero integer k the residue class modulo 2 of the number of factors p in k. In the same way, we associate with any prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\alpha]$ of norm at most y the function $\nu_{\mathfrak{p}}: \mathbb{Z}[\alpha] - \{0\} \to \mathbb{Z}/2\mathbb{Z}$ that maps an element to the residue class modulo 2 of the number of factors $\mathfrak{p}$ appearing in that element (cf. [10, Section 5]).

As suggested by Adleman [1], we also use characters obtained in the following way. Choose a collection of non-zero prime ideals $\mathfrak{q}$ of $\mathbb{Z}[\alpha]$ that are different from all primes $\mathfrak{p}$ used before and that do not divide the discriminant of f. With each such $\mathfrak{q}$ we associate the function $\chi_{\mathfrak{q}}: \mathbb{Z}[\alpha] - \mathfrak{q} \to \mathbb{Z}/2\mathbb{Z}$ defined by

$$\chi_{\mathfrak{q}}(x) = \begin{cases} 0 & \text{if } x \text{ is a square modulo } \mathfrak{q}, \\ 1 & \text{otherwise.} \end{cases}$$

The first part of the algorithm consists of the search for many pairs (a, b) of relatively prime rational integers for which both $a + bm$ and $a + b\alpha$ are smooth, and $a + bm > 0$. In the second part one looks for subsets S of the set of pairs that have been found for which

$$\prod_{(a,b)\in S} (a + bm) \quad \text{is a square in } \mathbb{Z},$$
$$\prod_{(a,b)\in S} (a + b\alpha) \quad \text{is a square in } K.$$

One hopes that this is ensured by the following three conditions:

$$\begin{aligned}
\sum_{(a,b)\in S} \nu_p(a + bm) &= 0 \bmod 2 && \text{for all prime numbers } p \le y, \\
\sum_{(a,b)\in S} \nu_{\mathfrak{p}}(a + b\alpha) &= 0 \bmod 2 && \text{for all prime ideals } \mathfrak{p} \text{ of } \mathbb{Z}[\alpha] \text{ of norm } \le y, \\
\sum_{(a,b)\in S} \chi_{\mathfrak{q}}(a + b\alpha) &= 0 \bmod 2 && \text{for all } \mathfrak{q} \text{ that have been chosen.}
\end{aligned}$$

Indeed, these conditions are necessary. If enough characters $\chi_{\mathfrak{q}}$ have been chosen then one may expect that the conditions are sufficient as well.

This leads to a large algebraic number γ that is given as a product of many small ones, and that is a square in $\mathbb{Z}[\alpha]$ (see [10]):

$$\gamma = f'(\alpha)^2 \cdot \prod_{(a,b)\in S} (a + b\alpha) = \beta^2 \qquad \text{with } \beta \in \mathbb{Z}[\alpha]. \tag{3.1}$$

We also know that the image of γ under φ,

$$\varphi(\gamma) = f'(m)^2 \cdot \prod_{(a,b)\in S} (a + bm) \bmod n,$$

satisfies

$$f'(m)^2 \cdot \prod_{(a,b)\in S} (a + bm) = f'(m)^2 \cdot \prod_{p\le y} p^{2e_p} = v^2,$$

where the integers e_p can be determined from the prime factorization of the numbers $a + bm$, and where

$$v = f'(m) \cdot \prod_{p\le y} p^{e_p}.$$

As for β, we know its decomposition as an *ideal* of $\mathbb{Z}[\alpha]$; but since we do not know generators for the prime ideals of norm at most y, this does not enable us to write down an explicit expression for β itself. However, we do know an expression for the *norm* of β:

$$\mathbb{N}(\beta) = \pm\mathbb{N}(f'(\alpha)) \cdot \prod_{p \le y} p^{f_p}, \tag{3.2}$$

where the f_p are non-negative integers that can be determined from the prime ideal decomposition of β. Furthermore, since $\beta \in \mathbb{Z}[\alpha]$ there exists a polynomial $B \in \mathbb{Z}[X]$ of degree at most $d-1$ such that $\beta = B(\alpha)$. We shall compute this polynomial.

The method suggested in [10] is as follows. First, look for an odd prime q such that the polynomial f remains irreducible modulo q. Then, compute γ mod q by performing all multiplications in the product (3.1) modulo q. We view γ mod q as an element of the finite field $\mathbb{F}_{q^d}$, and we can easily compute the square roots of this element. Next, we choose one of the two square roots and lift it to a square root modulo q^2, q^4, q^8, ..., using Newton's method, until the modulus is larger than twice a given estimate of the size of the coefficients of B. In this manner we find B. The congruence

$$B(m)^2 = \varphi(\beta)^2 = \varphi(\beta^2) = \varphi(\gamma) = v^2 \bmod n$$

suggests that $\gcd(B(m) - v, n)$ has a good chance to be a non-trivial factor of n.

One of the difficulties with this method is the very large size of the numbers that occur in the last iterations of Newton's method. The time taken by this computation is comparable to the time taken by the entire algorithm, except if one uses fast multiplication techniques; but even if that is done one may have serious practical difficulties with the very large integers that arise. It is particularly disconcerting that the huge numbers that we compute are ultimately replaced by their remainder modulo n.

The approach that we suggest is to work with many different moduli $m_i = q_i^{k_i}$, where the q_i are distinct odd primes for which f is irreducible modulo q_i. We first compute, as above, a square root β_i of γ modulo each m_i, i.e., a polynomial $B_i \in \mathbb{Z}[X]$ of degree at most $d-1$ such that $\beta_i = B_i(\alpha)$ satisfies $\beta_i^2 \equiv \gamma \bmod m_i$; the coefficients of B_i matter only modulo m_i. If $\beta = B(\alpha)$ denotes, as above, one of the two square roots of γ in $\mathbb{Z}[\alpha]$, then we have $\beta_i = \pm\beta \bmod m_i$, where the signs are *a priori* unknown. Our first problem is to compute those signs or, equivalently, to make sure that the various β_i are congruent to the *same* square root β modulo m_i. Next, using the Chinese remainder theorem, we can compute $\beta = B(\alpha) \in \mathbb{Z}[\alpha]$ and $\varphi(\beta) = (B(m) \bmod n) \in \mathbb{Z}/n\mathbb{Z}$. However, the coefficients of B and the number $B(m)$ are so large one should avoid explicitly calculating any of them. We shall see that once the $B(m) \bmod m_i$ are known, we can compute $B(m)$ modulo n without computing B or $B(m)$ itself.

3.2 Description and analysis of the method

We first consider the sign problem discussed at the end of Section 1.1. We shall make the assumption that the degree of the extension $K/\mathbb{Q}$ is *odd*. The basic observation is that, under this hypothesis, we have $\mathbb{N}(-x) = -\mathbb{N}(x)$ for any non-zero element x of K. Hence, exactly one of the two square roots of γ has positive norm. Let that one be called β. Suppose, as above, that we know a square root $\beta_i = B_i(\alpha)$ of γ modulo $m_i = q_i^{k_i}$ for each i, and that we want to test whether $\beta_i \equiv \beta \bmod m_i$ or $\beta_i \equiv -\beta \bmod m_i$. We can

decide this by looking modulo q_i. Thus, we compute the norm of $(\beta_i \bmod q_i)$, viewed as an element of the finite field of cardinality q_i^d; this norm is the $(q_i^d-1)/(q_i-1)$th power of $(\beta_i \bmod q_i)$, and it belongs to the prime field $\mathbb{Z}/q_i\mathbb{Z}$. We compare this norm with the residue modulo q_i of the norm of β, which is computed by means of formula (3.2), but with $\pm\mathbb{N}(f'(\alpha))$ replaced by its absolute value; the multiplications in (3.2) are performed modulo q_i. If the two norms are equal, then $\beta_i \equiv \beta \bmod m_i$, and we keep B_i. If they are opposite, then we replace B_i by $-B_i$.

Substituting m in B_i we find $B(m)$ modulo m_i for all i, and we wish to compute $B(m)$ modulo n. We discuss this problem in a more general setting.

3.2.1 Changing moduli.

In *modular arithmetic* one represents an integer by means of its residue classes modulo each of a set of pairwise coprime integers m_i. The theoretical basis of modular arithmetic is formed by the Chinese remainder theorem. An introduction to the algorithmic aspects of modular arithmetic, and a discussion of its applications, can be found in [28, Section 4.3.2].

We consider the following algorithmic problem from modular arithmetic (cf. [35, Section 4]). One is given a collection of pairwise coprime positive integers m_i, a positive integer n, for each i an integer x_i with $0 \le x_i < m_i$, and a small positive real number ϵ, for example $\epsilon = 0.01$. In addition, one is provided with the information that there exists an integer x satisfying $x \equiv x_i \bmod m_i$ for each i, and $|x| < (\frac{1}{2}-\epsilon)\prod_i m_i$; clearly, such an integer x is unique if it exists. The question is to compute the residue class of x modulo n.

If we define the quantities

$$M = \prod_i m_i, \tag{3.3}$$

$$M_i = \prod_{j \neq i} m_j = M/m_i, \tag{3.4}$$

$$a_i = 1/M_i \bmod m_i, \qquad 0 \le a_i < m_i, \tag{3.5}$$

then the number $z = \sum_i a_i M_i x_i$ is congruent to x modulo M. Hence, if we round z/M to an integer: $r = [\frac{z}{M} + \frac{1}{2}]$, then we have $x = z - rM$. The point is that we can calculate r without calculating the possibly very large number z, as follows.

From $x = z - rM$ and our hypothesis $|x| < (\frac{1}{2}-\epsilon)M$ it follows that $\frac{z}{M} + \frac{1}{2}$ is not within ϵ of an integer. Hence, to calculate r it suffices to know an approximation t to z/M with $|t - z/M| < \epsilon$. Such an approximation can be obtained from

$$\frac{z}{M} = \sum_i \frac{a_i x_i}{m_i}. \tag{3.6}$$

All terms in the sum are between 0 and $\max_i m_i$, so they can be computed as low precision real numbers.

This results in the following algorithm. Denote by $\mathrm{rem}(a,b)$ the remainder of the Euclidean division of a by b.

1. For each i, compute $\mathrm{rem}(M_i, m_i)$ by multiplying out the product (3.4) modulo m_i, and compute the numbers a_i as in (3.5) with the extended Euclidean algorithm.

2. Compute $\mathrm{rem}(M, n)$ by multiplying out the product (3.3) modulo n, and compute $\mathrm{rem}(M_i, n)$ for each i; if $\gcd(m_i, n) = 1$ one can do this by dividing $\mathrm{rem}(M, n)$ by m_i modulo n;

3. Compute a number t that differs by less than ϵ from the sum in (3.6), and round t to an integer: $r = [t + \frac{1}{2}]$.

4. Output

$$\mathrm{rem}(x, n) = \mathrm{rem}\Big(\Big(\sum_i a_i \,\mathrm{rem}(M_i, n) x_i\Big) - r\,\mathrm{rem}(M, n), n\Big).$$

(If m_i is much larger than n one may prefer to replace a_i and x_i by $\mathrm{rem}(a_i, n)$ and $\mathrm{rem}(x_i, n)$ in this expression.)

Note that we never handle numbers substantially larger than the moduli.

3.2.2 Size and complexity.

We derive upper bounds for the integers b_i for which $\beta = b_0 + b_1\alpha + \ldots + b_{d-1}\alpha^{d-1}$, with β as in (3.1). For $f = \sum_{i=0}^{d} a_i X^i$ we write $\|f\| = \big(\sum_{i=0}^{d} a_i^2\big)^{1/2}$, and we let u be an upper bound for all numbers $|a|$, $|b|$ for which $(a, b) \in S$.

Proposition 3.2.1 *We have*

$$|b_i| \le d^{3/2} \cdot \|f\|^{d-i} \cdot (2u\|f\|)^{\#S/2}$$

for $0 \le i \le d - 1$.

Proof. The field K has d embeddings into the field of complex numbers, and we denote the image of an element $\epsilon \in K$ under the kth embedding by $\epsilon^{(k)}$. We have $f = \prod_{i=1}^{d}(X - \alpha^{(i)})$, and

$$\max(1, |\alpha^{(k)}|) \le \prod_{j=1}^{d} \max(1, |\alpha^{(j)}|) \le \|f\| \tag{3.7}$$

for each k; the first inequality is trivial, and the second is due to Landau [29][34, Chapitre IV, Section 3.3].

Let $\delta_0, \delta_1, \ldots, \delta_{d-1} \in K$ be defined by $\sum_{i=0}^{d-1} \delta_i X^i = f/(X - \alpha)$, so that $\delta_i = \sum_{j=0}^{d-1-i} a_{i+j+1}\alpha^j$. By [30, Chapter III, Proposition 2] we have

$$b_i = \mathrm{Tr}(\delta_i \beta / f'(\alpha)) = \sum_{k=1}^{d} \delta_i^{(k)} \beta^{(k)} / f'(\alpha^{(k)}), \tag{3.8}$$

where $\mathrm{Tr}\colon K \to \mathbb{Q}$ is the trace function. The Cauchy-Schwarz inequality and (3.7) imply that

$$|\delta_i^{(k)}|^2 \le \|f\|^2 \cdot \sum_{j=0}^{d-1-i} |\alpha^{(k)}|^{2j} \le d \cdot \|f\|^{2(d-i)} \qquad (0 \le i \le d-1).$$

From

$$|\beta^{(k)}/f'(\alpha^{(k)})|^2 = \prod_{(a,b)\in S} |a + b\alpha^{(k)}| \leq (2u\|f\|)^{\#S}$$

we now obtain

$$|b_i| = \left|\sum_{k=1}^{d} \delta_i^{(k)} \beta^{(k)}/f'(\alpha^{(k)})\right| \leq d^{3/2} \cdot \|f\|^{d-i} \cdot (2u\|f\|)^{\#S/2},$$

as required.

If f is chosen as in [10], then we have $\|f\| \leq \sqrt{d} \cdot n^{1/d}$ and $|m| \leq n^{1/d}$, and therefore

$$|B(m)| \leq d^{(d+5)/2} \cdot n \cdot (2u\sqrt{d}n^{1/d})^{\#S/2}. \tag{3.9}$$

Note that the three factors in this upper bound are of completely different orders of magnitude. In realistic cases, the last factor has millions of decimal digits, the middle one has between one and two hundred digits, and the first one has just a few digits. We refer to [10, 9.3 and Section 11] for an estimate of u and $\#S$ as functions of n and d.

The estimate (3.9) is good enough to enable us to get a rough impression of the precision needed, i. e., the number and size of moduli m_i. Note that too many moduli would make us waste time, while not enough moduli would give an incorrect result. In order to get a more accurate estimate, we can explicitly compute the zeroes $\alpha^{(k)}$ of f as low precision complex numbers. We can then evaluate the complex numbers $\delta_i^{(k)}$ and $f'(\alpha^{(k)})$, and, multiplying out the product (3.1), the real numbers $|\beta^{(k)}|$. Then we obtain from (3.8) an upper bound for $|b_i|$. This leads to an upper bound for $B(m)$ that is better than (3.9).

We now give a rough estimate of the complexity of our method as a function of the logarithm of an upper bound like (3.9) for $B(m)$; let this logarithm be called s. For the sake of comparison, we mention that the square root method proposed in [10] takes time $s^{1+o(1)}$ if fast multiplication techniques are used, and $s^{2+o(1)}$ otherwise, and that the entire number field sieve is conjectured to run in time $s^{2+o(1)}$, see [10, 9.3 and Section 11]; here and below the $o(1)$ is for $n \to \infty$. The time taken by our method depends on the size and the number of the moduli, and on whether or not fast multiplication techniques are used. We consider two extreme cases.

In the first case the moduli are chosen as small as possible. We assume, heuristically, that f is irreducible modulo one out of every d primes (see the remark below). We take the m_i to be the first $ds(1 + o(1))/\log(ds)$ such primes. Their product will then be $s^{1+o(1)}$, which is large enough for the algorithm of 3.2.1. From $d = s^{o(1)}$ one sees that both the number of moduli and the largest of them is of the order $s^{1+o(1)}$. The most time-consuming part of the method is the computation of the product (3.1) modulo each m_i. This requires $s^{2+o(1)}$ multiplications. Since all multiplications are done with small numbers, it is not clear how fast multiplication techniques can help at all. It is conceivable, though, that the computation can be speeded up by some divide-and-conquer technique.

The second extreme possibility is to fix the number of moduli and to choose each m_i to be $\exp(s^{1+o(1)})$ for some positive constant c. In this case we can use fast multiplication, and the time taken is $s^{1+o(1)}$. This is also achieved in [10] by means of a single modulus. With this choice of moduli one does ultimately handle very large integers.

The conclusion is that from a theoretical point of view our method does not represent an improvement over [10]. In practice, however, our method has the advantage of offering the possibility to work with much smaller numbers, and in addition it can be run in parallel. The number and the size of the moduli to be used depend strongly on the features of the available computing equipment. In [8] many small moduli are chosen, which is justified by the use of a massively parallel computer. One can imagine that in other situations it is desirable to use larger moduli so as to take advantage of sophisticated multiplication techniques. In principle it is not necessary to let the moduli be of the same approximate size: if several different computers are used, then one can adapt the sizes of the moduli to the individual machines.

Remark. It was pointed out in [10] that primes q for which f is irreducible modulo q do not necessarily exist, but that for "most" f one may expect that one out of every d primes has this property (see [44]). If the degree d, which we assumed to be odd, is a prime number, then indeed every irreducible polynomial $f \in \mathbb{Z}[X]$ of degree d remains irreducible modulo at least one out of every d primes (asymptotically). This applies in particular to $d = 3$, 5, and 7. For the proof it suffices, by the argument of [10, Proposition 9.1], to show that every transitive permutation group G of prime degree d contains at least $\#G/d$ cycles of length d. Indeed, by Cauchy's theorem G has an element of order d, and this element must be a d-cycle. Letting G act by conjugation on the set of its d-cycles one finds that the number of d-cycles is divisible by $\#G/d$, as required.

The complete algorithm may be summarized as follows.

Algorithm. Let the integers n and m, the integer $v \bmod n$, the polynomial f, and the set S of pairs (a, b) be given, as in the number field sieve. This algorithm determines the possibly trivial factorization of n that the set S gives rise to.

1. Choose the moduli $m_i = q_i^{k_i}$ according to the above remarks. This necessitates the computation of complex approximations to the $\alpha^{(i)}$ and $|\beta^{(i)}|$.

2. Compute for each i the numbers $\mathrm{rem}(M_i, m_i)$, a_i, and $\mathrm{rem}(M_i, n)$ as in 3.2.1.

3. For each modulus m_i, compute the product

$$\gamma_i = f'^2 \cdot \prod_{(a,b)\in S} (a + bX) \bmod (f, m_i),$$

   as well as a square root β_i of γ_i.

4. Compute $N_{1,i}$, the norm of $\beta_i \bmod q_i$, and $N_{2,i}$, the product in (3.2) modulo q_i. If $N_{1,i} \neq N_{2,i}$ then replace β_i by $-\beta_i$. Let $B_i \in \mathbb{Z}[X]$ be a polynomial of degree $\leq d - 1$ for which $\beta_i = B_i \bmod (f, m_i)$, and compute $B_i(m)$ (modulo m_i). This step is to be performed for each i.

5. Compute $B(m) \bmod n$ from the $B_i(m)$ using the quantities calculated in step 2 (see 3.2.1).

6. Output $\gcd(B(m) - v, n)$.

Note that steps 3 and 4 can be parallelized.

Chapitre 4

Calcul des isogénies et cardinalité de courbes elliptiques

Dans mon travail sur les courbes elliptiques, j'ai été constamment aidé par François Morain. Les sections 4.1 et 4.2 ont été publiées dans un article écrit en commun, dont elles forment la première moitié [14]. La section 4.3 ne devrait pas connaître un sort trés différent. Je remercie René Schoof pour ses remarques concernant la section 4.3.

The heart of Schoof's algorithm for computing the cardinality m of an elliptic curve over a finite field is the computation of m modulo small primes ℓ. Elkies and Atkin have designed practical improvements to the basic algorithm, that make use of "good" primes ℓ. We show how to use powers of good primes in an efficient way. This is done by computing isogenies between curves over the ground field. We show as well how Elkies's ideas can be generalized to the case when the characteristic of the field is small.

An introduction to those questions can be found in the two papers by Morain and Schoof that will appear soon in the proceedings of the *Journées arithmétiques* at Bordeaux (1993) [36], [40].

4.1 A rough description of Schoof-Atkin-Elkies ideas

In this section, we assume for simplicity that the characteristic of the field is different from 2 and 3. The whole theoretical background for this section can be found in [24] chapters 12 and 13.

Let E be some elliptic curve over a primitive finite field $\mathbb{F}_q$ where $q = p^k$ and p is a prime integer. The curve is given by some equation $\mathcal{E} = 0$ in Weierstrass form

$$\mathcal{E} = Y^2 - X^3 - AX - B = 0,$$

so that a generic point on the curve is given by

$$(X, Y) \bmod \mathcal{E}.$$

We assume that ℓ is odd.

We recall that if π denotes the Frobenius action on the curve, π induces an automorphism of the ℓ-torsion space $E[\ell]$ which extends to Tate's module $T_\ell(E)$. The

ring of endomorphisms of the curve contains $\mathbb{Z}[\pi]$ and π satisfies the following degree 2 equation

$$\pi^2 - t\pi + q = 0,$$

where t is related to the cardinality of the curve by

$$\#E = q + 1 - t,$$

Of course, the same equality holds if we consider π as an element of $GL(E[\ell])$ or $GL(T_\ell(E))$. This remark leads to Schoof's idea: compute t modulo ℓ by looking at the action of π on the ℓ-torsion.

To achieve this goal, one first needs to compute the ℓ-torsion polynomial of E, $f_\ell^E(X)$, using the recurrence formulae. Then, a non zero ℓ-torsion point on E is given by

$$(X, Y) \,\mathbf{mod}\, (\mathcal{E}(X, Y), f_\ell^E(X)),$$

so that, for any $\lambda \,\mathbf{mod}\, \ell$ a residue modulo ℓ, one can test whether the trace of π is λ by checking the following identity, written in homogeneous coordinates:

$$(X^{q^2}, Y^{q^2}, 1) \ominus [\lambda](X^q, Y^q, 1) \oplus [q](X, Y, 1) = (0, 1, 0) \,\mathbf{mod}\, (\mathcal{E}, f_\ell^E).$$

For some λ the above equality will hold thus giving $t \,\mathbf{mod}\, \ell$. If one does the same computation for enough primes ℓ_i (i.e. such that $\prod_i \ell_i > 4\sqrt{q}$), then one knows the cardinality of E.

This leads to a polynomial time algorithm. The problem anyway is the size of the torsion polynomials. Indeed, $f_\ell^E(X)$ is of degree $(\ell^2 - 1)/2$. In practice one cannot hope to compute $\#E \,\mathbf{mod}\, \ell$ for ℓ greater than 40.

The center of Elkies' ideas ([19]) is that if $disc(\pi) = t^2 - 4q$ is a non-zero square modulo ℓ (the zero case works as well but in a slightly different way) then π has two rational distinct proper values τ_1 and τ_2 in $\mathbb{F}_\ell$ and even in $\mathbb{Z}_\ell$. Then, Tate's module decomposes as a sum of the two corresponding rational proper subspaces

$$T_\ell(E) = T_1^E \oplus T_2^E$$

and the ℓ-torsion as well.

We know that there exist $\ell + 1$ isogenies of degree ℓ

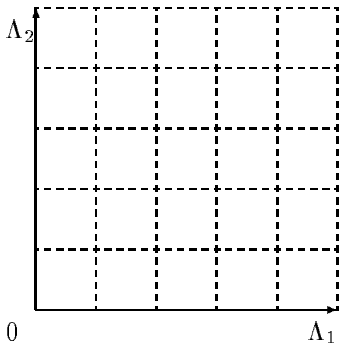
$$E \stackrel{I_u}{\rightarrow} E_u \ , 1 \leq u \leq \ell + 1$$

and we are looking for some explicit knowledge about these isogenies, such as their field of definition or their kernel for example. The kernel of those isogenies are the one dimensional subspaces of the ℓ-torsion. Furthermore, their definition field is the definition field of their kernel. So, the existence of two rational proper values to the Frobenius implies the existence of two isogenies defined over the base field. Namely, the ℓ-torsion polynomial will have two (non necessarily irreducible) factors h_1 and h_2 of degree $(\ell - 1)/2$, each corresponding to a proper value. We have two isogeneous curves E_i, for $i = 1, 2$, given by some equations $\mathcal{E}_i$:

$$\mathcal{E}_i = Y^2 - X^3 - A_i X - B_i = 0$$

together with two isogenies $I_1 : E \to E_1$ and $I_2 : E \to E_2$, with kernel $T_1^E \cap E[\ell]$ and $T_2^E \cap E[\ell]$. And for $P = (X, Y)$ **mod** $\mathcal{E}$ a point on E, $I_i(P) = (\frac{g_i(X)}{h_i^2(X)}, \frac{k_i(X)}{y h_i^3(X)})$ **mod** $\mathcal{E}_i$, for $i = 1, 2$.

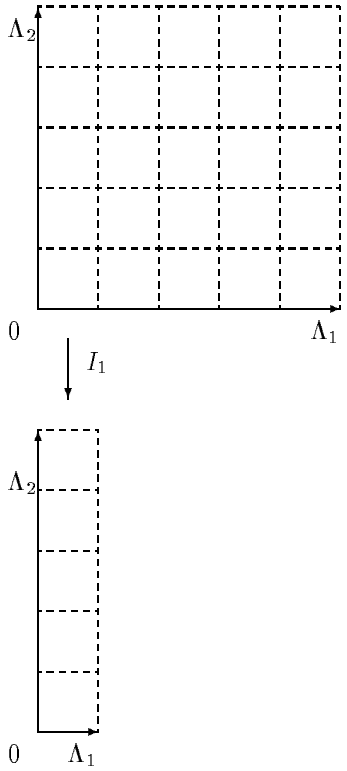
All along the chapter, we represent the ℓ-torsion on some elliptic curve as a parallelogram with sides the "rational directions". Here, for $\ell = 5$:



A non zero point in $T_1^E \cap E[\ell]$ is given by

$$(X, Y) \textbf{ mod } (\mathcal{E}, h_1(X)),$$

which is much nicer than the above, because of the degree of h_1. In view of those considerations, one would like to replace, in Schoof's algorithm, the torsion polynomial by some rational factor h_i when it exists. Or, more conceptually, the $[\ell]$-isogeny by some isogeny of degree ℓ.



We now need to compute the I_i, and firstly the h_i. Brute force factorization of f_ℓ^E would be even more difficult than the whole Schoff's method since we would need to compute $X^{q^{\frac{i-1}{2}}}$ **mod** f_ℓ^E in the worst cases. Nevertheless, the coefficients of h_1 and h_2 are modular functions over $\Gamma_0(\ell)$ and thus can be computed from analytic evaluation in $\mathbb{C}$. Indeed, one considers their Fourier expansion at infinity to find out some modular equation of degree $\ell+1$. The coefficients of those equations being integers can be reduced modulo p. The existence of some rational proper values to the Frobenius implies the existence of some roots in $\mathbb{F}_q$ to the modular equations. In fact, we have even better, since the decomposition type of such modular equations gives the permutation type of π seen as a permutation of $\mathbb{P}_1(\mathbb{F}_q)$ thus providing some knowledge about the (non necessarily rational) proper values: the multiplicative order of their quotient. This is the original remark of Atkin. One gets conditions over the residues modulo various primes ℓ_i of the cardinality and then tries to glue up all this knowledge thanks to a sieving process. Note that this is heavier but it works all the time, even if all the small primes we choose are bad.

Note that the whole method splits in two steps:

- Look for some rational root modulo q of the degree $\ell+1$ modular equations, and build h_1 from it if there is some. Otherwise factor the modular equation completely and deduce the (several) possible values of t **mod** ℓ (bad case).
- If you have found some h_1, compute (X^q, Y^q) **mod** $(\mathcal{E}, h_1)$ and then, look for some λ **mod** ℓ such that $(X^q, Y^q) = [\lambda](X, Y)$ **mod** $(\mathcal{E}, h_1(X))$ which gives the actual value of t **mod** ℓ (good case).

Note that in both steps we are dealing with polynomials of degree $\ell+1$ and $(\ell-1)/2$ which is much smaller than $(\ell^2-1)/2$.

Remark: We are not very explicit here about which equation to use. One may think about using the classical modular equation (or rather its quotient by Atkin-Lehner's involution). In this case, the solutions to those equations stand for the isogeneous curves and *not* for the isogenies themselves. It may be that there are two isogenies with distinct kernel and of the same degree, going to the same isogeneous curve. In this case, the endomorphism ring of the curve has a non rational element of norm ℓ^2. This indeed is a very strong condition that can be used to compute the cardinality of the curve.

Once we have computed the isogeneous curve thanks to some modular equation, there remains to compute an isogeny between the two curves. To achieve this goal, Elkies uses modular relations that happen to become trivial if the characteristic of the field is lower than ℓ. We show how to deal with that in section 4.3.

4.2 Walking along the rational cycles of isogeneous curves

We now suppose that $\pi \in GL(T_\ell)$ has two distinct rational proper values τ_1 and τ_2. We notice that, since the two isogenies I_1 and I_2 are rational, they commute with π. This implies that on the isogeneous curves, the proper values of the Frobenius are the same. Since the proper spaces T_1^E and T_2^E are independent, I_1 induces a bijection between T_2^E and the corresponding proper subspace on E_1 and reciprocally I_2 induces a bijection between T_1^E and the corresponding proper subspace on E_2.

The existence of two distinct rational proper values has another interesting consequence. It is that E_1 again has two rational isogenies of degree ℓ, one associated to each of the two proper values. We call I_{11} and I_{12} those isogenies and E_{11} and E_{12} the image curves. On the other hand, we know that, since I_1 is rational, the dual isogeny I_1^* must be rational as well (by uniqueness of it). Therefore I_1^* either equals I_{11} either equals I_{12}. By consideration of the restriction to T_1^E we see that

$$I_1^* = I_{12}.$$

We could express that by saying that the two rational directions are not only independent but dual.

We show all that on the picture 4.1.

Now, if E is a curve over $\mathbb{F}_q$ such that $t^2 - 4q$ is a non zero square mod ℓ we can build two infinite series of isogeneous curves over $\mathbb{F}_q$.

$$E \xrightarrow{I_1} E_1 \xrightarrow{I_{11}} E_{11} \xrightarrow{I_{111}} \cdots$$

$$E \xrightarrow{I_2} E_2 \xrightarrow{I_{22}} E_{22} \xrightarrow{I_{222}} \cdots$$

These series are computed in the following way. We use some modular equation, let's say the classical one, although it is far from being the most convenient from a practical point of view. We note this equation $\Phi_\ell(X, Y)$, a symmetric polynomial of degree $\ell + 1$ in both variables such that

$$\Phi_\ell(j(\tau), j(\ell\tau)) = 0.$$

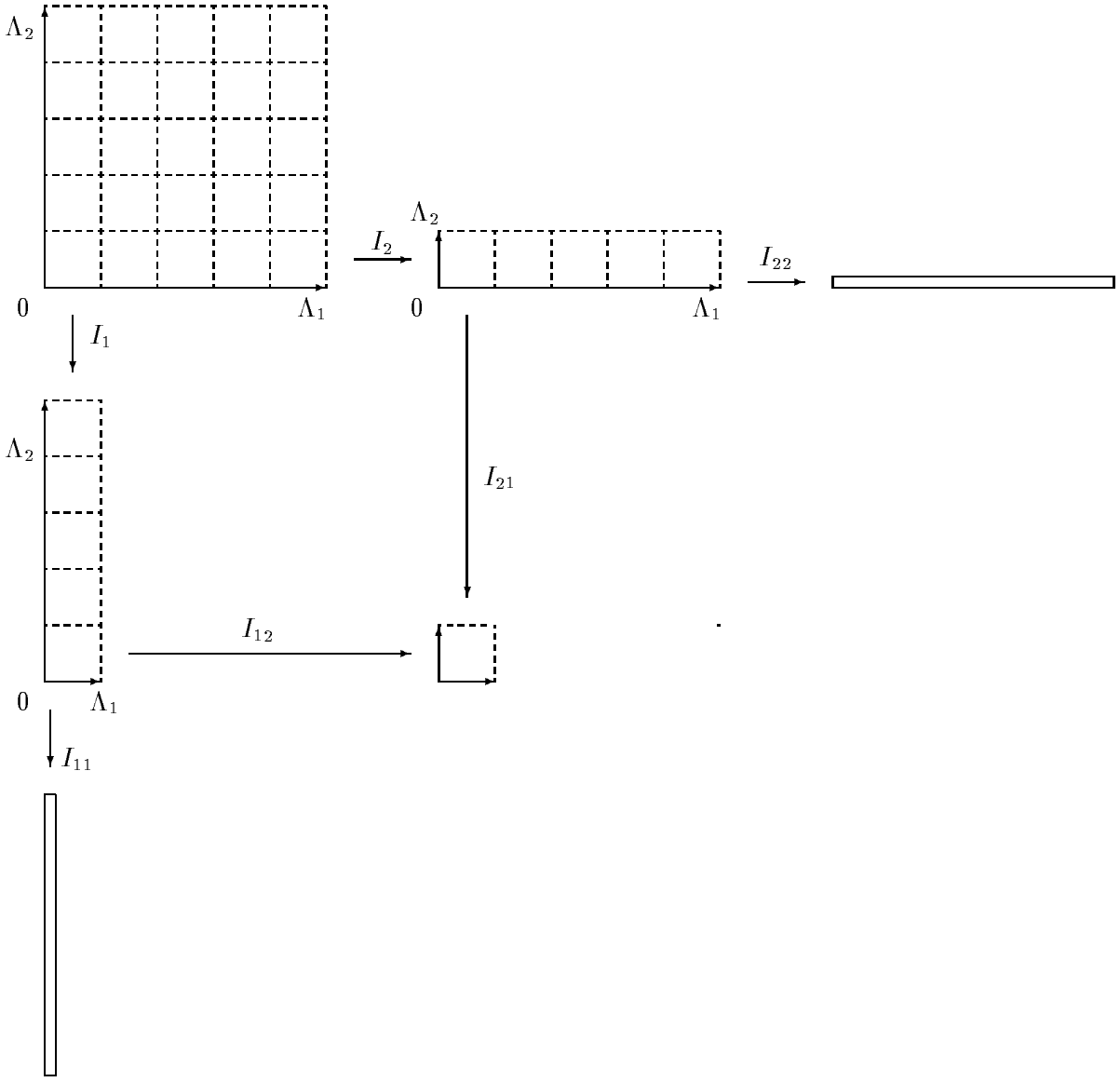


Figure 4.1: Action of the isogenies

Let's call j the invariant of E and let's solve $\Phi_\ell(X, j) = 0$ over $\mathbb{F}_p$. If we are in the "good case" we have two rational distinct simple roots j_1 and j_2 (we don't worry about the existence of non rational elements of norm ℓ^2 in the endomorphism ring). Let's now solve the equation $\Phi_\ell(X, j_1) = 0$ over $\mathbb{F}_p$. We find two rational distinct simple roots, one of them being j itself and corresponding to the dual isogeny I_1^*. We choose the other one and call it j_{11}. We go on, solving the equation $\Phi_\ell(X, j_{11}) = 0$....

Since the field is finite, the two series of curves are periodic and they provide an explicit description of the two rational subspaces of Tate's module. We ultimately get a cycle of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$, with the same cardinality as E. This cycle can be seen as one (oriented) connected component in the rational part of the lattice of all ℓ-isogenies.

For example, the factor of $f_\ell^E(X)$ corresponding to $T_1^E \cap E[\ell]$ is h_1, the denominator of I_1. Now, if we want the factor of $f_{\ell^2}^E$ corresponding to $T_1^E \cap E[\ell^2]$, we proceed in the following way. We first compute the polynomial h_{11} which is the denominator of I_{11}, in the same way we computed h_1 except that we replace E by E_1 and pay attention not to confuse I_{11} with $I_1^* = I_{12}$. Indeed we consider the isogeny from E_1 associated with τ_1. We then note that $T_1^E \cap E[\ell^2] = I_1^{-1}(T_1^{E_1} \cap E_1[\ell])$ so that the factor we are looking for is obtained by plugging I_1 into h_{11}. And so on ...

In this way one can compute factors of degree $\ell^{k-1}(\ell - 1)/2$ to the polynomial $f_{\ell^k}^E$ and then, using Schoof's idea compute the cardinality of E modulo ℓ^k rather than just ℓ. This allows us to take more advantage of the small good primes.

4.3 The case when the characteristic is small

The computation of the cardinality of elliptic curves over finite fields $\mathbb{F}_q$, following Schoof's ideas as in [39] plus the improvements by Atkin and Elkies, is a bit more difficult when the characteristic p of $\mathbb{F}_q$ is small. The main difficulty lies in the construction of isogenies defined over $\mathbb{F}_q$. The isogeneous curve itself can be found with a few modular equations. There remains to deduce the modular quantities arising in the full expression of the isogeny. We show how this problem can be solved in time similar to the one of Atkin-Elkies method, whatever the characteristic.

4.3.1 Principle of the method

We are interested in computing an isogeny of degree ℓ between two curves defined over a finite field $\mathbb{F}_q$ of characteristic p. We assume that ℓ is an odd prime different from p. We don't want to perform more than $O(\ell^{3+\epsilon})$ operations in the field $\mathbb{F}_q$. We will look for such an isogeny as a morphism of formal groups. More precisely, let $\mathcal{E}_a$ be an elliptic curve given by its equation $E_a(x, y)$ in normal form

$$E_a(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,$$

and similarly $\mathcal{E}_b$ an elliptic curve given by its equation $E_b(x, y)$

$$E_b(x, y) = y^2 + b_1xy + b_3y - x^3 - b_2x^2 - b_4x - b_6.$$

Then, an isogeny defined up to its sign, from $\mathcal{E}_a$ to $\mathcal{E}_b$, can be given as a rational function of x, of degree ℓ

$$x \mapsto \frac{g(x)}{h(x)^2},$$

where g is of degree ℓ and h is of degree $(\ell-1)/2$. If we set $z = 1/x$ on both sides we get

$$z \mapsto z\frac{\hat{h}(z)^2}{\hat{g}(z)},$$

where $\hat{h}(z) = z^{\frac{\ell-1}{2}}h(1/z)$ and $\hat{g}(z) = z^\ell g(1/z)$.

If we set $t = -x/y$ and $s = -1/y$, we can rewrite the equations in the plane of (t,s) coordinates as

$$E_a(t,s) = t^3 + a_1ts + a_2t^2s + a_3s^2 + a_4ts^2 + a_6s^3 - s.$$

Both s and $z = 1/x$ are power series in t,

$$s = t^3 + a_1t^4 + (a_1^2 + a_2)t^5 + ... \quad (4.1)$$
$$z = s/t = t^2 + a_1t^3 + ... \quad (4.2)$$

For this reason, given an isogeny from $\mathcal{E}_a$ to $\mathcal{E}_b$, we can associate to it a series in t,

$$t \mapsto \sum_{k\geq 1} u_k t^k.$$

Reciprocally, given such a series, we can recover the rational fraction. For we know that on $\mathcal{E}_b$, z is given as

$$z = t^2 + b_1t^3 + (b_1^2 + b_2)t^4 + ...,$$

so we substitute t by $\sum_k u_k t^k$ in the above series. The series we obtain must be a function of $z = t^2 + a_1t^3 + (a_1^2 + a_2)t^4 + ...$ on $\mathcal{E}_a$, so, by gradual elimination, we finally get a series

$$z \mapsto \sum_{k\geq 1} v_k z^k,$$

which is the series expansion of the isogeny at $z = 0$. Since this is a rational fraction of degree ℓ, the above series must satisfy a recurrence relation of depth ℓ for indices greater than ℓ. Such a relation can be detected by the Massey-Berlekamp algorithm in time linear in ℓ, see [7] chapter 7.

We recall that, associated to the curve $\mathcal{E}_a$, there is a formal group $F_a(t_1,t_2)$ given as a series in t_1 and t_2,

$$F_a(t_1,t_2) = t_1 + t_2 - a_1t_1t_2 + ...$$

The multiplication by an integer n on $\mathcal{E}_a$ is given by the series

$$[n]_a t = nt - \frac{n(n-1)}{2}a_1t^2 + O(t^3).$$

In particular we have

$$[p]_a t = c_a t^{p^h} + O(t^{2p^h})$$

where h is an integer called the height of the formal group and cannot be greater than 2 in the case of an elliptic curve. It is one if and only if the curve is non supersingular, which will always be the case for us. See [43] chapter IV paragraph 7 for all that.

Now the point is that the series $U(t) = \sum_k u_k t^k$ given by some isogeny must be a morphism of formal groups, i.e. it must satisfy the following identity

$$U(F_a(t_1, t_2)) = F_b(U(t_1), U(t_2)) \tag{4.3}$$

As a consequence we have for any integer n

$$U \circ [n]_a = [n]_b \circ U,$$

and specially

$$U \circ [p]_a = [p]_b \circ U \tag{4.4}$$

As we will see, there are more such morphisms than isogenies. In fact, the ring of endomorphisms of a formal group of height 1 is canonically isomorphic to $\mathbb{Z}_p$, and the set of homomorphisms between two formal groups with height 1 is a $\mathbb{Z}_p$-module of dimension 1. The proof of all that lies in the algorithm below.

For us, we will compute any generator S_0 of this module and then try to find out some scalar N in $\mathbb{Z}_p$ such that $[N]S_0 = S$ is the true development at 0 of the isogeny we are looking for.

So, in a first step we compute a power series S_0 with L terms of precision. The number of terms L is bounded by a small multiple of ℓ. It can be chosen to be 4ℓ or so.

$$L = 4\ell.$$

Then, we have to deal with the unknown integer N. But this does not make much indetermination. In fact, up to precision L, only the s first terms of N matter where s is the smalest integer such that $p^s > L$.

$$N = n_0 + n_1 p + ... + n_{s-1} p^{s-1} + O(p^s)$$

We see that there are no more than $p^s \leq pL$ such p-adic expressions. So we try all of them. For each $1 \leq N < p^s$ we compute $[N]S_0$ and thanks to Massey-Berlekamp algorithm we can test in $O(\ell)$ operations whether it satisfies a linear recurrence of depth ℓ. If this is the case (as it must be for at least one among them), we deduce a rational function that corresponds to an isogeny.

4.3.2 More details

In this section, we accumulate technical and theoretical data.

Composite series

Let U and V be two formal series

$$U = \sum_{k \geq 1} u_k t^k, \; V = \sum_{k \geq 1} v_k t^k.$$

Let's call $W = U \circ V$ and write it as

$$W = \sum_{k \geq 1} w_k t^k.$$

If $m \geq 3$ then w_{m+1} is a linear function of v_{m+1}, v_m. It is also linear in any u_k. Namely, there exists a polynomial f, in the u_k and v_k for $k \leq m-1$ such that

$$w_{m+1} = v_1^{m+1} u_{m+1} + u_1 v_{m+1} + m u_m v_1^{m-1} v_2 + 2 v_1 u_2 v_m + f(u_1, ..., u_{m-1}, v_1, ..., v_{m-1}).$$

Note that f is linear in the u_k. On the other hand the first terms of W are

$$\begin{aligned} w_1 &= u_1 v_1, \\ w_2 &= u_2 v_1^2 + v_2 u_1 \\ w_3 &= u_3 v_1^3 + 2 u_2 v_1 v_2 + v_3 u_1 \\ w_4 &= u_4 v_1^4 + 3 v_1^2 v_2 u_3 + 2 u_2 v_1 v_3 + u_2 v_2^2 + v_4 u_1. \end{aligned}$$

Hasse invariant and normalization

We recall that the multiplication by p on $\mathcal{E}_a$ is given by

$$[p]_a t = c_a t^p + O(t^{2p})$$

where c_a is a modular form of height $p-1$ and such that the absolute norm of c_a is related to the cardinality of the curve modulo p by

$$\sharp \mathcal{E}_a = \mathcal{N}(c_a) \pmod{p}.$$

For this reason, we can suppose that this invariant is the *same* for the two isogeneous curves. For example, if $p = 2$ we thus have

$$a_1 = b_1 = c_a = c_b = 1,$$

since the curve is not supersingular.

Computations

This computation is just based on a careful use of (4.3) and (4.4). We compute the u_m gradually for increasing m.

— If $m = 1$, we write the coefficient of t^p in equation (4.4) and get

$$u_1 c_a = c_b u_1^p,$$

and since $c_a = c_b$ we deduce that u_1 is in the prime field $\mathbb{F}_p$. This indetermination on u_1 corresponds to the first term of the p-adic N. We go from some u_1 to any other one u_1' by multiplying by the p-adic $N = u_1'/u_1 + O(p)$. So we choose u_1 to be 1 and go on.

— If m is not a power of p, then we can express u_m as a linear function of the u_k for $k < m$ thanks to (4.3). Indeed, u_m appears first in the term of degree m of the equation. We write this term as

$$u_m(t_1 + t_2)^m - u_m(t_1^m + t_2^m) + f(u_{m-1}, ..., u_1, t_1, t_2) = 0,$$

where f is a polynomial. This gives at least one non trivial linear equation in u_m in this case. Evidently, we don't work out the whole series with two variables. We put $t_2 = At_1$ where A is chosen so that the above equation remains non trivial i.e. $(1 + A)^m - 1 - A^m \neq 0$.

— If $m = p^k$ is a power of p we use (4.4) again where the first coefficient with u_m is the one of t^{mp} which gives

$$c_b u_m^p - c_a^m u_m + f(u_{m-1}, ..., u_1) = 0.$$

We suppose that the two curves have non zero invariant c_a and c_b and that these invariants are equal (we can always insure that because of the existence of some isogeny). It is clear from this equation that u_m is defined up to an additive constant in the prime field and that this indetermination corresponds to multiplying by $1 + p^k\lambda$ where $\lambda \in \mathbb{F}_p$. Indeed,

$$[p^k]_b t = c_b^{1+p+...+p^{k-1}} t^{p^k},$$

and if $\lambda \in \mathbb{F}_p$ then $\lambda c_b^{1+p+...+p^{k-1}}$ satisfies the equation

$$c_b X^p - c_a^m X = 0,$$

since $c_a = c_b$. We choose any solution and go on.

This way, we compute S_0 with L terms, a generator of the module of homomorphisms. It is defined up to a multiplicative p-adic

$$N = n_0 + n_1 p + ... + n_{s-1} p^{s-1} + O(p^s)$$

where s is the number of significant terms.

Complexity considerations

The complexity of multiplying two series of length L is $O(L^2)$ operations in the field. For the composition, the complexity is $O(L^3)$. The complexity of the addition formal law with precision $O(L)$ is $O(L^3)$ provide we have precomputed a few series attached to the formal group, see [24] on pages 238 and 239. We use the following tricks :

— If we already have computed the product $S_1 S_2$ with precision L, then getting the result with precision $L + 1$ just requires $O(L)$ operations. Similarly the cost of refining a composition or a formal addition is no more than $O(L^2)$.

— If we have to compute the composition $S_k \circ S_0$ for $O(L)$ different k and with precision $O(L)$, we can keep in memory the powers of S_0. This way the $O(L)$ compositions are done in $O(L^3)$ operations.

— The series $[p]t$ can be written $P(t^p)$ where P is of height 0. Then we get $[p^2]t$ as $P \circ {}^{\pi}P(t^{p^2})$ where π denotes the generator of the Galois group, that is to say p-exponentiation of the scalars. We go on like that.

Bibliographie

[1] L.M. Adleman. Factoring numbers using singular integers. *STOC*, pages 64–71, 1991.

[2] M.A. Armstrong. *Groups and Symmetry.* Springer, 1988.

[3] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime. Preprint, 1988.

[4] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime (ii). Preprint, 1992.

[5] A. O. L. Atkin and H.P.F. Swinnerton-Dyer. Modular forms over non-congruence subgroups. In *Proceedings of symposia in pure mathematics*, number 19. AMS, 1971.

[6] G.V. Belyi. On galois extensions of the maximal cyclotomic field. *Izvestiya Ak. Nauk. SSSR, ser. mat.*, 43:2:269–276, 1979.

[7] E. R. Berlekamp. *Algebraic coding theory.* McGraw-Hill, 1968.

[8] D.J. Bernstein and A.K. Lenstra. *A general number field sieve implementation*, volume 1554 of *Lect. Notes in Math.*, pages 98–119. Springer Verlag, 1993.

[9] Bryan Birch. Arithmetic of noncongruence subgroups. In *The theory of Grothendieck dessins d'enfants.* Cambridge University Press, 1994.

[10] J.P. Buhler, H.W. Lenstra, and C. Pomerance. *Factoring integers with the number field sieve*, volume 1554 of *Lect. Notes in Math.*, pages 48–89. Springer Verlag, 1993.

[11] H. Cohen. *A course in computational number theory.* Springer, 1993.

[12] Kevin Coombes and David Harbater. Hurwitz families and arithmetic galois groups. *Duke mathematical journal*, 52:821–839, 1985.

[13] J.-M. Couveignes and L. Granboulan. Dessins from a geometric point of view. In *The theory of Grothendieck dessins d'enfants.* Cambridge University Press, 1994.

[14] J.-M. Couveignes and F. Morain. Schoof's algorithm and isogeny cycles. In *Proceedings of the first ANTS conference.* Springer Verlag, 1994.

[15] Jean-Marc Couveignes. *Computing a square root for the number field sieve*, volume 1554 of *Lect. Notes in Math.*, pages 95–102. Springer Verlag, 1993.

[16] Jean-Marc Couveignes. Calcul et rationalité de fonctions de belyi en genre 0. *Annales de l'Institut Fourier*, 44(1):1–38, 1994.

[17] Pierre Deligne. Le groupe fondamental de la droite projective moins trois points. In Y. Ihara, K. Ribet, and J.-P. Serre, editors, *Galois groups over Q*, Mathematical Sciences Research Institute Publications. Springer Verlag, New York, 1989.

[18] Leila Schneps edt. *The theory of Grothendieck's dessins d'enfant.* Cambridge University Press, 1994.

[19] N.D. Elkies. Explicit isogenies. 1991.

[20] Michael D. Fried and Pierre Debes. Rigidity and real residue class fields. *Acta arithmetica*, LVI:291–322, 1990.

[21] Shabat G.B. and Voevodsky V.A. Drawing curves over number fields. *The Grothendieck Festschrift, Birkhauser*, pages 199–229, 1990.

[22] Alexandre Grothendieck. Esquisse d'un programme. *Non publié.*

[23] David Harbater. *Galois coverings of the arithmetic line*, volume 1240 of *Lect. Notes in Math.*, pages 165–195. Springer Verlag, 1987.

[24] D. Husemöller. *Elliptic curves.* Springer, 1987.

[25] Antoine Joux. *La réduction des réseaux en cryptographie.* École Polytechnique, 1993.

[26] Felix Klein. *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree.* London, 1913.

[27] D. E. Knuth. *The art of computer programming, second edition*, volume 2. Addison-Wesley, 1981.

[28] D.E. Knuth. *The art of computer programming.* Addison-Wesley, 1981.

[29] E. Landau. Sur quelques théorèmes de petrovič relatifs aux zéros des fonctions analytiques. *Bull. Soc. Math. France*, 33:251–261, 1905.

[30] S. Lang. *Algebraic number theory.* Addison-Wesley, 1970.

[31] Henri Lebesgue. *Leçons sur les constructions géométriques.* Gauthier-Villars, 1950.

[32] A.K. Lenstra, H.W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[33] A.K. Lenstra, H.W. Lenstra, M.S. Manasse, and J.M. Pollard. *The number field sieve*, volume 1554 of *Lect. Notes in Math.*, pages 11–40. Springer Verlag, 1993.

[34] M. Mignotte. *Mathématiques pour le calcul formel.* Presses Universitaires de France, 1989.

[35] P.L. Montgomery and R.D. Silverman. An fft extension to the $p-1$ factoring algorithm. *Math. Comp.*, 54:839–854, 1990.

[36] François Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. Submitted for publication of the Actes des Journées Arithmétiques 1993, March 1994.

[37] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.

[38] C.-P. Schnorr. A more efficient algorithm for lattice basis reduction. *J. Algorithms*, 9:47–62, 1988.

[39] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. of Comp.*, 44:483–494, 1985.

[40] René Schoof. Counting points on elliptic curves over finite fields. Preprint, February 1994.

[41] Jean-Pierre Serre. *Corps Locaux*. Hermann, 1968.

[42] Jean-Pierre Serre. *Topics in Galois theory*. Jones and Bartlett, 1992.

[43] J. H. Silverman. *The arithmetic of elliptic curves*. Springer, 1985.

[44] B.L. van der Waerden. *Algebra*. Springer-Verlag, 1966.

[45] André Weil. The field of definition of a variety. *Amer. J. Math.*, 78:509–524, 1956.

Table des matières