UNIVERSITÉ PARIS 7 — DENIS DIDEROT
UFR D'INFORMATIQUE

THÈSE DE DOCTORAT

présentée pour l'obtention du Diplôme de

Docteur de l'Université Paris 7

Spécialité : Informatique

par

Louis GRANBOULAN

Calcul d'objets géométriques à l'aide de méthodes algébriques et numériques

Dessins d'Enfants

Soutenue le 8 décembre 1997.
Composition du jury :

Henri COHEN
Jean-Marc COUVEIGNES
Philippe FLAJOLET
Daniel KROB
Daniel LAZARD
Andrew ODLYZKO *(Rapporteur)*
Jacques STERN *(Directeur)*
Alexandre ZVONKINE *(Rapporteur)*

Recherches effectuées au
Laboratoire d'Informatique
de l'École Normale Supérieure

ECOLE NORMALE SUPERIEURE

URA 1327 du CNRS
45, rue d'Ulm, 75230 Paris Cedex 05

Remerciements

Je remercie Jacques Stern pour avoir encadré mon travail depuis le D.E.A et pendant ces années de thèse. Il m'a permis de naviguer de la cryptographie à la théorie des nombres. Je lui dois de m'avoir accueilli dans son équipe où j'ai pu travailler sur cette thèse et sur bien d'autres sujets passionnants. L'ambiance du GRECC est une agréable incitation à s'intéresser à tous les aspects algorithmiques ou mathématiques ayant un lien avec la cryptographie.

Je tiens à remercier tout particulièrement Jean-Marc Couveignes pour son intuition et ses nombreux conseils. C'est grâce à lui que je me suis lancé dans le calcul des dessins d'enfants et je suis heureux qu'il ait accepté de faire partie de mon jury de thèse.

Je remercie Antoine Joux de m'avoir initié à l'utilisation de l'algorithme LLL en théorie des nombres. Merci aussi à mes autres amis du GRECC, qui ont tous été de sympathiques compagnons de travail.

De nombreuses discussions avec des mathématiciens du DMI, en particulier Leila Schneps, Pierre Lochak et Leonardo Zapponi, m'ont permis de mieux comprendre les mystères de la théorie des dessins d'enfants. Je leur suis reconnaissant d'avoir adapté leur langage à un interlocuteur informaticien.

Je remercie bien sûr Stéphane Aicardi, Farouk Boucekkine, Phong Nguyen et Benoît Semelin pour leur travail de relecture.

Je suis reconnaissant à Andrew Odlyzko et Alexandre Zvonkine d'avoir acceptés d'être rapporteurs de ma thèse. Leurs commentaires et leurs questions m'ont permis de clarifier ma rédaction et m'ont donné de nouvelles pistes de réflexion.

Je remercie tous les membres de mon jury de thèse, Henri Cohen, J.-M. Couveignes, Philippe Flajolet, Daniel Krob, Daniel Lazard et Alexandre Zvonkine, de me faire l'honneur d'assister à ma soutenance.

Merci enfin à toute ma famille, en particulier Marie, de m'avoir supporté et aidé.

Table des matières

Table des figures

Résumé

Cette thèse est découpée en quatre chapitres. Le premier chapitre est consacré aux méthodes de résolution de systèmes d'équations algébriques, dans un contexte général de calcul formel. Le second définit les dessins d'enfants et le principe de la correspondance de Grothendieck. Le troisième chapitre explique les techniques de calcul de cette correspondance et le quatrième donne des résultats de calcul.

Deux méthodes sont décrites dans le premier chapitre. Elles reposent sur des notions d'algèbre élémentaire, dont nous commençons par rappeler les définitions et les principales propriétés. Nous insistons sur l'approximation des nombres algébriques, qui est le cœur de la seconde méthode. La première méthode de résolution repose sur le calcul de base de Gröbner. Nous donnons le schéma de cette technique, à base de calculs exacts sur les polynômes. La seconde méthode commence par approcher numériquement la solution, puis reconstitue sa définition algébrique. On utilise en particulier l'algorithme LLL de réduction de réseaux.

Le second chapitre est plus théorique. Après une brève présentation informelle, nous commençons par une longue série de définitions mathématiques, issues des théories avec lesquelles interagissent les dessins. Ensuite, nous définissons formellement les dessins en insistant sur leurs deux visages, et la correspondance (de Grothendieck) entre les deux : nous regroupons d'une part les définitions liées à leur aspect combinatoire et d'autre part celles concernant leur aspect algébrique. Nous insistons sur les nombreuses variantes et généralisations des dessins d'enfants. Nous continuons avec l'action de Galois sur les dessins, en particulier la notion de corps des modules, dont les propriétés sont un élément fondamental du calcul explicite de l'aspect algébrique d'un dessin. Nous en profitons pour évoquer l'application de ces calculs explicites au problème de Galois inverse.

Le troisième chapitre expose la principale méthode pour le calcul explicite de la correspondance de Grothendieck. Nous partons de la description combinatoire du dessin, nous définissons un système algébrique dont les solutions décrivent les propriétés algébriques et arithmétiques du dessin. Nous exposons quelques autres méthodes, appliquées dans certains cas particuliers, puis nous détaillons les avantages de la résolution numérique du système par rapport à des techniques plus algébriques.

Le quatrième chapitre donne des exemples de calculs explicites de dessins. Il commence avec les dessins les plus élémentaires, qui servent à visualiser les plus simples de ces objets, puis il continue en décrivant une série de calculs d'"arbres en Y", qui servent de prétexte à une comparaison des techniques de calcul. Nous montrons ensuite quelques dessins ayant un intérêt particulier, et nous concluons avec des calculs servant à la résolution d'instances du problème de Galois inverse.

Introduction

ALEXANDER GROTHENDIECK a inauguré l'étude des *dessins d'enfants*, une famille d'objets mathématiques qu'il voulait considérer comme les éléments de base d'une approche intuitive de la géométrie algébrique et de l'action du groupe de Galois absolu. Le lien entre les propriétés topologiques (visuelles) et algébriques d'un dessin est appelé *correspondance de Grothendieck*. [24, 38]

Comme souvent, la compréhension en profondeur de la structure d'objets abstraits demande qu'on en connaisse suffisamment d'exemples pratiques pour asseoir son intuition. L'un des problèmes qui se posent est donc le calcul des propriétés algébriques d'un dessin, à partir de ses données topologiques, c'est-à-dire le calcul de la correspondance de Grothendieck.

De tels calculs ont déjà été réalisés par de nombreux auteurs, dans divers contextes et selon plusieurs méthodes [2, 7, 8, 16, 23, 29, 30, 31, 42, 43, ...]. Pour réussir à calculer des exemples résistant aux approches classiques, nous avons dû développer des techniques originales, qui ont pu prouver leur efficacité.

LES DESSINS D'ENFANTS présentent deux visages, ce qui donne naissance à une interaction qui fait leur richesse. D'un point de vue géométrique, nous définissons un dessin comme un élément du corps des fonctions d'une courbe algébrique, ayant au plus trois valeurs critiques. On en déduit de façon très naturelle une description combinatoire, sous la forme d'un graphe plongé dans une surface. Ce qui est plus surprenant est que cette correspondance peut être rendue bijective. Mais le calcul explicite des propriétés algébriques à partir de la description combinatoire d'un dessin pose de nombreux problèmes algorithmiques.

À part pour les dessins de genre 0, ce calcul est toujours fait au cas par cas, pour des exemples simples. En genre 0, il existe une approche systématique, qui passe par la résolution d'un système d'équations algébriques.

LES SYSTÈMES D'ÉQUATIONS ALGÉBRIQUES servent à la résolution de beaucoup de constructions géométriques et en particulier au calcul de la correspondance de Grothendieck. Le premier chapitre de cette thèse est consacré aux méthodes de résolution de systèmes algébriques, dans le contexte général du calcul formel. Nous décrivons les deux techniques généralement employées, et qui sont les plus efficaces : le calcul de bases de Gröbner d'un idéal, pour en déduire un système triangulaire, et le calcul d'approximations numériques d'une solution, qui permet de reconstruire un point de la variété solution.

Historiquement, le calcul numérique a été remplacé par les bases de Gröbner, parce qu'elles permettent la résolution systématique, automatique et exacte de nombreux problèmes algébriques. Pour les dessins d'enfants, c'est ainsi que Malle a réalisé le catalogue actuellement le plus exhaustif de dessins de genre zéro [30]. Le principal avantage de cette technique est qu'à l'aide d'opérations exactes sur les polynômes, un résultat est obtenu dont on a prouvé la validité. Malheureusement, la manipulation de polynômes à coefficients entiers est très gourmande en mémoire et en puissance de calcul et Malle a dû intervenir "manuellement" pour son calcul d'un polynôme de groupe de Galois $Aut(M_{22})$ [29].

Nous voulons montrer qu'une approche numérique, faisant appel à l'intuition géométrique, est au moins aussi efficace pour résoudre les cas les plus difficiles du calcul de la correspondance de Grothendieck.

La comparaison entre ces deux techniques est faite à la fois sur le plan théorique et à l'aide d'exemples. La nature des résultats obtenus est assez différente : la résolution par bases de Gröbner donne toutes les solutions du système, tandis qu'une résolution numérique ne donne que l'orbite galoisienne d'une solution, celle qui est proche d'une approximation initiale. L'inconvénient de ne pas être exhaustif se révèle un avantage lorsque le système d'équations est mal défini (cf. IV.4.3).

La complexité, dans le cas le pire, du calcul de bases de Gröbner est une exponentielle du nombre de variables du système. En pratique, le nombre de solutions est plus représentatif du temps de calcul d'un système triangulaire au moyen de bases de Gröbner. De même, la dernière étape du calcul numérique (récupération d'une description algébrique de la solution) est principalement limitée par le nombre de solutions conjuguées. Lorsqu'on effectue une batterie de tests comme au paragraphe IV.3 de cette thèse, il apparaît qu'en pratique les temps de calcul des deux méthodes sont très comparables.

Le principal inconvénient de la résolution par approximations numériques est qu'elle nécessite une surveillance humaine. Des trois étapes du calcul numérique (choix d'une approximation, convergence vers une solution suffisamment précise, puis récupération d'une description algébrique de la solution), les deux dernières étapes se font automatiquement, mais la première étape demande un peu de doigté et n'a été automatisée que pour les arbres [31].

Nous utilisons une intuition géométrique de ce que sera la "vraie" forme du dessin, et il n'existe malheureusement aucun théorème qui permette d'automatiser cette intuition. Ce trou dans la théorie est même assez frappant, et certains calculs comme celui illustré par la figure IV.3 montrent qu'il y a une notion de "masse" d'un morceau de dessin qui apparaît. Par exemple, les sommets ayant beaucoup de voisins ayant tendance à être plus éloignés de ces voisins que des sommets de valence plus petite. Ce genre de considérations m'a permis de réaliser par approximations successives presque n'importe quel exemple de dessin déjà calculé, et quelques calculs originaux. Les dessins qui résistent sont ceux dont la régularité algébrique est telle qu'une résolution spécifique donne de meilleurs résultats qu'une résolution générique.

Le cas des revêtements ramifiés au dessus de quatre points généralise les dessins d'enfants. Le calcul de ces revêtements à partir de leur description combinatoire est bien plus accessible à la résolution numérique qu'à la résolution algébrique. En effet, comme la variété solution du système correspondant est de dimension 1, les méthodes efficaces pour le calcul de bases de Gröbner sont affaiblies. En revanche, la méthode numérique peut exploiter des propriétés géométriques : le déplacement relatif des quatre valeurs de ramification donne une famille continue de revêtements, chacun étant une "bonne" approximation de ceux qui en sont proches. Lorsque nous confondons deux ramifications, l'élément dégénéré de cette famille, ramifié au dessus de trois points, est un dessin bien plus simple dont on calcule plus facilement la description algébrique. On peut ensuite, de proche en proche, calculer les propriétés de l'ensemble de la famille.

Cette approche a permis le calcul effectif du premier polynôme dont on sache que le groupe de Galois est le groupe de Mathieu M_{24}. Une application de nos techniques d'approximation est donc le calcul de revêtements de degré assez élevé, en particulier ceux que détecte l'utilisation de méthodes de rigidité pour le problème de Galois inverse. Le calcul massif de dessins doit être mis en œuvre avec des techniques de bases de Gröbner, et l'utilisation conjointe des deux approches peut se révéler fructueuse.

En conclusion , nous exploitons une approche résolument expérimentale du calcul mathématique. En l'absence d'une compréhension en profondeur des dessins d'enfants, nous calculons des exemples sur lesquels pourrront se baser des conjectures. Pour mener ces calculs à bien, nous utilisons une intuition géométrique (au sens classique du terme) qui nous mène donc à une description géométrique. Nous profitons de la puissance de l'algorithme LLL pour vérifier la pertinence de notre intuition en retrouvant la valeur algébrique exacte.

Chapitre I

Résolution d'un système algébrique

Nous commençons par énumérer les concepts mathématiques dont nous aurons besoin, en fixant les conventions de notation et en rappelant les propriétés dont nous nous servons. Nous définirons ainsi le problème de la résolution d'un système algébrique, que nous attaquerons de deux façons.

La recherche de bases de Gröbner est l'une de ces approches, c'est l'objet de la seconde section. Nous ne prétendons pas exposer l'intégralité des travaux dans le domaine, ni même une synthèse de ceux-ci, mais nous voulons plutôt donner un aperçu des principes de cette méthode. Nous regarderons en particulier le cas des systèmes de dimension 0. Il s'agit de pouvoir comparer cette méthode algébrique avec notre approche numérique.

La troisième section décrit donc la méthode de résolution numérique, que nous avons utilisée pour les dessins d'enfants. Nous verrons que son inconvénient est qu'elle ne peut prétendre fournir l'ensemble de la solution, ce qui peut devenir un avantage lorsque le système est mal défini. De plus cette approche numérique utilise plus facilement la description géométrique de la solution.

I.1 Notions d'algèbre

Les fondements du calcul **algébrique** sont les polynômes sur un anneau ou un corps. On parle de **géométrie** lorsqu'on considère les corps des réels $\mathbb{R}$ ou des complexes $\mathbb{C}$. On parle d'**arithmétique** à propos des rationnels $\mathbb{Q}$ et des corps de nombres.

Dans cette section nous rappelons quelques définitions élémentaires d'algèbre principalement. Ensuite, nous présenterons les corps de nombres, en faisant allusion à leur interaction avec la géométrie, par leurs plongements dans $\mathbb{C}$ et les métriques sous-jacentes. Nous esquisserons enfin le lien entre géométrie et algèbre qui se présente sous la forme de variétés algébriques solutions de systèmes polynomiaux, et qui peut mener à la géométrie algébrique.

Nous profitons de cette présentation pour définir le groupe de Galois abolu $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, mais cette notion ne sera utilisée que dans le second chapitre, sur les *dessins d'enfants*. Son étude est l'une des motivations du calcul explicite des dessins.

I.1.1 Définitions

a. Anneau

On ne s'intéressera qu'aux anneaux unitaires intègres commutatifs. On note $\mathbb{A}^\times$ le groupe multiplicatif des éléments inversibles.

b. Idéal

Nous rappelons qu'un idéal $I \subset \mathbb{A}$ est un sous-groupe de $\mathbb{A}$ stable par multiplication par tout élément de $\mathbb{A}$. On note (F) l'idéal engendré par une partie $F \subset \mathbb{A}$, c'est-à-dire le plus petit idéal contenant F. C'est la somme des idéaux principaux $x\mathbb{A}$ pour $x \in F$. Un idéal propre est un idéal différent de $\mathbb{A}$.

Un idéal propre est **maximal** s'il n'est contenu dans aucun autre idéal propre. Un idéal **premier** est tel que $ab \in I \Rightarrow a \in I$ ou $b \in I$. Le **radical** d'un idéal est $\sqrt{I} = \{x \mid \exists n : x^n \in I\}$.

La relation $x\mathcal{R}y \Leftrightarrow x - y \in I$ définit le quotient $\mathbb{A}/I$, qui est un anneau. Cet anneau est intègre si I est premier, c'est un corps si I est maximal.

c. Polynôme à une indéterminée

Un **polynôme** à coefficients dans un anneau $\mathbb{A}$ est une application à support fini $P : \mathbb{N} \to \mathbb{A}, \quad n \mapsto P_n$. On note $P(X) = \sum P_n X^n$, on dit que P_n est le coefficient de X^n. On note $\mathbb{A}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{A}$. C'est un anneau, commutatif si $\mathbb{A}$ l'est.

Le **degré** du polynôme est le plus petit $d \in \mathbb{N} \cup \{-\infty\}$ tel que $\forall n > d, P_n = 0$. Par convention, le degré du polynôme nul est donc $-\infty$. Le coefficient dominant d'un polynôme non nul est P_d. S'il vaut 1, on dit que le polynôme est **unitaire**.

d. Polynôme à plusieurs indéterminées

Un **polynôme à m indéterminées** est une application à support fini $P : \mathbb{N}^m \to \mathbb{A}, \quad \alpha = (\alpha_1, ..., \alpha_m) \mapsto P_\alpha$. On note $P(\mathbf{X}) = \sum P_\alpha \mathbf{X}^\alpha$ ou bien $P(X_1, ..., X_m) = \sum P_{\alpha_1,...,\alpha_m} X_1^{\alpha_1} ... X_m^{\alpha_m}$. Les polynômes à m indéterminées à coefficients dans $\mathbb{A}$ forment un ensemble noté $\mathbb{A}[\mathbf{X}]$ ou $\mathbb{A}[X_1, ..., X_m]$. C'est un anneau isomorphe à $\mathbb{A}[X_1, ..., X_{m-1}][X_m]$.

Le **degré total** du monôme $\mathbf{X}^\alpha$ est égal à $\alpha_1 + ... + \alpha_m$. Son degré en X_m est α_m. On appellera **support** du polynôme l'ensemble des $\mathbf{X}^\alpha$ tels que $P_\alpha \neq 0$ (et non l'ensemble des α comme on le fait parfois). Le degré total d'un polynôme non nul est le plus grand degré total des monômes de son support. On dit qu'un polynôme est **homogène** si tous les monômes de son support ont même degré total.

e. Fonction polynomiale

Si $\mathbb{A}$ est commutatif, on notera aussi $P(x_1, ..., x_m)$ l'image par la fonction polynomiale associée à P du m-uplet $(x_1, ..., x_m) \in \mathbb{A}^m$. C'est l'élément $\sum P_{\alpha_1,...,\alpha_m} x_1^{\alpha_1} ... x_m^{\alpha_m} \in \mathbb{A}$.

On peut remarquer que si $\mathbb{E}$ est une algèbre (commutative) sur $\mathbb{A}$, l'anneau $\mathbb{A}[\mathbf{X}]$ s'injecte dans $\mathbb{E}[\mathbf{X}]$. Le sous-ensemble de $\mathbb{E}^m$ tel que $P(x_1, ..., x_m) = 0$ est noté $V_{\mathbb{E}}(P)$. Cette notation sera utilisée lorsque nous chercherons à résoudre des systèmes d'équations polynomiales.

Les éléments de $V_{\mathbb{E}}(P)$ sont appelés **zéros** de P (dans $\mathbb{E}^m$). Si $m = 1$, on parle alors de **racines**.

f. Irréducibilité

L'anneau $\mathbb{A}[\mathbf{X}]$ est factoriel si $\mathbb{A}$ l'est. Si P peut se factoriser en polynômes de degré au plus 1, on dit qu'il est **scindé**. S'il n'admet pas de facteurs non triviaux, on dit qu'il est **irréductible**.

Si $x \in \mathbb{A}$ est une racine de P, alors $X - x$ divise P. Si $(X - x)^n$ est la plus grande puissance divisant P, on dit que x est racine de P avec **multiplicité** n.

g. Corps

On ne s'intéressera qu'aux corps commutatifs.

h. Extension algébrique

Un corps $\mathbb{L}$ est une **extension** du corps $\mathbb{K}$ si $\mathbb{L}$ contient $\mathbb{K}$. C'est alors un espace vectoriel sur $\mathbb{K}$, de dimension notée $[\mathbb{L} : \mathbb{K}]$ et appelée degré de l'extension. Si $\mathbb{L} \neq \mathbb{K}$, c'est une extension propre.

Un élément $x \in \mathbb{L}$ est **algébrique** sur $\mathbb{K}$ s'il existe un polynôme non nul $P \in \mathbb{K}[X]$ tel que $P(x) = 0$. Une extension est algébrique si elle ne contient que des éléments algébriques. Toute extension finie (i.e. de degré fini) est algébrique.

Pour tout élément x algébrique sur $\mathbb{K}$, il existe un unique polynôme unitaire de degré minimal annulant x, le **polynôme minimal**. Ce polynôme est irréductible sur $\mathbb{K}$. On dit que x et y sont conjugués s'il ont même polynôme minimal.

i. Transcendance

Soit une extension $\mathbb{L}$ de $\mathbb{K}$. Un élément $x \in \mathbb{L}$ est **transcendant** sur $\mathbb{K}$ s'il n'est pas algébrique. Le degré $[\mathbb{L} : \mathbb{K}]$ est alors infini.

Pour $x_1, .., x_m \in \mathbb{L}$, nous définissons l'anneau $\mathbb{K}[x_1, ..., x_m] \subset \mathbb{L}$, qui est l'image de $\mathbb{K}[X_1, ..., X_m]$ par le morphisme $X_i \mapsto x_i$. Son corps des fractions $\mathbb{K}(x_1, ..., x_m)$ est le sous-corps de $\mathbb{L}$ engendré par $\mathbb{K}$ et $x_1, ..., x_m$.

Le **degré de transcendance** de $\mathbb{L}$ sur $\mathbb{K}$ est le plus petit m tel que $\mathbb{L}$ soit une extension algébrique d'un corps $\mathbb{K}(x_1, ..., x_m)$. Par exemple, si $\mathbb{L}$ est algébrique sur $\mathbb{K}$, son degré de transcendance est 0. Autre exemple, le degré de transcendance de $\mathbb{R}$ sur $\mathbb{Q}$ est infini.

j. Polynôme caractéristique, trace et norme

Soit $x \in \mathbb{L}$ une extension finie de $\mathbb{K}$. La multiplication par x dans $\mathbb{L}$ peut être vue comme une application linéaire de $\mathbb{L}$ en tant qu'espace vectoriel sur $\mathbb{K}$. Son polynôme caractéristique est appelé **polynôme caractéristique** de l'élément x dans l'extension $\mathbb{L}$ de $\mathbb{K}$, il est noté $Car_{\mathbb{L}/\mathbb{K}}(x)$. Il est égal au polynôme minimal de x, à la puissance $[\mathbb{L} : \mathbb{K}(x)]$.

Nous écrivons $Car_{\mathbb{L}/\mathbb{K}}(x) = \sum(-1)^{d-i}s_{d-i}(x)X^i$, où $d = [\mathbb{L} : \mathbb{K}]$. Le nombre $s_k(x) \in \mathbb{K}$ est appelé **k-ième fonction symétrique de x dans $\mathbb{L}/\mathbb{K}$**. La trace et la norme sont respectivement $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = s_1(x)$ et $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(x) = s_d(x)$.

k. Clôture algébrique

Un corps $\mathbb{K}$ est algébriquement clos s'il n'a pas d'extension algébrique propre. Cela signifie que tout polynôme de $\mathbb{K}[X]$ est scindé.

Une extension algébrique de $\mathbb{K}$ qui est algébriquement close est appelée **clôture algébrique** de $\mathbb{K}$. Les clôtures algébriques de $\mathbb{K}$ sont isomorphes, on en choisit une qu'on note $\bar{\mathbb{K}}$.

I.1.2 Corps de nombres

La théorie algébrique est plus facile à appréhender lorsque le corps de base est un corps primitif: le corps des nombres rationnels $\mathbb{Q}$ ou un corps premier $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Les systèmes algébriques que nous manipulerons seront définis sur $\mathbb{Q}$.

Un **corps de nombres** est une extension $\mathbb{K}$ de degré fini du corps $\mathbb{Q}$ des rationnels. Les éléments d'un corps de nombres sont donc algébriques sur $\mathbb{Q}$. On les appelle les **nombres algébriques**.

a. Anneau des entiers

Il faut remarquer que $\mathbb{Q}$ est le corps des fractions de l'anneau $\mathbb{Z}$ des entiers relatifs. Si les coefficients du polynôme minimal d'un nombre algébrique sont tous des entiers relatifs, on dit que ce nombre est un **entier algébrique**. L'ensemble des entiers algébriques de $\mathbb{K}$ est appelé l'**anneau des entiers**, noté $\mathbb{Z}_{\mathbb{K}}$. C'est un $\mathbb{Z}$-module libre de rang $[\mathbb{K} : \mathbb{Q}]$, dont les bases sont appelées **bases intégrales** de $\mathbb{K}$.

On appelle **contenu** d'un polynôme $P \in \mathbb{Q}[X]$ le plus grand rationnel positif c tel que $c^{-1}P$ n'ait que des coefficients entiers. Par abus de langage, on appelle aussi polynôme minimal d'un nombre algébrique le quotient du polynôme minimal par son contenu. C'est ainsi le polynôme à coefficients entiers, de degré minimal et de coefficient dominant minimal positif, annulant ce nombre. Les entiers algébriques sont alors les nombres dont le polynôme minimal est unitaire.

b. Élément primitif

Le théorème de l'élément primitif affirme que tout corps de nombres est isomorphe à un quotient $\mathbb{Q}[X]/(P)$, où P est de degré $d = [\mathbb{K} : \mathbb{Q}]$. Le polynôme P a au moins une racine α dans $\mathbb{K}$, qui est par définition un **élément primitif** de $\mathbb{K}$.

La famille $(1, \alpha, \alpha^2, ..., \alpha^{d-1})$ engendre $\mathbb{K}$ comme espace vectoriel sur $\mathbb{Q}$, ce qui signifie que $\mathbb{K}$ est égal à $\mathbb{Q}[\alpha]$. En revanche, l'anneau $\mathbb{Z}[\alpha]$ n'est que rarement égal à $\mathbb{Z}_{\mathbb{K}}$.

Si α est un entier algébrique, on a évidemment l'inclusion $\mathbb{Z}[\alpha] \subset \mathbb{Z}_{\mathbb{K}}$. On note alors $[\mathbb{Z}_{\mathbb{K}} : \mathbb{Z}[\alpha]]$ l'indice du sous-groupe $\mathbb{Z}[\alpha]$ dans $\mathbb{Z}_{\mathbb{K}}$ (cf. paragraphe II.1.2.d.). On l'appelle aussi **indice** de α dans $\mathbb{Z}_{\mathbb{K}}$. Si $d > 2$, il n'existe pas toujours d'élément d'indice 1, par exemple dans $\mathbb{Q}[X]/(X^3 + X^2 - 2X + 8)$.

c. Plongements

Soit $\mathbb{L}$ est une extension algébriquement close du corps de nombres $\mathbb{K}$, par exemple le corps $\mathbb{C}$ des nombres complexes ou $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. Le polynôme minimal d'un élément primitif $\alpha \in \mathbb{K}$, irréductible de degré d sur $\mathbb{Q}$, a d racines distinctes α_i dans $\mathbb{L}$. Chaque application $\alpha \mapsto \alpha_i$ donne un **plongement** de $\mathbb{K}$ dans $\mathbb{L}$. Ce sont les seuls. Nous notons σ_i ces plongements. Dans le cas $\mathbb{L} = \mathbb{C}$, chaque plongement donne ainsi une vision géométrique du corps $\mathbb{K}$.

On dit qu'un corps de nombres de degré d est **galoisien** ou normal, si les ensembles $\sigma_i(\mathbb{K})$ sont égaux dans $\mathbb{L}$. C'est le cas si et seulement si le polynôme minimal de α est scindé dans $\mathbb{K}$, ce qui signifie que α a d conjugués. Le corps $\mathbb{K}$ est galoisien si, et seulement si, il a d automorphismes distincts, qui sont les $\sigma_i\sigma_j^{-1}$. Ces automorphismes forment un groupe qu'on note $Gal(\mathbb{K}/\mathbb{Q})$. Les automorphismes d'une clôture algébrique $\bar{\mathbb{Q}}$ forment le groupe de Galois absolu $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

d. Discriminant

Soit $[\mathbb{K} : \mathbb{Q}] = d$ et une famille $(x_1, ..., x_d) \in \mathbb{K}$. Le déterminant de la matrice $(\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x_i x_j))_{i,j}$ est un nombre rationnel, dont le carré est appelé discriminant de la famille, noté $d(x_1, ..., x_d)$. C'est aussi le nombre $[det(\sigma_i(x_j))]^2$.

Le discriminant d'une base intégrale de $\mathbb{K}$ ne dépend pas du choix de la base intégrale, et est donc appelé **discriminant** du corps de nombres, noté $d(\mathbb{K})$. Deux corps de nombres distincts peuvent avoir même discriminant. Par exemple $\mathbb{Q}[X]/(X^4+2X^3+6X^2-6)$ et $\mathbb{Q}[X]/(X^4+2X^3-3X^2-4X-2)$ ont pour discriminant -8640 et sont distincts.

Pour un polynôme irréductible $P \in \mathbb{Q}[X]$ de degré d et de coefficient dominant c, on note $d(P)$ le discriminant du polynôme, qui vaut $c^{2(d-1)}d(1, \alpha, ...\alpha^{d-1})$ où α est une racine quelconque de P. Si $\mathbb{K} = \mathbb{Q}[X]/(P)$, alors $d(P) = d(\mathbb{K})f^2$ où f est appelé **indice** du polynôme et est égal à l'indice de α.

e. Représentation d'un corps de nombres

Le livre de Cohen [11] est la référence sur les problèmes algorithmiques en théorie des nombres.

On peut représenter $\mathbb{K}$ comme sous-corps d'un corps défini auparavant, ou bien par un polynôme tel que $\mathbb{K} \simeq \mathbb{Q}[X]/(P)$. Plusieurs polynômes conviennent, il est préférable d'en trouver un de petite «taille» (voir en particulier [11, p171]). Le calcul d'une base intégrale et du discriminant du corps est souvent la première étape de l'étude d'un corps de nombres. Des algorithmes le permettent, mais le temps de calcul est souvent impraticable.

f. Représentation d'un nombre algébrique

Si ce nombre est dans un corps $\mathbb{K}$ connu, dont on connaît une base sur $\mathbb{Q}$ (une base intégrale par exemple) on utilise ses coordonnées dans cette base.

Nous aurons besoin de faire des opérations dans un corps de nombres inconnu a priori. Il est donc naturel de représenter un nombre par son polynôme minimal, et d'effectuer les opérations de $\bar{\mathbb{Q}}$ à l'aide de calcul de résultants de polynômes [11, pp156–159]. Mais cette représentation ne distingue pas les nombres algébriques conjugués. Pour y arriver, on utilise en plus une approximation du nombre considéré.

I.1.3 Approximation d'un nombre algébrique

La méthode numérique que nous proposons dans la section I.3 utilise des approximations de la solution du système algébrique. Nous devons donc définir une distance entre les éléments de $\bar{\mathbb{Q}}$.

a. Corps métrique

Un corps $\mathbb{K}$ est un corps métrique s'il est muni d'une fonction φ de $\mathbb{K}^\times$ dans $\mathbb{R}_{>0}$ telle que $\varphi(x+y) \leqslant \varphi(x) + \varphi(y)$ et $\varphi(xy) = \varphi(x)\varphi(y)$, étendue sur $\mathbb{K}$ avec $\varphi(0) = 0$. La fonction φ est appelée une **valeur absolue**. Elle est ultramétrique lorsque $\varphi(x+y) \leqslant \max(\varphi(x), \varphi(y))$. Nous ignorerons la valeur absolue triviale où $\varphi(\mathbb{K}^\times) = \{1\}$.

La distance entre x et y est $\varphi(x-y)$. Une suite (x_n) **converge** vers x si la limite (réelle) de $\varphi(x_n - x)$ est 0. Deux valeurs absolues sur $\mathbb{K}$ sont équivalentes si elles définissent la même notion de convergence, c'est-à-dire la même topologie. Les valeurs absolues équivalentes à φ sont les φ^α, pour $\alpha > 0$. Les classes d'équivalence de valeurs absolues sont appelées **places**.

b. Valeur absolue p-adique

On appelle **valuation discrète**† d'un corps $\mathbb{K}$ toute fonction v de $\mathbb{K}$ dans $\mathbb{Z} \cup \{-\infty\}$ telle que $v(0) = -\infty$, $v(\mathbb{K}^\times) = \mathbb{Z}$, $v(xy) = v(x) + v(y)$ et $v(x+y) \geqslant \min(v(x), v(y))$.‡

Sur tout corps $\mathbb{K}$ muni d'une valuation discrète v, on construit une **valeur absolue** associée comme suit : on choisit un réel $\rho \in]0,1[$; la valeur absolue de x est $|x|_v = \rho^{v(x)}$. Cette valeur absolue est ultramétrique.

Soit π un idéal premier de l'anneau des entiers $\mathbb{Z}_\mathbb{K}$, on définit la valuation π-adique sur $\mathbb{K}$ qui à tout $x \in \mathbb{K}^\times$ associe l'entier $v_\pi(x)$ tel que l'idéal principal (x) se décompose en $(x) = \pi^{v_\pi(x)} \frac{\mathfrak{a}}{\mathfrak{b}}$ où les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ ne sont pas divisibles par π. En particulier, si p est un entier premier, la valuation p-adique sur $\mathbb{Q}$ donne $v_p(x)$ tel que $x = p^{v_p(x)} \frac{a}{b}$ avec a et b non divisibles par p. Ce sont des valuations discrètes. Les valeurs absolues associées sont notées $|\cdot|_\pi$ et $|\cdot|_p$.

c. Places de $\mathbb{Q}$ et de ses extensions

Si on choisit un plongement σ de $\mathbb{K}$ dans $\mathbb{C}$, le module des nombres complexes est une valeur absolue de $\mathbb{K}$, qu'on note $|\cdot|_\sigma$. Pour les rationnels, c'est la valeur absolue usuelle.

Toutes les valeurs absolues sur $\mathbb{K}$ sont équivalentes à une valeur absolue π-adique (places finies) ou à une valeur absolue $|\cdot|_\sigma$ (places infinies).

---

† Ce que nous avons appelé *valeur absolue* est souvent appelé *valuation*. Une valuation discrète est alors une valuation dont l'image est un sous-groupe discret de $\mathbb{R}_{>0}$, et ce que nous appelons *valuation discrète* est appelé *valuation exponentielle*.

‡ Un exemple est le degré d'une fraction rationnelle, dans le corps $\mathbb{K}(X)$.

d. Complétion

Soient $\mathbb{K}$ un corps métrique et $x \in \mathbb{K}$. Si l'élément $\tilde{x}$ est à une distance au plus ϵ de x, on dit que $\tilde{x}$ est une approximation à ϵ près de x. Si nous avons une suite $(\tilde{x}_n)_{n\in\mathbb{N}}$ et un réel $\rho \in]0,1[$ tels que tout $\tilde{x}_n$ est une approximation à ρ^n près des $\tilde{x}_k$ pour $k > n$, il est légitime de considérer que cette suite converge vers une certaine valeur. On dit qu'un corps métrique $\mathbb{K}$ est **complet** si toutes ces suites (dites de Cauchy) convergent dans $\mathbb{K}$.

Le complété de $\mathbb{Q}$ pour $|\cdot|_\infty$ est l'ensemble des nombres réels $\mathbb{R}$. La clôture algébrique de $\mathbb{R}$ est le corps (complet) des nombres complexes. C'est aussi le complété de $\bar{\mathbb{Q}}$ pour ses places infinies.

Les complétés de $\mathbb{Q}$ pour les valeurs absolues p-adiques sont les corps p-adiques $\mathbb{Q}_p$. Les complétés des corps de nombres pour les places finies sont des extensions finies de $\mathbb{Q}_p$. Leur clôture algébrique $\bar{\mathbb{Q}}_p$ n'est pas complète. On appelle $\mathbb{C}_p$ le complété de $\bar{\mathbb{Q}}_p$, qui est lui aussi algébriquement clos.

e. Approximation d'un rationnel dans la métrique usuelle

Soit $x \in \mathbb{R}$. Soient deux entiers $N \geqslant 2$ et $k \in \mathbb{Z}$. Il existe un nombre de la forme $\tilde{x} = AN^{-k}$ où $A \in \mathbb{Z}$ tel que $|x - \tilde{x}|_\infty \leqslant N^{-k}$. On dit que $\tilde{x}$ est une approximation à k décimales en base N du nombre x. Si $x = \frac{a}{b} \in \mathbb{Q}$, on calcule A comme quotient euclidien de aN^k par b.

f. Approximation d'un rationnel dans une métrique p-adique

Soit $x \in \mathbb{Q}_p$. Soit un entier $k \in \mathbb{Z}$. Il existe un nombre de la forme $\tilde{x} \in \mathbb{Z}$ tel que $v_p(x - \tilde{x}) \geqslant k$, c'est-à-dire $|x - \tilde{x}|_p \leqslant \rho^k$. On dit que $\tilde{x}$ est une approximation p-adique de précision k. Si $x = p^{v_p(x)}a/b \in \mathbb{Q}$, on calcule $\tilde{x}$ comme suit :

- lorsque $v_p(x) \geqslant k$, $\tilde{x} = 0$,
- lorsque $v_p(x) \leqslant k$, $\tilde{x} = p^{v_p(x)}\left(a/b \bmod p^{k-v_p(x)}\right)$.

g. Approximation d'un nombre algébrique dans $\mathbb{C}$

Le corps $\mathbb{C}$ est une extension de $\mathbb{R}$ de degré 2. Tout nombre complexe peut donc s'écrire sous la forme $a + ib$ avec $a, b \in \mathbb{R}$. Étant donné un plongement de $\bar{\mathbb{Q}}$ dans $\mathbb{C}$, nous pouvons approcher tout nombre algébrique par un couple d'approximations de réels.

L'inconvénient de ce type d'approximation est que la précision est difficile à maîtriser. Le calcul par intervalles (plusieurs milliers de publications sur le sujet, d'après Neumaier [35]) est une solution élégante aux problèmes de précision, mais nous nous contenterons de vérifier a posteriori les résultats (algébriques) de nos calculs.

h. Approximation p-adique d'un nombre algébrique

Le corps $\mathbb{C}_p$ est de degré infini sur $\mathbb{Q}_p$. La clôture algébrique $\bar{\mathbb{Q}}_p$ est elle aussi de degré infini sur $\mathbb{Q}_p$. Nous ne pouvons donc pas approcher les nombres algébriques aussi simplement qu'avec la métrique usuelle.

Cependant, pour tout n fixé, il y a un nombre fini d'extensions de $\mathbb{Q}_p$ de degré n. Il existe donc une famille finie $(\theta_i) \in \bar{\mathbb{Q}}_p$ telle que tout élément algébrique sur

$\mathbb{Q}_p$ de degré au plus n soit une combinaison linéaire des θ_i à coefficients dans $\mathbb{Q}_p$. Mais cet ensemble n'est pas stable par multiplication, il est donc impossible de s'en servir pour faire des calculs approchés.

En revanche, pour tout corps de nombres $\mathbb{K}$, il existe une infinité de p tels que $\mathbb{K} \hookrightarrow \mathbb{Q}_p$ (Tchebotarev). Si $\mathbb{K} = \mathbb{Q}[X]/(P)$, ce sont les p tels que P ait au moins une racine modulo p. Pour un tel p, on peut faire des calculs approchés dans la métrique p-adique.

I.1.4 Système algébrique

Nous donnons les définitions qui nous sont nécessaires. Le livre de Fulton [21] donne une présentation agréable des bases de la géométrie algébrique, nettement plus complète et très lisible.

a. Espace affine, projectif

Pour un corps $\mathbb{K}$, nous notons $\mathbb{A}^m(\mathbb{K})$ l'espace affine $\mathbb{K}^m$ de dimension m. Les zéros dans $\mathbb{K}$ d'un polynôme de $\mathbb{K}[X_1, ..., X_m]$ sont donc éléments de $\mathbb{A}^m(\mathbb{K})$.

Si P est un polynôme homogène, tout multiple d'un zéro de P est aussi un zéro. L'ensemble des zéros d'un polynôme homogène est donc un ensemble de droites passant par l'origine. Nous notons $\mathbb{P}_m(\mathbb{K})$ l'espace projectif de dimension m, qui est l'ensemble des droites de $\mathbb{K}^{m+1}$ passant par l'origine.

b. Variété algébrique

Nous appellerons **système algébrique** une famille $F = (f_i)$ de polynômes de $\mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, ..., X_m]$. On s'intéresse aux zéros simultanés de tous ces polynômes, dans $\mathbb{K}$ ou dans $\bar{\mathbb{K}}$.

L'intersection des $V_{\mathbb{K}}(f_i)$ (zéros sur $\mathbb{K}$ de f_i) est une partie de $\mathbb{A}^m(\mathbb{K})$ qu'on appelle un ensemble algébrique affine sur $\mathbb{K}$. L'intersection des $V_{\bar{\mathbb{K}}}(f_i)$ est une **variété algébrique** (affine).† Si V est une variété algébrique, on note $V(\mathbb{K})$ l'ensemble des points $\mathbb{K}$-rationnels de V, c'est-à-dire $V \cap \mathbb{A}^m(\mathbb{K})$.

Lorsqu'on considère des polynômes homogènes de $\mathbb{K}[X_0, ..., X_m]$, l'ensemble des points annulant le système est une **variété projective**, incluse dans l'espace projectif $\mathbb{P}^m(\bar{\mathbb{K}})$.

c. Homogénéisation, déshomogénéisation

Dans la plupart des cas, il y a une correspondance entre variétés affines et projectives et entre polynômes de $\mathbb{K}[X_1, ..., X_m]$ et polynômes homogènes de $\mathbb{K}[X_0, ..., X_m]$. Il existe cependant quelques pièges que nous ne détaillerons pas, dus à la présence de l'hyperplan à l'infini; voir par exemple [21, p96 et suivantes]. Nous nous placerons donc dans le cas affine en sachant qu'il aurait été possible d'étudier le cas projectif.

Pour $P \in \mathbb{K}[X_1, ..., X_m]$ de degré total d, nous notons P^* le polynôme homogène correspondant, qui vaut $P^*(X_0, ..., X_m) = X_0^d P(X_1/X_0, ..., X_m/X_0)$. À l'inverse, la déshomogénéisation d'un polynôme homogène P est le polynôme $P_*(X_1, ..., X_m) = P(1, X_1, ..., X_m)$.

† Fulton définit une variété algébrique comme un ensemble algébrique affine **irréductible** sur un corps algébriquement clos. Nous ne limitons pas au cas irréductible, car la résolution d'un système algébrique amène habituellement à une variété ayant plusieurs composantes.

d. Idéal engendré

Nous notons $I = \langle f_i \rangle$ l'idéal de $\mathbb{K}[\mathbf{X}]$ engendré par les polynômes f_i. L'ensemble intersection des $V(f_i)$ ne dépend que de l'idéal, on le note donc $V(I)$.

Soit X une partie quelconque de l'espace affine $\mathbb{A}^m$. L'ensemble de polynômes s'annulant sur X est un idéal qu'on note $I(X)$.

Le théorème des bases de Hilbert affirme que tout idéal de $\mathbb{K}[\mathbf{X}]$ est engendré par un nombre fini de polynômes. Cela signifie que nous pouvons nous restreindre aux systèmes algébriques finis.

e. Corps de définition

On dit qu'une variété est **définie** sur un corps $\mathbb{K}$ si elle admet un modèle sur $\mathbb{K}$, c'est-à-dire si l'idéal $I(V)$ est engendré par $I(V) \cap \mathbb{K}[X]$.

f. Composantes irréductibles

On dit qu'un ensemble algébrique V est **irréductible** s'il n'est pas la réunion d'ensembles algébriques plus petits. Cette condition est vérifiée si et seulement si l'idéal $I(V)$ est premier.

Tout ensemble algébrique se décompose de façon unique en la réunion d'un nombre fini d'ensembles algébriques irréductibles (dont aucun n'est inclus dans un autre), ses **composantes irréductibles**.

g. Fonctions rationnelles

Si V est une variété irréductible définie sur $\mathbb{K}$, $\Gamma(V) = \mathbb{K}[X_1, ..., X_m]/I(V)$ est un anneau intègre, qu'on appelle **anneau des coordonnées** ou anneau des fonctions régulières de V. Il peut être identifié avec l'anneau des fonctions polynomiales sur V.

Son corps des fractions $\mathbb{K}(V)$ est le corps des **fonctions rationnelles**.

h. Systèmes équivalents

On dit que deux systèmes (f_i) et (g_i) sont équivalents si et seulement s'ils ont la même solution. C'est en particulier le cas si $\langle f_i \rangle = \langle g_i \rangle$. Cependant, la réciproque est fausse : $V(I) = V(J) \not\Rightarrow I = J$. Un contre-exemple est $I = \langle X \rangle$ et $J = \langle X^2 \rangle$.

Sur un corps algébriquement clos, le théorème des zéros de Hilbert (souvent appelé **Nullstellensatz**) donne le critère $V(I) = V(J) \Leftrightarrow \sqrt{I} = \sqrt{J}$.

i. Dimension de la solution

Soit V une variété irréductible sur un corps $\mathbb{K}$. Si nous considérons le corps $\mathbb{K}(V)$ des fonctions rationnelles sur V, on appelle **dimension** de V son degré de transcendance sur $\mathbb{K}$.

Une variété de dimension 0 est un ensemble fini de points. On appelle **courbe algébrique** les variétés de dimension 1. Une **surface** est une variété de dimension 2.

j. Résolution d'un système algébrique

L'objectif de la résolution du système peut être :

1. savoir tester si un polynôme f est élément de I.
2. trouver un ou plusieurs zéros du système, quelques éléments de $V_{\mathbb{K}}(I)$.
3. connaître le nombre d'éléments de $V_{\mathbb{K}}(I)$.
4. calculer les composantes irréductibles de $V_{\mathbb{K}}(I)$, leur dimension.

k. Exemple de système, pour un dessin très simple

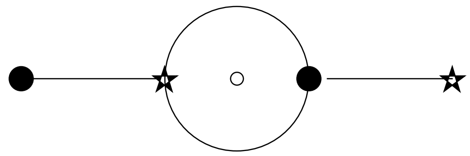


FIG. I.1 – *Exemple de dessin, de valences [31,31,31]*

On cherche la fonction de Belyi du dessin de la figure I.1, c'est-à-dire une fraction rationnelle β, telle que la préimage $\beta^{-1}([0,1])$ dessine le graphe de la figure. Le système correspondant est défini par (cf. chapitres II et III) :

$$(x+p_a)^3(x+p_b) = \lambda x + (x+q_a)^3(x+q_b). \tag{I.1}$$

La variété solution a deux composantes :

$$\begin{array}{llll} \lambda = 0, & p_a = q_a, & p_b = q_b, & \Gamma'' \text{ de dimension } 2\,; \\ \lambda = -16p_a^3, & p_a+q_a = p_b+q_b = 0, & 3p_a+p_b = 0, & \Gamma' \text{ de dimension } 1. \end{array}$$

Si on élimine la première composante (en imposant $\lambda \neq 0$, par exemple en rajoutant une inconnue μ et l'équation $\lambda\mu = 1$) et si on fixe l'échelle du dessin (en rajoutant l'équation $p_a + p_b = 2$) le système obtenu a une unique solution :

$$\lambda = 16, \quad \mu = 1/16, \quad p_a = -1, \quad p_b = 3, \quad q_a = 1, \quad q_b = -3.$$

L'égalité (I.1) est donc $(x-1)^3(x+3) = 16x+(x+1)^3(x-3)$, dont on déduit

$$\beta = \frac{(x-1)^3(x+3)}{16x}.$$

l. Exemple pour un dessin plus élaboré

Le système correspondant au dessin de la figure I.2 (voir aussi § IV.4.3) se construit à partir de l'égalité ci-dessous, plus quelques considérations supplémentaires :

$$\begin{aligned}(x^3+p_ax^2+p_bx+p_c)^4 &= \lambda x^3(x^2-x+r_a)^4 \\ &\quad +(x^5+q_ax^4+q_bx^3+q_cx^2+q_dx+q_e)^2(x^2+q_fx+q_g)\end{aligned}$$

La variété solution qui nous intéresse est de dimension 0, elle a quatre éléments conjugués dans le corps de nombres $\mathbb{Q}[X]/(X^4-2X^3-2X+1)$. Si α est une racine de X^4-2X^3-2X+1, on a :

- $p_a = (19507 - 3072\alpha - 29052\alpha^2 + 9976\alpha^3)/7678$

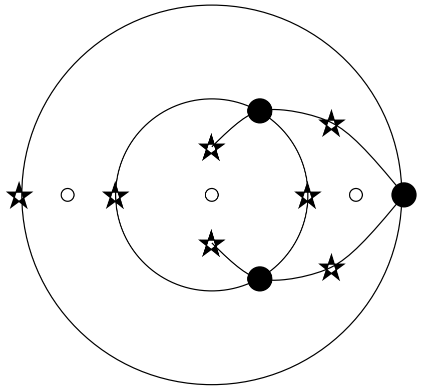


FIG. I.2 – *Exemple de dessin moins simple, de valences* $[1 4^2 3, 4^3, 2^5 1^2]$

- $p_b = (-57446893 + 36552960\alpha - 78891720\alpha^2 + 40777808\alpha^3)/58951684$
- $p_c = (763448412011 + 69993771648\alpha - 1206701651460\alpha^2 + 300422694344\alpha^3)/4978941327272$
- ...
- $r_a = (1541977 - 1470816\alpha + 12130864\alpha^2 - 4799104\alpha^3)/16077732$
- $\lambda = (-2009543040 + 223727616\alpha + 2094239232\alpha^2 - 718792704\alpha^3)/56206799$

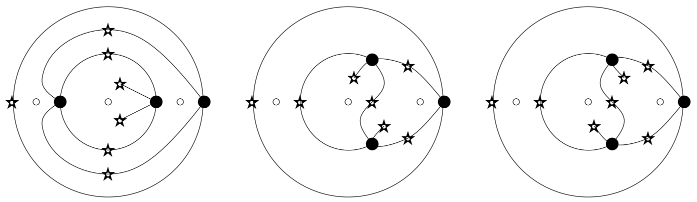


FIG. I.3 – *Les conjugués du dessin de la figure I.2.*

I.2 Calcul de bases de Gröbner

I.2.1 Un calcul formel sur les polynômes

a. Étapes d'une résolution par bases de Gröbner

La donnée est une famille finie de polynômes engendrant un idéal I de $\mathbb{K}[\mathbf{X}]$. On commence par calculer une base de Gröbner de cet idéal. C'est une autre famille génératrice, permettant de tester facilement l'appartenance à l'idéal I.

Ensuite, il est possible d'en déduire quelques informations sur la structure de la variété solution.

b. Valeur des résultats obtenus

Des algorithmes tels celui de Buchberger [10] construisent une base de Gröbner engendrant l'idéal I. Le calcul de la base de Gröbner puis la résolution du système se font avec des opérations exactes, sur les polynômes, leurs résultats sont donc utilisables directement.

Malheureusement, la puissance de calcul et la mémoire nécessaires empêchent souvent le recours à cette méthode. La principale raison de cette lenteur est qu'il est nécessaire de manipuler des polynômes à plusieurs variables, à coefficients dans $\mathbb{K}$. Même des implantations très performantes comme le logiciel GB [19], qui fait aussi des calculs modulo p pour limiter la taille des données, atteignent vite leurs limites lors du calcul de dessins d'enfants.

c. Affine ou projectif

Nous ne décrirons que le cas affine, mais la théorie du calcul de variétés algébriques et d'idéaux de polynômes est plus simple dans le cas homogène (projectif). Cependant, les principes restent les mêmes.

I.2.2 Réduction dans $\mathbb{K}[\mathbf{X}]$

a. Terme dominant d'un polynôme

Soit un polynôme $f = \sum_\alpha f_\alpha \mathbf{X}^\alpha \in \mathbb{K}[\mathbf{X}]$. Nous appellerons† monôme le produit de puissances $\mathbf{X}^\alpha$ et terme un élément non nul $f_\alpha \mathbf{X}^\alpha$. Pour comparer les polynômes, nous choisissons un ordre total sur les monômes. Nous notons $\max(f)$ le monôme dominant du polynôme f, qui est l'élément maximal de son support, et nous notons $\mathrm{maxt}(f)$ le terme correspondant.

b. Principe

Étant donnés deux polynômes f et g, la réduction de f modulo g est une opération qui calcule un certain polynôme $h = f - kg$ où $k \in \mathbb{K}[\mathbf{X}]$ est choisi de telle sorte que $\max(g)$ ne divise aucun élément du support de h. Un tel k est unique, si l'ordre sur les monômes vérifie certaines propriétés de compatibilité (cf. § f.). On a bien sûr l'égalité des idéaux engendrés $\langle h, g\rangle = \langle f, g\rangle$. Lorsque $\max(g)$ ne divise aucun élément du support de f, on dit que f ne peut pas être réduit par g.

La réduction peut se noter comme une règle de réécriture $f \longrightarrow_g h$. Soit une famille de polynômes G, on dit que f se réduit en h par rapport à G s'il existe une suite non vide de réductions de f par des éléments de G qui aboutit à h. Cela se note $f \xrightarrow{+}_G h$. Cette opération permet de transformer une famille génératrice d'un idéal en une autre plus simple.

On dit que r est un **reste de la réduction** de f par G si $f \xrightarrow{+}_G r$ et si r est nul ou ne peut être réduit par aucun élément de G.

† La terminologie varie selon les auteurs. M. Giusti appelle *forme dominante* ce que nous appelons *terme dominant*.

c. Le cas des polynômes à une variable

Les monômes sont bien sûr ordonnés par leur degré. La division euclidienne nous donne la réduction dans $\mathbb{K}[X]$: le polynôme k est le quotient de la division de f par g et le polynôme h en est le reste.

d. Le cas linéaire

Nous devons choisir un ordre sur les indéterminées, par exemple $X_i < X_j$ si $i < j$. La réduction du pivot de Gauss est un exemple de l'opération de réduction décrite plus haut.

Soient f et g deux polynômes linéaires non nuls, avec $X_i = \max(g)$. Si le coefficient f_i est non nul, alors la réduction de Gauss calcule $h = f - \frac{f_i}{g_i} g$ qui ne fait plus intervenir la variable X_i.

e. Généralisation

Voici un algorithme de réduction. Si $\max(g)$ divise un terme non nul X de f, nous calculons $h = f - \frac{X}{\mathrm{maxt}(g)} g$, que nous notons $f \bmod_X g$. Si l'ordre sur les monômes est compatible, cette opération diminue le nombre de termes divisibles par $\max(g)$, le polynôme $f \bmod g$ est obtenu après avoir effectué toutes les réductions par g possibles.

f. Ordre sur les monômes

Pour que la réduction ait les propriétés ci-dessus, l'ordre sur les $\mathbf{X}^\alpha$ doit vérifier les trois conditions ci-dessous :

- ce doit être un ordre total,
- le monôme 1 est strictement inférieur à tous les autres,
- si $\mathbf{X}^\alpha < \mathbf{X}^\beta$ alors $\mathbf{X}^{\alpha+\gamma} < \mathbf{X}^{\beta+\gamma}$.

Les ordres habituellement choisis par les programmes de calcul formel sont les quatre ci-dessous. Ils présupposent un ordre sur les indéterminées, donné par leurs indices. Les ordres *du degré* sont une transposition au cas affine des ordres sur les monômes homogènes. Il ont ainsi de meilleures propriétés théoriques.

L'ordre lexicographique où $\mathbf{X}^\alpha <_{lex} \mathbf{X}^\beta$ s'il existe un indice i tel que : $\alpha_0 = \beta_0, ..., \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i$.

L'ordre lexicographique réverse : est défini comme suit : $\mathbf{X}^\alpha <_{revlex} \mathbf{X}^\beta$ s'il existe un indice i tel que : $\alpha_i > \beta_i, \alpha_{i+1} = \beta_{i+1}, ..., \alpha_m = \beta_m$.

L'ordre du degré, lexicographique : nous avons $\mathbf{X}^\alpha <_{deglex} \mathbf{X}^\beta$ si le degré total de $\mathbf{X}^\alpha$ est strictement inférieur à celui de $\mathbf{X}^\beta$, ou bien s'ils ont même degré total et sont dans l'ordre lexicographique.

L'ordre du degré, lexicographique réverse : $\mathbf{X}^\alpha <_{degrevlex} \mathbf{X}^\beta$ si le degré total de $\mathbf{X}^\alpha$ est strictement inférieur à celui de $\mathbf{X}^\beta$, ou bien s'ils ont même degré total et sont dans l'ordre lexicographique réverse. Il diffère de l'ordre du degré lexicographique dès qu'il y a au moins trois variables.

g. Calcul du reste

Nous pouvons imaginer un algorithme élémentaire pour calculer un reste de la réduction de f par rapport à G : Nous commençons par poser $h = 0$. S'il existe un g_i tel que $\max(g_i)$ divise $\max(f)$, nous réduisons f modulo g_i. Sinon, nous remplaçons f par $f - \mathrm{maxt}(f)$ et h par $h + \mathrm{maxt}(f)$. Cet algorithme s'arrête. La valeur finale de h est un reste de la réduction de f par G.

L'exemple de la réduction de $f = X_1$ par $G = \{X_1 + X_2, X_1 - X_2\}$ nous montre que le reste de la réduction de f par un ensemble G n'est pas unique, il dépend des choix de g_i à chaque étape.

Dans le cas ou G est un idéal, le reste de la réduction par G est unique. C'est le théorème de division d'Hironaka [25].

h. Notion de base de Gröbner

Une partie finie G d'un idéal $I \subset \mathbb{K}[\mathbf{X}]$ est une base de Gröbner (terminologie de Buchberger) ou base standard (terminologie d'Hironaka) si et seulement si, pour tout $f \in I$ non nul, il existe $g \in G$ tel que $\max(g)$ divise $\max(f)$. Cela s'écrit aussi, avec les notations de réécriture : $f \in I \Leftrightarrow f \xrightarrow{*}_G 0$.

Nous pouvons remarquer que si on ajoute un polynôme de l'idéal à une base de Gröbner, la propriété est conservée. Une base de Gröbner est minimale si ce n'est plus une base lorsqu'on enlève un polynôme. Dans une telle base, les $\max(g)$ sont distincts. La résolution du système utilise le calcul d'une base de Gröbner minimale.

I.2.3 Réduction de S-polynômes

a. Les S-polynômes

Si g_1 et g_2 sont deux polynômes non nuls, nous pouvons définir L le PPCM formel des monômes $\max(g_1)$ et $\max(g_2)$. Le S-polynôme (qu'on appelle aussi polynôme de syzygie dans le cas homogène) de g_1 et g_2 est par définition :

$$S(g_1, g_2) = \frac{L}{\mathrm{maxt}(g_1)} g_1 - \frac{L}{\mathrm{maxt}(g_2)} g_2.$$

C'est une généralisation du PGCD qui permet de mesurer l'ambiguité introduite par le choix d'une réduction modulo g_1 ou g_2. En effet, si $h_1 = f \bmod_X g_1$ et $h_2 = f \bmod_X g_2$, alors $h_2 - h_1 = \frac{X}{L} S(g_1, g_2)$.

L'idée fondamentale de Buchberger limite la définition d'une base de Gröbner à l'étude des S-polynômes : G est une base de Gröbner de l'idéal qu'elle engendre si et seulement si $\quad \forall g_i, g_j \in G, \quad S(g_i, g_j) \xrightarrow{+}_G 0$.

b. Calcul d'une base de Gröbner

Ceci permet de concevoir un algorithme pour calculer une base de Gröbner, en calculant les restes de la réduction par G des $S(g_i, g_j)$.

L'algorithme de Buchberger ajoute progressivement et récursivement au système $G = \{g_i\}$ tous les restes non nuls de la réduction par G de tous les $S(g_i, g_j)$. Les stratégies de sélection des $S(g_i, g_j)$ ont fait l'objet de nombreuses recherches, la stratégie dite du *sucre* est habituellement considérée comme la plus performante [22].

Le logiciel GB, pour les systèmes à coefficients entiers calcule simultanément une base modulo p.

c. Choix de l'ordre des monômes

Pour l'ordre lexicographique, la manipulation de polynômes de degré élevé handicape le calcul d'une base de Gröbner. On prouve que si les polynômes du système de départ sont de degré au plus d avec m variables, la complexité du calcul est $d^{\mathcal{O}(m^3)}$ si le système est de dimension 0.

En revanche, l'ordre du degré réverse limite le degré des polynômes manipulés et obtient une bien meilleure efficacité avec une complexité de d^{m^2} (qui descend à d^m si le système homogène correspondant est de dimension 0).

Il est bien plus facile de déduire la géométrie de la solution à partir d'une base lexicographique, dont les premiers éléments font intervenir un petit nombre de variables.

Faugère, Gianni, Lazard et Mora [20] ont donc proposé une méthode efficace pour changer d'ordre, en dimension 0. Cet algorithme a été implanté dans GB et Axiom. L'efficacité de cette méthode est telle qu'on a souvent intérêt à calculer une base pour l'ordre du degré puis à la transformer en une base pour l'ordre lexicographique, plutôt qu'un calcul entièrement selon l'ordre lexicographique.

d. Dimension 0 et systèmes triangulaires

La description d'une variété d'une façon intelligible n'est pas facile lorsqu'elle est de dimension positive. Une variété de dimension 0 peut être décrite par la liste (finie) de ses points, dans leur corps de définition. On représente ceci sous la forme d'une collection de systèmes triangulaires, chacun correspondant à quelques orbites sous l'action de Galois.

Sur $\mathbb{K}[X_1, ..., X_m]$ avec les variables ordonnées dans cet ordre, un ensemble de m polynômes est dit **triangulaire** si le i-ième polynôme est un polynôme unitaire de $\mathbb{K}[X_1, ..., X_{i-1}][X_i]$. Tout idéal maximal admet une base triangulaire, ce qui permet de prouver que toute variété de dimension 0 est réunion d'un nombre fini de variétés issues de systèmes triangulaires.

D. Lazard [27] propose des méthodes pour rendre cette représentation effective, à partir d'une base de Gröbner de l'idéal. Ceci est nettement plus efficace à partir d'une base de Gröbner pour l'ordre lexicographique, ce qui confirme la remarque du paragraphe précédent.

On peut remarquer qu'il est facile de tester si une variété est de dimension 0 lorsqu'on en connaît une base de Gröbner (pour n'importe quel ordre). C'est le cas si, et seulement si, l'ensemble des monômes dominant des éléments de la base contient une puissance de chacun des X_i.

I.3 Méthode numérique

I.3.1 Un calcul approché dans un corps de nombres

a. Méthode en trois étapes

La donnée est une famille finie de polynômes engendrant un idéal I de $\mathbb{K}[X_1, ..., X_m]$, où $\mathbb{K}$ est un corps de nombres, habituellement $\mathbb{Q}$. Nous construisons une approximation de la solution, c'est à dire un ou plusieurs points très proches de $V_{\mathbb{K}}(I)$, et nous en déduisons la structure algébrique de cette variété.

Pour cela, nous commençons par fabriquer une approximation grossière d'un point solution. Nous faisons ensuite converger numériquement cette valeur vers une meilleure approximation, suffisamment précise. Cela nous permettra de retrouver la valeur exacte du point solution, et ensuite d'en déduire (une partie au moins) de la structure de la variété solution.

Chacune de ces étapes doit être adaptée au type de système étudié, si nous voulons que cette méthode puisse être compétitive avec la recherche d'une base de Gröbner. C'est envisageable si le système n'est pas quelconque mais s'il est construit pour représenter un objet plus riche, tel un dessin d'enfant.

b. Valeur des résultats obtenus

Il est toujours possible de vérifier par des calculs exacts (dans $\mathbb{K}[X_1, ..., X_m]$) le résultat de nos calculs. Cette méthode permet donc de trouver une solution du système, ou bien une famille de solutions.

Il est parfois possible d'en déduire une description de l'ensemble solution mais, en général, si notre méthode ne trouve pas de solution, cela ne prouve pas que le système n'en a pas. De plus, si la variété se décompose en variétés irréductibles de dimensions différentes, il est très probable que la méthode numérique n'aboutisse qu'à des points des composantes de dimension maximale.

I.3.2 Convergence

a. Algorithme de Newton

À partir d'une valeur $\tilde{y} = (\tilde{y}_1, ..., \tilde{y}_m)$ proche d'une solution y du système, nous allons construire des approximations de y aussi précises que nécessaire.

La formule de Taylor, valable pour toute norme, nous donne :

$$||F(\tilde{y} + \delta) - (F(\tilde{y}) + DF(\tilde{y})[\delta])|| = \mathcal{O}(||\delta||^2).$$

Si nous cherchons l'écart $\delta = y - \tilde{y}$, nous savons que $||\delta||$ est petit puisque par hypothèse $\tilde{y}$ est proche de y. Or y est solution du système donc $||F(y)|| = 0$. La formule de Taylor devient $||F(\tilde{y}) + DF(\tilde{y})[\delta]|| = \mathcal{O}(||\delta||^2)$.

Si $DF(\tilde{y})$ est inversible (et donc carrée), nous avons donc un moyen d'obtenir une approximation $\tilde{\delta}$ de δ, et chaque étape de l'algorithme de Newton remplace $\tilde{y}$ par $\tilde{y} + \tilde{\delta}$ où

$$\tilde{\delta} = -DF(\tilde{y})^{-1}[F(\tilde{y})].$$

Il faut inverser $DF(\tilde{y})$, ce qui n'est pas toujours stable numériquement, et il s'agit d'un développement au premier degré, qui ne permet pas toujours de se rapprocher de la solution.

b. Choix de la norme

Lorsqu'on affirme que $\tilde{y}$ est proche de y, cela signifie que nous utilisons une certaine norme sur $\mathbb{K}^m$, donc une valeur absolue sur $\mathbb{K}$. Si deux normes sont équivalentes, la résolution du système se fera de la même façon. C'est donc le choix de la valeur absolue qui importe.

Le choix le plus intuitif est la valeur absolue usuelle (dans $\mathbb{C}$), ce que nous conseillons.

c. Dans $\mathbb{Q}_p$

Lorsqu'on connaît un premier p tel que $\mathbb{K} \hookrightarrow \mathbb{Q}_p$, ce qui n'est pas évident puisqu'habituellement on ne connaît pas $\mathbb{K}$, une approximation p-adique d'une solution y avec une précision k est une solution $\tilde{y}$ du système modulo p^k. Comme la valeur absolue p-adique est ultramétrique, l'algorithme de Newton (qui s'appelle alors lemme de Hensel) restera dans la boule de rayon ρ^k autour de y.

Pour pouvoir inverser la matrice $DF(\tilde{y})$ il faut que son déterminant soit non nul modulo p^k. Ce qui signifie que l'algorithme (de Newton) ne convergera vers y que si l'approximation initiale $\tilde{y}$ est une solution du système modulo p^k où k est supérieur à la valuation p-adique de $DF(y)$.

Sauf pour les petits p, on peut espérer que $k = 1$ suffit, mais la recherche d'une solution modulo p n'est pas facile. On peut l'obtenir par calcul d'une base de Gröbner modulo p, mais si cette recherche aboutit, un logiciel comme GB [19] arrivera vraisemblablement à calculer une base de Gröbner dans $\mathbb{Z}$.

Malle [29] a utilisé la métrique 23-adique pour le groupe $Aut(M_{22})$ des automorphismes du groupe de Mathieu M_{22}, mais cette approche ne paraît pas prometteuse dans le cas général : il avait une connaissance a priori du corps $\mathbb{K}$, et nous montrons au paragraphe IV.5.2 qu'on peut arriver au même résultat à l'aide d'approximations dans $\mathbb{C}$.

d. Dans $\mathbb{C}$

Une variante (classique) de l'algorithme de Newton permet (presque) toujours de se rapprocher d'une solution : on remplace $\tilde{y}$ par $\tilde{y} = \tilde{y} + k\tilde{\delta}$ avec $k \in]0,1]$ de telle sorte que $||F(\tilde{y} + k\tilde{\delta})|| < ||F(\tilde{y})||$. En réalité, on se rapproche ainsi d'un minimum local de $||F||$. Le système et l'approximation initiale doivent être étudiés pour que ce soit un zéro.

Une fois que $\tilde{y}$ est dans la zone de convergence, l'algorithme de Newton aboutit rapidement à la précision demandée. Le nombre de chiffres significatifs gagnés double à chaque étape, ce qui permet de connaître la précision de l'approximation que nous avons calculée.

Il est possible de converger plus vite, par exemple en calculant la différentielle seconde de F.

I.3.3 Choix de l'approximation initiale

a. Problématique

Dans le cas des *dessins d'enfants*, toutes les solutions du système ne sont pas intéressantes. En particulier, il faut éviter les solutions triviales, qui correspondent à la collision de plusieurs points. Ceci peut être obtenu en utilisant une formulation du système qui élimine la plupart des solutions parasites (cf. section III.1.2).

Il faut aussi choisir l'approximation initiale de telle sorte que nous puissions maîtriser la solution vers laquelle convergera le système. C'est ainsi que nous pouvons calculer suffisamment de points pour obtenir la description d'une solution de dimension 1 ou plus.

b. Difficulté du cas général

Dans le cas général, une valeur de départ quelconque risque de ne pas permettre de convergence. En particulier si la variété solution est de dimension 1 ou plus, il y a le risque de se rapprocher de la variété sans se rapprocher d'un point particulier de celle-ci. On voit alors par exemple une fuite vers l'infini.

c. Résolution successives de problèmes proches

Après une étude spécifique, il peut être possible de trouver un système algébrique plus simple, dont les solutions sont proches de celles du système étudié.

Dans le cas de revêtements (dessins d'enfants), le choix naturel est un dessin dont la structure topologique est proche de notre problème. Sa géométrie est alors assez proche de la solution cherchée (cf. III.3.1 et III.3.3).

I.3.4 Algébrisation

a. Conditions

Nous devons connaître a priori la dimension de la variété et avoir suffisamment de points très proches de cette variété.

Le nombre de points et la précision nécessaires ne sont pas toujours faciles à estimer. Nous pouvons contourner cet obstacle en vérifiant formellement nos résultats et en calculant de nouveaux points ou avec une précision plus grande si besoin.

b. Dépendance algébrique, pour une solution de dimension 0

La variété solution est un ensemble fini de points de $\bar{\mathbb{K}}^m$. Pour chaque point $y = (y_1, ..., y_m)$ de la solution nous sommes intéressés par le calcul de son corps de définition $\mathbb{L}$ qui nous permettra d'exprimer ses coordonnées en termes exacts.

Si nous connaissons une borne supérieure $d \geqslant [\mathbb{L} : \mathbb{K}]$ et si P le polynôme minimal de $\xi = y_i$ est de degré supérieur à $d/2$, on en déduit que $\mathbb{L} = \mathbb{K}[X]/(P)$. Nous devons donc trouver le polynôme minimal d'un nombre algébrique dont on connaît une approximation $\alpha \simeq \xi$.

Le calcul de P se fait en remarquant que $P(\alpha)$ est proche de 0. Il s'agit donc de trouver une relation de dépendance linéaire entre $1, \alpha, \alpha^2, ...\alpha^d$ telle que $\sum_{j=0}^d p_j \alpha^j \simeq 0$.

Supposons que $\mathbb{K} = \mathbb{Q}$, nous devons alors chercher des $p_j \in \mathbb{Z}$ tels que $|\sum_{j=0}^d p_j \alpha^j|$ soit minimal. Comme suggéré par Lenstra, Lenstra et Lovász [28], ceci peut être réalisé par la recherche d'un vecteur court dans le réseau décrit au paragraphe suivant.

Il importe que α soit suffisamment proche de ξ, pour que ces p_j soient les coefficients de P. Le paragraphe d'après étudie cette question.

c. Utilisation de l'algorithme LLL

Soit $(V_j)_{j=1..p}$ une famille libre de vecteurs de $\mathbb{Q}^n$. L'ensemble des combinaisons linéaires $\sum_j q_j V_j$ avec $q_j \in \mathbb{Z}$ forme un **réseau** dont (V_j) est une base. Le déterminant du réseau est l'aire p-dimensionnelle du parallélépipède engendré par les V_j ; il ne dépend pas du choix de la base. La notion de **base réduite** d'un réseau peut être définie de plusieurs façons qui ne sont pas équivalentes. Les vecteurs d'une base réduite ont une norme assez petite et sont presque orthogonaux les uns aux autres. Les algorithmes de réduction de réseau, dont LLL, calculent une base réduite, donc un vecteur non nul de norme assez petite. On peut considérer qu'en pratique cette norme est inférieure à la racine p-ième du déterminant Δ du réseau. Il est possible de prouver que pour LLL elle est inférieure à $2^{p(p-1)/2}\Delta^{1/p}$.

À tout polynôme $Q(X) = \sum_{j=0\ldots d} q_j X^j$ on associe le vecteur du réseau $V_Q = \sum_j q_j V_j$. Nous construirons un réseau tel que V_P soit très probablement son vecteur le plus court.

Nous avons le choix de l'algorithme de réduction de réseau : l'algorithme LLL est le plus rapide, il s'exécute en temps polynomial. L'algorithme Korkine-Zolotarev donne une base beaucoup plus réduite, mais en temps exponentiel. Les variantes intermédiaires Block-KZ (avec ou sans élagage de l'arbre de recherche) sont polynomiales mais bien plus lentes que LLL.

Si un algorithme de réduction plus puissant que LLL trouve V_P dans la base réduite du réseau, il est toujours possible, en augmentant légèrement la précision avec laquelle α approche ξ, de construire un autre réseau tel que LLL trouve V_P. L'expérimentation confirme que cette augmentation de précision n'est pas pénalisante et que nous avons intérêt à utiliser LLL, bien plus rapide que les autres algorithmes de réduction.

d. Précision nécessaire

Nous plongeons $\bar{\mathbb{Q}}$ dans $\mathbb{C}$, donc $\xi \in \mathbb{C}$, et nous supposons que $\alpha \in \mathbb{C}$ est un nombre quelconque, proche de ξ. Il faut trouver une valeur $N \in \mathbb{R}_{>0}$ suffisante pour qu'on puisse calculer P dès que $|\alpha - \xi| < 1/N$.

Si nous avons un tel N, nous notons $\Re_j$ et $\Im_j$ les parties entières des parties réelles et imaginaires de $N\alpha^j$. Les $d+1$ vecteurs $V_j = (0, ..., 1, ..., 0, \Re_j, \Im_j)$ pour $j = 0...d$ (avec un 1 en j-ième position) sont libres dans $\mathbb{Q}^{d+3}$ et engendrent donc un réseau. Lorsque $\max|q_j| = K$, sa norme est environ :

$$\|V_Q\| \simeq \max\big(Kd, |NQ(\alpha)|\big).$$

L'ensemble $\mathbb{Z}_{K,d}[X]$ des polynômes de $\mathbb{Z}[X]$ de degré au plus d et de coefficients majorés par K a un nombre fini d'éléments. Si ξ est racine d'un de ces polynômes, alors il existe une borne minimale $\phi_{K,d}$ telle que $\forall\, Q \in \mathbb{Z}_{K,d}[X]$, $Q(\xi) = 0$ ou $|Q(\xi)| \geqslant \phi_{K,d}$.

Supposons que nous avons une borne K sur les coefficients de P le polynôme minimal que nous cherchons. Si $N > Kd/\phi_{K,d}$, alors $\|V_Q\| < Kd \Leftrightarrow Q = P$. Si de plus $N > K^{d+1}$, alors le vecteur calculé par LLL est très probablement V_P.

Malheureusement, la borne $\phi_{K,d}$ est difficile à calculer. Expérimentalement, on remarque que ce n'est pas nécessaire pour les dessins d'enfants. Nous avons mesuré des valeurs comprises entre $0,53$ et $1,18$ pour $\frac{1}{d+1}\frac{\log N}{\log K}$, pour d valant jusqu'à 60. On a aussi remarqué que pour les corps de définition des dessins calculés, $K < 10^{2d}$, ce qui nous donne en première estimation $N = 10^{2d^2}$.

e. Solution de dimension 1

Nous devons calculer des approximations numériques d'un grand nombre de points de la courbe V, pour trouver ensuite un paramétrage naturel. Ceci se fait donc en deux étapes.

Pour avoir suffisamment de valeurs sur V, nous devons faire varier un paramètre du système, par exemple en changeant l'approximation initiale à partir de laquelle nous allons faire converger vers une solution. Il existe une variable y_i du système telle que la projection de V sur le i-ième axe de coordonnées ne soit pas réduite à un point. Nous cherchons par exemple des points de V ayant leur i-ième coordonnée fixée a priori.

Nous avons ainsi un grand nombre de valeurs $\tilde{y} = (\tilde{y}_1, ..., \tilde{y}_m)$ que nous supposerons suffisamment proches de la courbe solution du système, définie sur $\mathbb{K}$. Nous cherchons alors un paramètre rationnel de cette courbe.

Nous devons trouver un nombre suffisant de fonctions ξ_i, fractions rationnelles en les variables du système, pour en extraire un paramètre naturel. Nous faisons ceci par étapes : si nous trouvons une équation polynomiale $P_1(\xi_0, \xi_1) = 0$, nous construisons un paramètre t_2 de la courbe définie par P_1, en désingularisant cette équation. Puis nous cherchons une équation $P_2(t_2, \xi_2) = 0$, d'où un paramètre t_3, jusqu'à avoir un paramètre de V. C'est ce que nous avons mis en œuvre pour le calcul d'un polynôme de groupe de Galois M_{24} (voir § IV.5.4.d.).

Chapitre II

Dessins d'enfants

Les dessins d'enfants ont été nommés d'après les remarques de Grothendieck, qui proposait d'étudier le groupe de Galois absolu $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ au moyen de concepts élémentaires, *si simples qu'un enfant peut les connaître en jouant* [24]. De nombreux mathématiciens ou physiciens ont en effet joué avec ces concepts (voir par exemple l'excellent panorama réuni par L. Schneps [38]).

On peut regrouper les propriétés des dessins en deux ensembles : les propriétés combinatoires, et les propriétés géométriques. Les propriétés combinatoires mêlent théorie des groupes et topologie ; les propriétés géométriques mêlent géométrie algébrique ou analytique et arithmétique. Le lien entre ces deux ensembles de propriétés est souvent appelé *correspondance de Grothendieck*.

Ce chapitre est découpé en trois sections. La première section sert d'introduction, la seconde définit explicitement les dessins d'enfants et les variantes, la troisième section donne quelques propriétés sur le corps des modules d'un dessin, qui facilitent le calcul de la correspondance de Grothendieck.

Nous commençons par décrire de façon informelle et peu rigoureuse les dessins, en présentant rapidement les deux aspects principaux. Ensuite, il est nécessaire de rappeler les nombreuses définitions de combinatoire et de géométrie qui interviennent pour une présentation plus complète des dessins. Nous parlerons des graphes et de leurs plongements dans une surface : les cartes. Les cartes ont naturellement une structure combinatoire et nous rappelerons quelques faits sur les groupes opérant sur un ensemble. Nous définirons aussi les revêtements de variétés, et leur groupe de monodromie. Nous étudierons plus en détail la sphère.

Après cet inventaire de définitions, nous explicitons dans la seconde section les principales propriétés des dessins d'enfants, qui peuvent être vus de nombreuses manières. Évitant le langage des catégories (avec objets et flèches) nous donnons des présentations équivalentes, se correspondant bijectivement, en commençant par les définitions combinatoires (variations sur le thème du graphe) et en continuant avec les définitions géométriques (en terme de revêtements). Nous ferons attention à préciser le vocabulaire, car il n'existe pas de terminologie officielle et chaque auteur adapte le principe des dessins d'enfants aux buts de son étude.

La troisième section s'intéresse au corps des modules d'un dessin, dont le degré est une bonne estimation de la difficulté de calcul de la correspondance de Grothendieck. L'étude des morphismes de dessins permet de parfois se ramener à un dessin plus simple. L'étude de l'action de Galois et l'énumération des dessins ayant même liste de valence permet d'avoir une borne a priori sur le nombre de conjugués galoisiens.

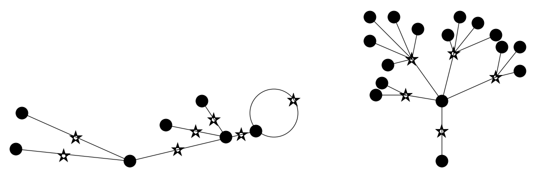
Nous présentons rapidement la théorie de la rigidité, qui permet de réduire certaines instances du problème de Galois inverse sur $\mathbb{Q}(T)$ au calcul explicite de la correspondance de Grothendieck. Plus généralement, l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur l'ensemble des dessins peut donner des indices sur la structure de ce groupe assez mystérieux.

II.1 Introduction aux dessins

II.1.1 Présentation informelle

a. Dessins dans le plan

Dans le plan ($\mathbb{R}^2$ ou $\mathbb{C}$) nous plaçons un nombre fini de points de deux types, et nous traçons de lignes (ne se croisant pas) reliant deux points de types différents. Ceci est un dessin marqué de genre 0, représenté par une carte plane bipartite. Par exemple le *bonhomme* et la *fleur de Leila* ci-dessous.



Si nous déformons ce dessin dans le plan, sa structure combinatoire est conservée. De cette description combinatoire, on peut déduire une description algébrique. C'est la correspondance de Grothendieck.

Il n'y a qu'une façon (à similitude directe près, ou échange des types des sommets) de tracer ce dessin dans le plan, qui corresponde à cette description algébrique. Grâce à des petits dessins, nous avons une façon élémentaire de représenter des objets algébriques qui peuvent être très complexes.

b. Préimage de $[0,1]$ par une fonction méromorphe

La préimage d'un segment par une fonction méromorphe β est la réunion de plusieurs segments. On appelle **valeurs critiques** de β les images des racines de β'. La préimage d'un segment par β ne peut avoir de points multiples qu'en une racine de β'.

Si nous choisissons une fonction méromorphe sur une surface compacte, par exemple la sphère $\mathbb{C} \cup \{\infty\}$, la préimage d'un point est un ensemble fini. Si de plus β n'a que deux valeurs critiques, 0 et 1 par exemple, l'image réciproque du segment réel $[0,1] \subset \mathbb{R} \subset \mathbb{C}$ trace un graphe connexe dans le plan. C'est un dessin au sens ci-dessus, dont les deux types de sommets correspondent aux préimages de 0 et 1.

c. Sur une surface compacte

Il est plus canonique de considérer qu'un dessin plan est dessiné sur la sphère $\mathbb{C} \cup \{\infty\}$ et non sur le plan. Le choix de la position ∞ sur la sphère est un marquage du dessin. C'est pour cela que nous avons défini un dessin plan comme *dessin marqué de genre 0.*

Si la surface n'est pas une sphère, mais une autre surface de Riemann compacte (de genre g) nous avons des dessins de genre g. C'est le cadre le plus général pour étudier la correspondance de Grothendieck.

II.1.2 Structures mathématiques

a. Combinatoire des graphes

La représentation visuelle d'un dessin est un graphe (non orienté), c'est-à-dire un ensemble de points qu'on relie par des traits. Nous définissons ceci plus rigoureusement :

On appelle **multi-ensemble** un ensemble fini dont les éléments peuvent être répétés plusieurs fois. Plus formellement, les multi-parties de cardinal $k > 0$ sont des k-uplets, modulo une permutation, et les multi-parties non vides de S sont les éléments de $\mathcal{MP}^*(S) = \cup_{k>0}(S^k/\mathfrak{S}_k)$.

On appelle **hypergraphe** un couple (S, A) où S est un ensemble fini de sommets et A est une multi-partie de $\mathcal{MP}^*(S)$, les arêtes. Deux sommets membres d'une même arête sont **reliés** par celle-ci. Si un sommet apparaît plusieurs fois dans une même arête, on parle d'incidence multiple. Si une même arête apparaît plusieurs fois dans A, il s'agit d'une arête multiple. La valence d'une arête est son cardinal, la valence d'un sommet est le nombre de fois que celui-ci apparaît dans les arêtes de l'hypergraphe. On appelle **graphe** un hypergraphe dont les arêtes sont de valence 2. Une boucle est une arête dont les deux éléments sont le même sommet. On parle de graphe simple s'il n'y a ni boucles ni arêtes multiples : A est alors un ensemble de paires de S.

Un graphe ou un hypergraphe est **connexe** si tout couple de sommets est relié par un chemin, c'est-à-dire une suite d'arêtes ayant un sommet commun. Un graphe se représente visuellement par un ensemble de points (A), reliés par des traits (S). On parle de graphe planaire si celui-ci peut être dessiné dans le plan sans que deux arêtes se croisent. Dès qu'on considère le plongement (c'est-à-dire le tracé des sommets, reliés par des arêtes ne se croisant pas) d'un graphe dans une surface, on parle de graphe plan ou de **carte**.

Sur la figure II.1, ni le deuxième, ni le troisième graphe n'est plan, mais le deuxième est planaire. Le quatrième graphe n'est pas simple, le cinquième n'est pas connexe.

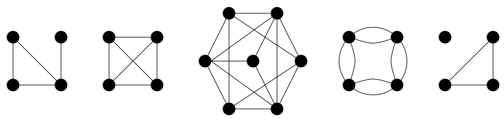


FIG. II.1 – *Exemples de graphes.*

b. Cartes d'une surface

Si nous dessinons un graphe sur une surface, cela nous donne un découpage de la surface suivant les arêtes du graphe. Si les morceaux ont tous la forme approximative d'un disque, on parle de carte cellulaire. Plus rigoureusement :

Soit X une surface (réelle) compacte et connexe orientable. Une **cellule** est un ouvert de X homéomorphe au disque ouvert (de $\mathbb{R}^2$). Un **segment** est un ouvert de X homéomorphe au segment ouvert (de $\mathbb{R}$).

On appelle graphe cellulaire sur X ou **carte** un triplet (S, K, X) tel que $S \subset K \subset X$ vérifient :

- S contient un nombre fini de points (les sommets du graphe)
- $K - S$ est l'union disjointe d'un nombre fini de segments (les arêtes).
- $X - K$ est l'union disjointe d'un nombre fini de cellules.

Deux sommets, arêtes ou cellules sont **adjacents** si l'un est dans l'adhérence de l'autre. Deux sommets ou deux faces sont adjacents s'ils sont adjacents à une même arête. Nous utiliserons le même terme, alors qu'on fait parfois la différence entre adjacence et incidence.

On définit le graphe sous-jacent comme suit : ses sommets sont les éléments de S, ses arêtes sont les paires de sommets adjacents. C'est un graphe connexe. Son graphe dual est celui-ci : ses sommets sont les cellules de la carte, ses arêtes sont les paires de cellules adjacentes.

On peut construire une **carte duale** en choisissant un point dans chaque cellule, ce qui donne l'ensemble fini S^*. On trace un arc entre deux points correspondant à des cellules adjacentes, ce qui donne K^* et une décomposition cellulaire $S^* \subset K^* \subset X$.

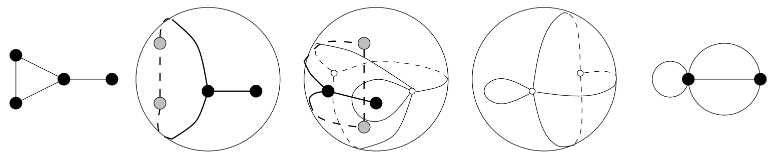


FIG. II.2 – *Carte et carte duale (sur la sphère, et représentation plane).*

Deux cartes sont homéomorphes s'il existe un homéomorphisme de X vers X' induisant des homéomorphismes de K vers K' et de S vers S'. Deux cartes isomorphes réalisent le même graphe.

Si les cellules sont des triangles (chaque cellule est adjacente à exactement trois sommets distincts, donc à trois arêtes) on dit que la carte est une **triangulation**.

Les cartes d'une surface sont des exemples très simples de CW-complexes finis.

c. Hypercartes

Sur une surface compacte connexe orientable X, on définit une hypercarte, ou hypergraphe cellulaire. C'est une carte où les cellules sont de trois types, que nous appelons hyper-sommets, hyper-arêtes et hyper-faces et où chaque sommet est adjacent à trois cellules, une de chaque type.

Les cellules adjacentes à une cellule donnée sont alors de deux types distincts, en alternance. Une cellule est donc délimitée par $2k$ arêtes, k est sa valence.

L'hypergraphe sous-jacent est défini comme suit : ses sommets sont les hyper-sommets, ses multi-arêtes sont les ensembles d'hyper-sommets ayant une hyper-arête adjacente en commun. L'hypercarte duale est celle où on échange le rôle des hyper-sommets et des hyper-faces.

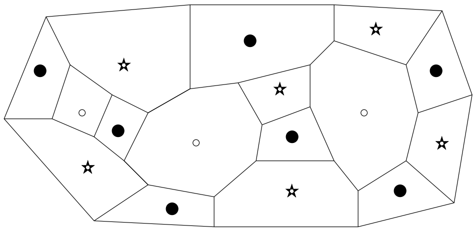


FIG. II.3 – *Hypercarte.*

d. Combinatoire des groupes

Lorsque nous définirons la monodromie, et pour toutes les allusions à la théorie de Galois, nous manipulons des groupes, la plupart du temps de cardinal fini ou opérant sur un emsemble. Il faut donc rappeler les définitions. À la fin de ce chapitre, nous utiliserons les notions plus compliquées de classes de conjugaison et de caractères irréductibles, nous profitons de ce paragraphe pour les définir et donner quelques propriétés.

Nous notons $|G|$ le cardinal d'un groupe fini G, qu'on appelle **ordre** du groupe. Le **centre** d'un groupe est l'ensemble $\mathcal{Z}(G)$ des éléments qui commutent avec tout le groupe, c'est un sous-groupe.

Si H est un sous-groupe de G, nous notons $H\backslash G = \{gH | g \in G\}$ l'ensemble des **translatés** (classes à gauche ou *cosets*) de H. On dit que H est **d'indice fini** si cet ensemble est fini.

On définit deux sous-groupes : le **normalisateur** de H dans G, qui contient les éléments $g \in G$ tels que $gH = Hg$, et le **centralisateur** qui réunit les éléments de G commutant avec tous les éléments de H.

Deux éléments h et h' de G sont **conjugués** s'il existe $g \in G$ tel que $h' = g^{-1}hg$, ce qu'on écrit $h' = h^g$. C'est une relation d'équivalence entre les éléments de G, l'ensemble des classes de conjugaisons est noté $\mathrm{C}\ell(G)$.

Rappelons qu'un groupe G opère sur un ensemble E s'il existe une action de $G \times E$ dans E telle que $(gh).x = g.(h.x)$ et $1.x = x$. Le **stabilisateur** d'un élément $x \in E$ est le sous-groupe H de G défini par $H = \{g \in G | g.x = x\}$. L'**orbite** d'un élément $x \in E$ est l'ensemble $\{g.x, g \in G\}$ des images de x par le groupe. Un groupe agit **transitivement** si l'image par le groupe de tout $x \in E$ est l'ensemble E en entier. Un groupe agit **fidèlement** si aucun élément non trivial de ce groupe n'agit trivialement sur E.

Le groupe $Inn(G)$ des automorphismes intérieurs de G (qui sont $h \mapsto h^g$) opère donc par conjugaison sur G. Pour tout sous-groupe H, le groupe G opère transitivement (par translation, $g.(hH) = (gh)H$) sur les $H\backslash G$.

On appelle **groupe de permutations** un sous-groupe de $\mathfrak{S}_n$. C'est donc un groupe opérant sur $\{1, ..., n\}$. La conjugaison dans un groupe de permutations correspond à une renumérotation de l'ensemble $\{1, ..., n\}$. Nous choisissons de noter les permutations par leur décomposition en cycles, en les faisant agir à droite. Ainsi le produit de $(1,2)$ et de $(2,3)$ est $(1,2)(2,3)=(1,3,2)$.

Si G est un groupe, $\mathbb{K}$ un corps et V un espace vectoriel de dimension finie sur $\mathbb{K}$, on appelle **représentation linéaire** une application $\rho : G \to GL(V)$ qui est un homomorphisme vers le groupe des *automorphismes* de V. Une représentation est irréductible s'il n'y a pas de sous-espace vectoriel propre de V qui soit stable par l'image de G. Toute représentation se décompose en somme directe de représentations irréductibles. On appelle caractère l'application χ de G dans $\mathbb{K}$ telle que $g \mapsto Tr(\rho(g))$ où Tr est la trace des endomorphismes linéaires. Un **caractère irréductible** est le caractère d'une représentation irréductible. On s'intéresse au cas où $\mathbb{K}=\mathbb{C}$.

Les caractères sont constants sur chaque classe de conjugaison. Il y a autant de caractères irréductibles que de classes de conjugaisons. De même que nous avons noté $C\ell(G)$ l'ensemble de ses classes de conjugaison, nous notons $X(G)$ l'ensemble des caractères irréductibles. Au paragraphe II.3.4.c. et pour tester la rigidité, nous aurons à calculer les valeurs des caractères irréductibles. Il suffit pour cela de regarder dans une table comme dans l'Atlas des groupes finis ([13], pour les groupes simples) ou d'utiliser un logiciel gratuit et efficace, tel GAP.

L'image de G par ses caractères irréductibles est dans un corps de nombres $\mathbb{K}$. Cela nous permettra au paragraphe II.3.5.e. de parler de $\mathbb{K}$-rationalité d'une classe de conjugaison. Nous appelons **exposant** du groupe fini G le plus petit commun multiple des ordres de ses éléments, que nous allons noter ici N, c'est un diviseur de l'ordre du groupe. L'image de G par $X(G)$ est dans le corps cyclotomique $\mathbb{Q}(\zeta_N)$ où ζ_N est une racine primitive N-ième de l'unité. Le groupe de Galois de $\mathbb{Q}(\zeta_N)$ sur $\mathbb{Q}$ est isomorphe au groupe $(\mathbb{Z}/N\mathbb{Z})^\times$. Il agit sur $C\ell(G)$ et sur $X(G)$ comme suit : $n \in (\mathbb{Z}/N\mathbb{Z})^\times$ envoie $c \in C\ell(G)$ sur c^n, ensemble des puissances n-ièmes des éléments de c, et $\sigma_n \in Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ envoie $\chi \in X(G)$ sur $g \mapsto \chi(g^n)$. On note c^* la réunion des c^n.

e. Variété analytique

L'autre aspect des dessins d'enfants se décrit à l'aide de revêtements. On parle ainsi de revêtement de surfaces de Riemann ou de revêtement de courbes algébriques. Nous allons donc définir une notion analytique de variété, différente de la notion de variété algébrique qu'on a vu au paragraphe I.1.4.b..

Une **variété analytique** (ou différentielle,† ou topologique ; les variétés utilisées pour les dessins d'enfants peuvent être munies de toutes ces structures) de dimension m est un espace localement isomorphe à $\mathbb{R}^m$, c'est-à-dire muni d'un atlas. Cela signifie qu'en tout point de la variété on peut définir une carte qui est ici un isomorphisme entre un voisinage de ce point et un ouvert de $\mathbb{R}^m$, et que les cartes sont compatibles (analytiquement, différentiellement ou topologiquement) sur l'intersection des voisinages correspondants. Une variété est ainsi munie d'une topologie qui permet de considérer sa connexité et sa compacité. Elle est orientable si les cartes peuvent être orientées de façon compatible.

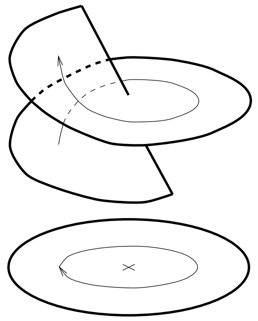
Si nous choisissons deux points b et c quelconques dans une variété X, un **chemin** de b à c est une application continue l de $[0,1]$ dans X tel que $l(0)=b$ et $l(1)=c$. Deux chemins l_0 et l_1 sont homotopes s'il existe φ de $[0,1]\times[0,1]$

† Une référence pour ce qui concerne les variétés différentielles et leurs avatars est les *Éléments d'analyse* de Dieudonné [18].

dans X, continue et telle que $\varphi(\bullet, 0) = l_0(\bullet)$, $\varphi(\bullet, 1) = l_1(\bullet)$ et $\forall x$, $\varphi(0, x) = b$ et $\varphi(1, x) = c$. C'est une déformation continue de chemins. Un chemin de b à b est appelé **lacet** de point base b.

Les classes d'équivalence de lacets homotopes sur une variété connexe sont naturellement munies d'une structure de groupe, c'est le **groupe fondamental** de la variété, qu'on note π_1. Si tous les lacets d'une variété sont homotopes, elle est simplement connexe.

On peut remarquer que le groupe fondamental de la sphère S moins n points est le groupe libre engendré par $n-1$ boucles autour de tous ces points sauf un (la boucle autour du dernier point ôté est la composition des autres). Les classes d'homotopie de lacets correspondent en effet au nombre de tours autour des trous.



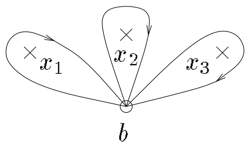


FIG. II.4 – *Relèvement d'un lacet autour d'une valeur de ramification. Générateurs du π_1 de $S - \{x_1, x_2, x_3\}$.*

f. Revêtement

Soient deux variétés X et Y. Un **revêtement** (analytique, différentiel, ou topologique) est une application surjective ϕ de Y dans X, telle tout point de X admette un voisinage V dont la préimage est isomorphe à $F \times V$ où F est un ensemble discret.† On appelle **fibre** la préimage d'un point. Le cardinal de F est constant sur chaque composante connexe de X. Si X est connexe, c'est le **degré** du revêtement. Un revêtement fini est un revêtement de degré fini.

Le **revêtement universel** d'une variété connexe est un revêtement connexe et simplement connexe, qui est unique à isomorphisme près.

Une surface est une variété analytique de dimension 2. Les courbes projectives lisses définies sur $\mathbb{C}$ peuvent être munies d'une structure de surface orientable. En particulier, $\mathbb{P}_1\mathbb{C}$ est une sphère. Un morphisme de courbes algébriques irréductibles $\phi : Y \to X$ est aussi appelé **revêtement algébrique**. C'est un revêtement **ramifié** de surfaces, ce qui siginifie qu'il existe un sous-ensemble discret $R \subset X$ tel que la restriction de ϕ à $\phi^{-1}(X - R)$ est un revêtement analytique. Les points de R sont appelés valeurs de ramification ou **valeurs critiques** et $\phi^{-1}(R)$ est l'ensemble des points de ramification.

† Plus précisément: il existe une bijection analytique (ou différentielle...) ψ entre $F \times V$ et $\phi^{-1}(V)$ telle que $\psi \circ \phi$ soit une projection de $F \times V$ dans F.

g. Relèvement et monodromie

Si nous avons un revêtement (non ramifié) $\phi : Y \to X$ et un chemin l de b à c dans X et si on choisit un point de la fibre au dessus de b, on appelle **relèvement** l'unique chemin de Y partant de ce point et ayant pour image l par ϕ. Le point final du relèvement de l est donc dans la fibre au dessus de c.

Le théorème de monodromie affirme que ce point ne dépend que de la classe d'homotopie de l. Cela signifie que les relèvements de deux chemins homotopes aboutissent au même point.

le groupe fondamental de X agit donc en permutant la fibre du point base. Le groupe de permutations ainsi engendré est appelé **monodromie**. Il est transitif si, et seulement si, Y est connexe.

h. La sphère et la droite projective

Les dessins d'enfants peuvent être vus comme des revêtements de la sphère $\mathbb{P}_1\mathbb{C}$. Nous allons étudier un peu plus en détail les propriétés de la droite projective.

Par définition, les éléments de $\mathbb{P}_1\mathbb{K}$ sont les droites de $\mathbb{K}^2$ passant par l'origine (cf. § I.1.4.a.). Ce sont donc les couples $(x : y)$ où $(kx : ky) = (x : y)$ pour $k \in \mathbb{K}^\times$. Pour tout corps, $\mathbb{P}_1\mathbb{K}$ contient au moins les trois points $(0 : 1)$, $(1 : 1)$ et $(1 : 0)$.

Les endomorphismes de $\mathbb{P}_1\mathbb{K}$ sont les homographies $(x : y) \mapsto (ax+b : cy+d)$ où $ad - bc \neq 0$. Les homographies sont en bijection avec les triplets de points distincts de $\mathbb{P}_1\mathbb{K}$, par exemple les images de $(0 : 1)$, $(1 : 1)$ et $(1 : 0)$ par l'homographie.

Si nous identifions $\mathbb{P}_1\mathbb{K}$ à $\mathbb{K}\cup\{\infty\}$, avec $(x : y) \mapsto x/y$ si $y \neq 0$ et $(x : 0) \mapsto \infty$, les trois points précédemment cités sont 0, 1 et ∞. Une homographie est alors l'application $x \mapsto (ax+b)/(cx+d)$. Lorsqu'on fixe $\infty \mapsto \infty$, ce sont les similitudes directes $x \mapsto ax + b$.

Il existe six homographies particulières, qui correspondent aux permutations de l'ensemble $\{0, 1, \infty\}$. Ce sont x, $1/(1-x)$, $(x-1)/x$, $x/(x-1)$, $1/x$ et $1-x$.

II.2 Double visage combinatoire – géométrie

II.2.1 Aspect combinatoire

Nous donnons sept présentations équivalentes des dessins d'enfants, qu'il est utile de combiner pour en percevoir les applications. L'équivalence entre ces descriptions est classique et date de bien avant l'étude des dessins d'enfants. Nous n'en ferons donc pas des démonstrations complètes.

a. Topologie

Présentation 1 (Carte bipartite) *Une carte (S, K, X) est bipartite si elle est munie d'une application $S \to \{\bullet, \bigstar\}$ donnant un type aux sommets, telle que chaque arête soit adjacente à deux sommets de types différents.*

La catégorie $\mathcal{P}_1$ a pour objets les cartes bipartites sur une surface orientable et les morphismes sont les homéomorphismes conservant le type des sommets.

Ceci est la définition la plus visuelle, celle qui permet de tracer effectivement des dessins au sens commun du terme. Pour encore plus de simplicité, nous pouvons oublier le type des sommets d'un dessin et obtenir un dessin propre (cf. § II.2.2.b.).

Présentation 2 (Triangulations bicolorées) *Une triangulation* (S, K, X) *est bicolorée si ses cellules (triangles) sont de deux couleurs déterminés par* $X - K \to \{\pm 1\}$ *telle que deux triangles adjacents sont de couleurs différentes.*

Nous pouvons remarquer que si une surface compacte X est munie d'une triangulation bicolorée, elle est orientable. On aborde parfois le sujet des dessins d'enfants par l'étude des triangulations [3].

Présentation 3 (Triangulations tripartites) *Une triangulation* (S, K, X) *est tripartite si elle est munie d'une application* $S \to \{\bullet, \bigstar, \circ\}$ *donnant un type aux sommets, telle que chaque arête soit adjacente à deux sommets de types différents.*

Ces deux dernières présentations sont équivalentes. Si nous avons une triangulation tripartite, chaque cellule a trois sommets de types distincts. Pour chacune, l'ordre des sommets $\bullet, \bigstar, \circ$ donne une orientation. Lorsque nous avons choisi une orientation sur X, cela nous donne une bicoloration des cellules.

Réciproquement, soit une triangulation bicolorée. Nous choisissons un sommet $a \in S$ qui sera de type $\bullet$ et un sommet b adjacent à a qui sera de type $\bigstar$. Ceci permet de construire de proche en proche un partition des sommets telle que les trois sommets d'un triangle soient de types différents. À cause de la bicoloration, le nombre de triangles adjacents à un sommet donné est pair, cette construction est donc cohérente.

Nous pouvons construire une correspondance entre la présentation $\mathcal{P}_3$ des dessins sous la forme de triangulations tripartites et la présentation $\mathcal{P}_1$ sous la forme de cartes bipartites. Prenons une triangulation tripartite (S, K, X). Soit S' l'ensemble des sommets de type $\bullet$ ou $\bigstar$, et soit K' la réunion des sommets de S' et des arêtes reliant deux sommets de S'. Alors (S', K', X) est une carte bipartite. Il y a un point $\circ$ dans chaque cellule, et cette cellule est la réunion des triangles touchant ce point.

Présentation 4 (Hypercartes) *Un dessin est aussi une classe d'homéomorphisme d'hypercartes sur une surface connexe compacte orientable.*

Cette présentation est équivalente aux précédentes. En effet, si (S, K, X) est la carte délimitant les cellules (de trois types) d'une hypercarte $\mathcal{P}_4$, sa carte duale est une triangulation tripartite $\mathcal{P}_3$.

b. Choix de terminologie

À cause des propriétés géométriques et algébriques (voir $\mathcal{P}_8$), nous appellerons **zéro** les points de type $\bullet$ et **un** ceux de type $\bigstar$. Nous appellerons **face** les cellules, ou bien les points $\circ$. La description $\mathcal{P}_3$ sous la forme de triangulations tripartites montre qu'il est facile de permuter les rôles de ces trois types de points.

Nous appellerons **flèche** un segment reliant un $\bullet$ et un $\bigstar$ (selon $\mathcal{P}_1$), ou bien le triangle positif contigu (selon $\mathcal{P}_2$) ou le sommet positif correspondant (selon

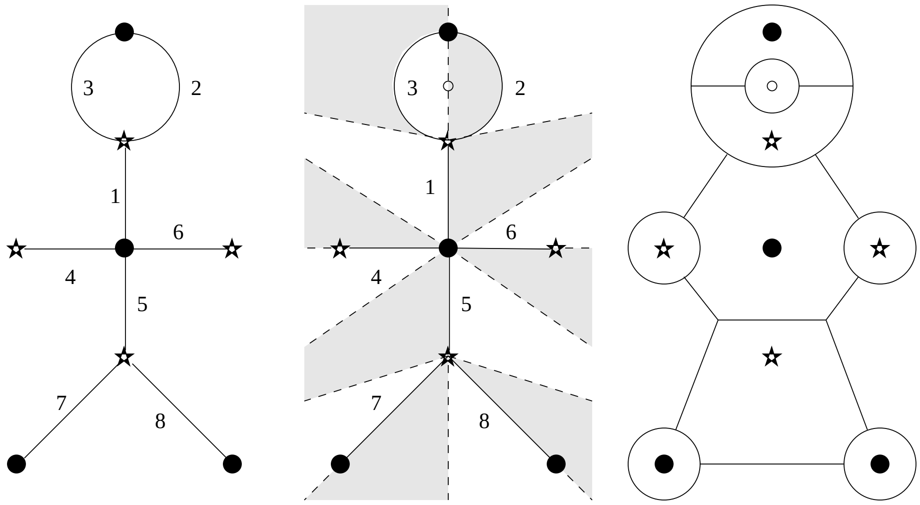


FIG. II.5 – *Le "petit bonhomme" : carte bipartite, triangulation et hypercarte (les* flèches *sont numérotées de 1 à 8).*

$\mathcal{P}_4$). † Nous appellerons **triangle** chaque cellule de la triangulation (selon $\mathcal{P}_2$ ou $\mathcal{P}_3$). Les triangles positifs correspondent aux demi-segments de $\bullet$ vers $\bigstar$ et les triangles négatifs aux demi-segments de $\bigstar$ vers $\bullet$. ‡ Nous appellerons **fléchette** les six types de demi-segments, $\bullet - \bigstar$, $\bigstar - \bullet$, $\bullet - \circ$, $\circ - \bullet$, $\bigstar - \circ$ ou $\circ - \bigstar$. ◇ Nous évitons ainsi le terme de *drapeau* qui sert à désigner parfois les flèches, parfois les triangles. Le **degré du dessin** est le nombre de flèches. C'est donc le nombre d'arêtes de la carte bipartite (catégorie $\mathcal{P}_1$) ou bien le nombre de triangles de chaque type ($\mathcal{P}_2$).

Si g est le genre de X, N le degré du dessin, a le nombre de zéros, b le nombre de uns et c le nombre de faces, la caractéristique d'Euler vaut :

$$\chi = 2 - 2g = a + b + c - N$$

c. Groupes

Étant donnée une triangulation tripartite sur une surface (non nécessairement orientée) X, nous définissons une action sur les triangles : $\rho_0, \rho_1, \rho_\infty$ associent respectivement à un triangle son symétrique par rapport aux côtés $\bigstar - \circ$, $\circ - \bullet$ et $\bullet - \bigstar$. Ce sont les générateurs du groupe hypercartographique $\mathcal{H}_2 = \langle \rho_0, \rho_1, \rho_\infty | \rho_0^2 = \rho_1^2 = \rho_\infty^2 = 1 \rangle$ (nous utilisons les notations de Jones et Singerman [26]).

† On trouve les noms de *drapeaux* (Couveignes [16, p27], Zapponi [48]), de *flags* (Couveignes et Granboulan [17, p80]), de *oriented flags* (Schneps [37, p51], Shabat et Voevodsky [43, p206]), de *darts* (Jones et Singerman [26, p116]) ou de *brins* (Bauer et Itzykson [3, p181], Cori [15, p12]).

‡ On trouve les noms de *repères*, *drapeaux* ou *biarcs* (Grothendieck [24]), de *flags* (Schneps [37, p51], Shabat et Voevodsky [43, p205], Jones et Singerman [26, p120]) ou de *blades* (Bryant et Singerman, 1985).

◇On trouve le nom de *standards* (Couveignes et Granboulan [17, p81]).

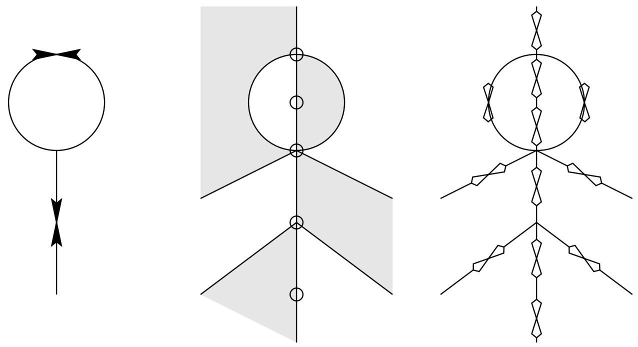


FIG. II.6 – *Flèches, triangles et fléchettes*

Étant donné un dessin (sur une surface orientée X) nous définissons aussi une action sur les flèches : en un sommet se rencontrent plusieurs flèches, qu'on ordonne selon l'orientation de la surface. Cette action associe à une flèche la suivante autour du sommet considéré. Par définition, $\sigma_0, \sigma_1, \sigma_\infty$ agissent respectivement par rotation autour des $\bullet$, $\bigstar$, $\circ$. Ils engendrent le groupe hypercartographique orienté $\mathcal{H}_2^+ = \langle \sigma_0, \sigma_1, \sigma_\infty | \sigma_0\sigma_1\sigma_\infty = 1\rangle$. On peut remarquer que $\mathcal{H}_2^+$ est le sous-groupe d'indice 2 de $\mathcal{H}_2$ engendré par $\sigma_0 = \rho_1\rho_\infty$, $\sigma_1 = \rho_\infty\rho_0$ et $\sigma_\infty = \rho_0\rho_1$. On peut aussi remarquer que $\mathcal{H}_2^+$ est isomorphe au groupe libre engendré par σ_0 et σ_1.

Présentation 5 (Sous-groupes d'indice fini) *Le dessins sont en correspondance avec les classes de conjugaison de sous-groupes d'indice fini du groupe hypercartographique* $\mathcal{H}_2^+$.

Le stabilisateur d'une flèche est un sous-groupe $\mathcal{B}$ d'indice fini de $\mathcal{H}_2^+$, l'action de ce groupe sur $\mathcal{B}$ et ses translatés est identique à l'action sur les flèches. Elle est identique pour tous les conjugués de $\mathcal{B}$.

En sens inverse, nous pouvons reconstruire un dessin comme Schneps [37, p53] par recollement des triangles d'une triangulation, ou bien comme Jones et Singerman [26, p124] par quotient d'une hypercarte universelle de type $[p, q, r]$.

On dit qu'une hypercarte (un dessin) est de type $[p, q, r]$ si ces nombres (qui peuvent prendre la valeur ∞) sont des multiples des valences des hyperfaces, hyper-arêtes et hyper-sommets. Les groupes triangulaires orientés, ou fuchsiens, agissent sur les flèches de tels dessins. On note ces groupes $\Delta_{(p,q,r)} = \langle \sigma_0, \sigma_1, \sigma_\infty | \sigma_0^p = \sigma_1^q = \sigma_\infty^r = \sigma_0\sigma_1\sigma_\infty = 1\rangle$.

Présentation 6 (Sous-groupes d'indice fini, bis) *Le dessins sont en correspondance avec les classes de conjugaison de sous-groupes d'indice fini d'un groupe triangulaire* $\Delta_{(p,q,r)}$ *où* p, q *et* r *sont finis.*

L'action de ce groupe sur les d flèches d'un dessin se traduit par une représentation du groupe dans le groupe de permutations $\mathfrak{S}_d$.

Présentation 7 (Triplets de permutations) *Un dessin est aussi un triplet de permutations* $(\sigma_0, \sigma_1, \sigma_\infty)$ *opérant transitivement sur un ensemble fini (de flèches), telles que* $\sigma_0\sigma_1\sigma_\infty = 1$*, défini à conjugaison près (renumérotation de l'ensemble des flèches).*

Les sommets $\bullet$ (resp. $\bigstar$ ou $\circ$) sont en correspondance avec les cycles (orbites) de σ_0 (resp. σ_1 ou σ_∞), la valence du sommet est égale à la longueur du cycle. Cette présentation des hypercartes comme triplet de permutations est très classique et les hypercartes sont parfois définies en tant que permutations [15].

À cause de la présentation $\mathcal{P}_8$ d'un dessin comme revêtement ramifié, nous appelons monodromie le triplet $(\sigma_0, \sigma_1, \sigma_\infty)$, qui correspond à l'action du π_1 sur le revêtement. La monodromie du dessin de la figure II.5 est par exemple :
$\sigma_\infty = (1, 2, 6, 5, 8, 7, 4)$
$\sigma_0 = (1, 4, 5, 6)(2, 3)$
$\sigma_1 = (1, 2, 3)(5, 7, 8)$

II.2.2 Variantes

a. Marquage

Si l'une des faces (cellules $\circ$) du dessin est distinguée des autres, il s'agit d'un **dessin marqué**. Ceux-ci ont des propriétés algébriques un peu plus simples qu'en l'absence de marquage. Ils interviennent lors de l'étude du groupe modulaire $\Gamma(1) = PSL_2(\mathbb{Z})$ et de son sous-groupe de congruence $\Gamma(2)$. Birch les appelle *drawings* [7].

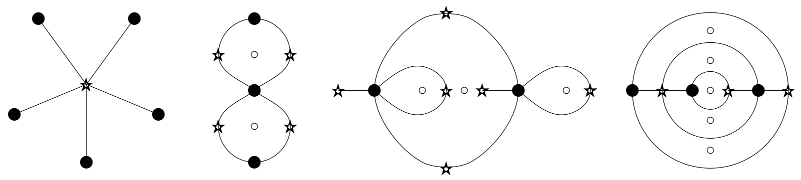


FIG. II.7 – *Exemples de dessins marqués de genre 0 (dans le plan).*

Si le dessin n'a qu'une face, celle-ci est donc naturellement marquée. En genre 0, le graphe correspondant n'a pas de cycle. On dit alors que le dessin est un **arbre**. Les arbres ont une importance particulière parmi les dessins d'enfants : leur étude est plus facile et peut suffire, par exemple lorsqu'on cherche à caractériser l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur les dessins.

b. Restrictions de valences

Si nous demandons à ce que les sommets $\bigstar$ aient une valence égale à 2, nous pouvons regrouper deux à deux les arêtes et le dessin est alors une carte de X, ayant pour sommets les $\bullet$ et ayant une $\bigstar$ sur chaque arête. Lorsqu'on trace ces dessins, on omet habituellement de placer les $\bigstar$ au milieu des arêtes. Nous les appelons les **dessins propres** (*clean*, ou *pure*). C'est ce que Shabat et Voevodsky ont appelé *dessin* [43].

Si nous acceptons des sommets $\bigstar$ de valence 1 ou 2, il s'agit d'un **dessin cartographique**.† Ils correspondent au groupe cartographique orienté $\mathcal{C}_2^+ = \Delta_{(\infty,2,\infty)}$.

Ces deux variantes sont les plus étudiées par les combinatoriciens.

† Ce sont les dessins *pre-clean* ou *pré-propres* selon la terminologie de Schneps [37] ou Zapponi [48].

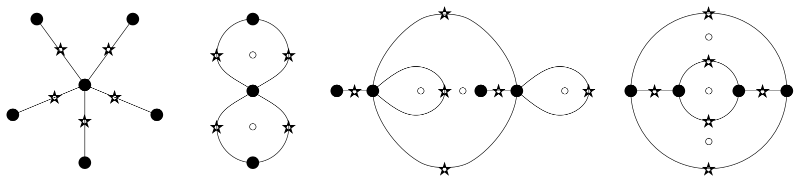


FIG. II.8 – *Exemples de dessins propres.*

Si les sommets • sont de valence 1 ou 3 et les sommets ★ de valence 1 ou 2, nous avons les **dessins triangulaires**. Ils correspondent au groupe triangulaire orienté $\mathcal{T}_2^+ = \Delta_{(\infty,2,3)}$.

Les dessins triangulaires marqués servent par exemple à l'étude du groupe modulaire $PSL_2(\mathbb{Z}) = \Gamma(1)$.

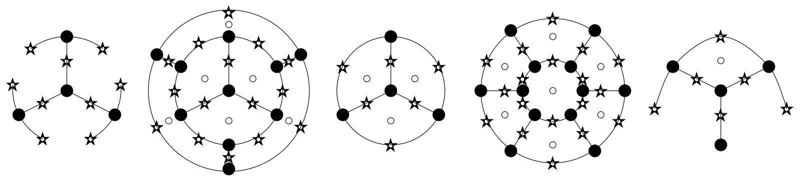


FIG. II.9 – *Exemples de dessins triangulaires.*

Si les sommets • sont tous de même valence p, les sommets ★ de même valence q et les cellules de même valence r, nous avons les **dessins semi-réguliers**. Les dessins galoisiens (c'est-à-dire les dessins dont le nombre des automorphismes est égal au degré, on les appelle aussi dessins réguliers) sont des dessins semi-réguliers, la réciproque est fausse en genre $\geqslant 1$.

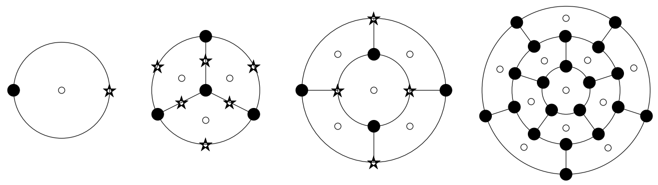


FIG. II.10 – *Exemples de dessins (semi-)réguliers de genre 0.*

c. Dessin sur une surface quelconque

Nous avons défini les dessins sur une surface X, compacte, connexe et orientable. La surface X peut être munie d'une structure de courbe algébrique (variété algébrique de dimension 1) ou de surface de Riemann (analytique de dimension 1 sur $\mathbb{C}$).

Si X est une surface connexe, éventuellement non orientable, éventuellement avec un bord. Il est encore possible d'y tracer un graphe cellulaire (bipartite), mais cette surface n'a pas la même richesse algébrique et analytique.

L'étude de cette généralisation des dessins d'enfants est faite par exemple par Jones et Singerman [26]. Elle ne présente que peu d'intérêt pour nous puisque ces dessins n'ont pas les propriétés algébriques permettant d'étudier l'aspect arithmétique d'un revêtement.

d. Sous-groupes du groupe modulaire

L'étude des sous-groupes du groupe modulaire et de leur action sur le plan hyperbolique est une façon de s'intéresser aux dessins d'enfants [2, 7].

On rappelle que le groupe modulaire

$$PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\} = \left\{ \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

agit sur le demi-plan hyperbolique sous la présentation

$$PSL_2(\mathbb{Z}) = \left\{ z \mapsto \frac{az+b}{cz+d} \middle| \, a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Parmi ses sous-groupes on distingue les sous-groupes de congruence, par exemple les $\Gamma(n)$ tels que $b \equiv c \equiv 0 \bmod n$.

Le groupe triangulaire orienté $\mathcal{T}_2^+$ peut être identifié au groupe $\Gamma(1) = PSL_2(\mathbb{Z})$ et le groupe hypercartographique orienté $\mathcal{H}_2^+$ au sous-groupe de congruence $\Gamma(2)$, mais il faut remarquer que l'injection canonique du sous-groupe des translations $\mathbb{Z} \hookrightarrow PSL_2(\mathbb{Z})$, avec $n \mapsto (z \mapsto z + n)$, définit un marquage du dessin correspondant. C'est pour cela que lorsqu'on aborde ainsi les dessins d'enfants, on considère les dessins marqués

II.2.3 Aspect géométrique

Nous avons donc défini les dessins d'enfants topologiquement comme un graphe à l'intérieur d'une surface X, sans en fixer la position dans cette surface. Il existe une définition équivalente, comme revêtement de $\mathbb{P}_1$ moins trois points, qui donne la "vraie" forme d'un dessin en imposant la forme de ce graphe.

a. Revêtement complexe ramifié

Présentation 8 (Revêtement) *On s'intéresse aux revêtements finis $\beta : X \to \mathbb{P}_1\mathbb{C}$ ramifiés au dessus de 0, 1 et ∞ seulement, à $\bar{\mathbb{Q}}$-isomorphisme près.*

Cette définition d'un dessin d'enfant est équivalente aux définitions topologiques. Ceci est la **Correspondance de Grothendieck**.

On fait se correspondre la monodromie du revêtement et la présentation du dessin comme triplet de permutations.

Un dessin d'enfant, au sens de $\mathcal{P}_5$, est en bijection avec les classes de conjugaison des sous-groupes d'indice fini de $\mathcal{H}_2^+$.

Or π_1, le groupe fondamental de $\mathbb{P}_1\mathbb{C} - \{0, 1, \infty\}$, engendré par les trois boucles autour de 0, 1 et ∞, est isomorphe au groupe $\mathcal{H}_2^+$.

Un théorème classique (par exemple [37, lemme I.1, p48]) prouve que les classes de conjugaison des sous-groupes d'indice fini de π_1 sont en bijection avec les revêtements finis de $\mathbb{P}_1\mathbb{C} - \{0, 1, \infty\}$. Si $\mathcal{B}$ est un sous-groupe d'indice fini de π_1 et si $\tilde{X}$ est le revêtement universel de $\mathbb{P}_1\mathbb{C} - \{0, 1, \infty\}$, alors le quotient $\mathcal{B}\backslash\tilde{X}$ définit un revêtement fini, et réciproquement $\mathcal{B}$ est le stabilisateur dans π_1 d'un point du revêtement.

b. Correspondance de Grothendieck d'un point de vue élémentaire

Visuellement, cette correspondance s'obtient comme suit : à partir d'un revêtement $\beta : X \to \mathbb{P}_1\mathbb{C}$, la préimage sur X de $[0,1] \subset \mathbb{P}_1\mathbb{C}$ trace un dessin. L'ensemble fini $\beta^{-1}(0)$ est l'ensemble des sommets $\bullet$, l'ensemble $\beta^{-1}(1)$ contient les $\bigstar$, et $\beta^{-1}(\infty)$ les $\circ$. Les flèches sont les composantes de $\beta^{-1}(]0,1[)$, qui relient les $\bullet$ et les $\bigstar$. De même, $\beta^{-1}(]1,\infty[)$ relie les $\bigstar$ et $\circ$ et $\beta^{-1}(]\infty,0[)$ relie les $\circ$ et $\bullet$. Nous avons ainsi une triangulation ($\mathcal{P}_2$ et$\mathcal{P}_3$) et les triangles de chaque type sont les préimages de chaque demi-sphère $\mathbb{P}_1\mathbb{C} - \mathbb{R}$.

Dans l'autre sens, on part d'une triangulation bicolorée et on construit l'application β en envoyant chaque triangle dans la demi-sphère $\mathbb{P}_1\mathbb{C} - \mathbb{R}$ correspondant au type du triangle. On utilise par exemple le théorème d'existence de Riemann pour relever une structure complexe.

L'application β est appelée **application de Belyi**. Toute fonction rationnelle sur X ayant au plus trois valeurs critiques est une application de Belyi. En effet, le choix du triplet $\{0,1,\infty\}$ n'est pas limitatif puisque tout triplet de points rationnels de $\mathbb{P}_1$ peut être envoyé par une homographie sur $\{0,1,\infty\}$. Parfois, on choisit $\{0,1728,\infty\}$, lorsqu'on étudie le groupe modulaire [2, 7].

c. Aspect arithmétique

La contribution de Belyi [5] est la suivante. On peut tracer un dessin d'enfant sur n'importe quelle courbe définie sur $\bar{\mathbb{Q}}$.

Théorème 1 (Belyi) *Soit X une courbe algébrique (projective, connexe et lisse) définie sur $\mathbb{C}$. Alors X est une courbe arithmétique si et seulement s'il existe un revêtement ramifié $\beta : X \to \mathbb{P}_1\mathbb{C}$ tel que ses valeurs critiques soient dans $\{0,1,\infty\}$. Le couple (X,β) est appelé* **paire de Belyi**.

Preuve : Le sens *si* est une conséquence (pas si évidente [47]) d'un critère de Weil. La preuve de l'autre sens, due à Belyi, se fait en construisant β à partir d'une fonction $\bar{\mathbb{Q}}$-rationnelle quelconque sur X.

On procède en deux étapes : on diminue le nombre de valeurs critiques non rationnelles, au prix d'une augmentation de la ramification au dessus de l'infini, puis on diminue le nombre de valeurs critiques finies, jusqu'à ce qu'il n'en reste que deux.

Une courbe arithmétique est par définition une courbe algébrique définie sur $\bar{\mathbb{Q}}$. Un élément ϕ de son corps des fonctions sur $\bar{\mathbb{Q}}$ définit un revêtement de $\mathbb{P}_1$ ramifié sur un sous-ensemble fini de $\mathbb{P}_1(\bar{\mathbb{Q}})$.

La première étape se fait en composant à gauche ϕ par une suite de polynômes diminuant le nombre de valeurs critiques non rationnelles. Soit C l'ensemble des valeurs critiques de ϕ non rationnelles et leurs conjuguées par $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. Soit h le polynôme à coefficients rationnels s'annulant sur C. Alors les valeurs critiques de $h \circ \phi$ sont 0, ∞ et les valeurs critiques de h, qui seront annulées par un polynôme de degré strictement inférieur à $d^o h$.

$$z \mapsto \frac{(m+n)^{m+n}}{m^m n^n} z^m (1-z)^n$$

La seconde étape se fait en composant à gauche par des polynômes de la forme ci-dessus, qui envoient les valeurs critiques $\{\infty, 0, 1, m/(m+n)\}$ en $\{\infty, 0, 1\}$, et réduisent donc le nombre de valeurs critiques rationnelles. □

Belyi a proposé une variante de cette seconde étape, où on compose par une unique fraction rationnelle, dont les points de ramification sont des entiers positifs, et dont les valeurs de ramification sont $\{0, 1, \infty\}$. De telles fractions rationnelles sont les fonctions de Belyi d'une famille de dessins d'enfants, pour lesquels il a donné une construction explicite (cf. § III.2.1.b.).

II.2.4 Généralisations

a. Revêtements de la sphère

Nous pouvons considérer les revêtements $\phi : X \to \mathbb{P}_1$ ramifiés au dessus de $k > 3$ points. Comme Adrianov et Shabat [1], nous pouvons appeler ϕ une **fonction de Fried** si $k = 4$, mais ce terme n'a pas la même audience que "fonction de Belyi". Contrairement au cas des fonctions de Belyi, la position relative dans $\mathbb{P}_1$ des 4 valeurs de ramification change les propriétés algébriques du dessin.

b. Graphes enrubannés

Partant d'une paire de Belyi (X, β), nous traçons sur X la préimage du cercle unité. Nous obtenons ainsi une carte sur X ayant un $\bullet$ ou un $\circ$ au centre de chaque face (les faces sont donc de deux couleurs) et dont les sommets sont des $\bigstar$ et sont de valence paire.

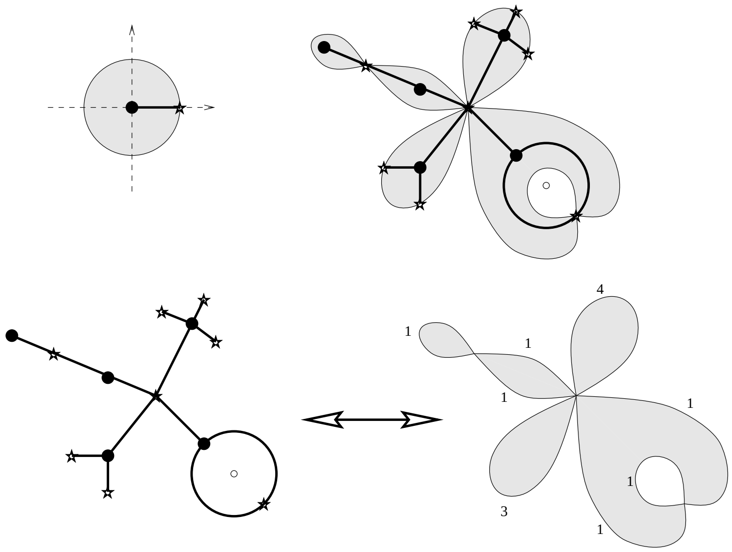


FIG. II.11 – *Dessins et graphes enrubannés.*

Selon la terminologie de [49], un **graphe enrubanné** est une carte dont tous les sommets ont pour valence au moins 3. Un graphe enrubanné est orientable s'il est possible de le munir d'une bicoloration des cellules. Les valences des sommets sont alors toutes paires. Si on ignore les $\bigstar$ de valence 2, la préimage du cercle unité est donc un graphe enrubanné orienté.

Pour avoir une bijection, nous devons associer à chaque arête du graphe enrubanné un entier positif, sa longueur, qui est est égale au nombre de ★ sur l'arête, plus un.

Les graphes enrubannés métriques sont les graphes enrubannés dont chaque arête est étiquetée par un réel positif, sa longueur. Ils forment donc une généralisation (topologique) des dessins d'enfants.

c. Différentielles de Strebel

Les différentielles de Strebel sont aux graphes enrubannés métriques ce que les applications de Belyi sont aux dessins d'enfants.

Une forme différentielle quadratique ω n'ayant que des pôles doubles est une **différentielle de Strebel** si on peut y associer † un graphe critique Γ qui délimite une décomposition cellulaire de la surface X.

Un théorème de Strebel [44] montre que pour tout n-uplet de points distincts $P_1, .., P_n$ étiquetés par des réels strictement positifs $p_1, ..., p_n$, il existe une et une seule différentielle de Strebel ayant $P_1, .., P_n$ comme pôles et $p_1, ..., p_n$ comme périmètre des faces correspondantes.

Si (X, β) est une paire de Belyi, nous voyons X comme une surface de Riemann et β comme une fonction méromorphe sur X. Nous pouvons construire la forme différentielle méromorphe $\vartheta_\beta = \frac{d\beta}{2\pi i\beta}$. Son carré

$$\omega_\beta = \left(\frac{d\beta}{2\pi i\beta}\right)^{\otimes 2}$$

est une différentielle de Strebel dont le graphe critique est aussi le graphe enrubanné préimage du cercle unité par β.

Le problème de la rationalité ou de l'algébraïcité des paramètres d'une différentielle de Strebel n'est pas facile.

II.3 Corps des modules

II.3.1 Action de Galois

a. Corps de définition

Soit $\mathbb{K}$ un corps de nombres. On dit qu'un dessin est défini sur $\mathbb{K}$ s'il peut être représenté par un couple (X, β) où β est une fonction de X définie sur $\mathbb{K}$. Pour un dessin marqué, nous demandons que la face marquée soit définie sur $\mathbb{K}$.

Remarquer que les automorphismes du dessin (s'il y en a) ne sont pas nécessairement définis sur $\mathbb{K}$. Par exemple $x \mapsto x^3$.

---

† Si $\mathbf{P}$ est l'ensemble des pôles de ω, il existe une métrique localement euclidienne définie par ω sur $X - \mathbf{P}$ dont nous regardons les géodésiques. Les *trajectoires horizontales* sont les géodésiques γ telles que $\omega(\gamma') \geqslant 0$. Celles qui passent par un zéro de ω sont les trajectoires critiques.

Pour un pôle $P \in \mathbf{P}$, le *disque maximal* $D(P)$ est la réunion de P et de toutes les trajectoires horizontales fermées autour de P. Si tous les pôles de ω sont doubles, on pose $\Gamma = X - \cup_{P\in\mathbf{P}} D(P)$. Si Γ est l'union des trajectoires critiques, et forme un CW-complexe de dimension 1 dans X, alors ω est une différentielle de Strebel.

Les $D(P)$ sont alors les faces d'une décomposition cellulaire et nous pouvons regarder leur périmètre (dans la métrique définie par ω).

b. Corps des modules

Le groupe $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ agit sur les dessins (revêtements). On peut voir cela comme son action sur les coefficients des équations de n'importe quelle paire de Belyi. On va appeler $\Gamma_{\mathcal{D}}$ le stabilisateur d'un dessin $\mathcal{D}$. Le corps $\mathbb{K}_{\mathcal{D}}$ des modules du dessin est le corps fixé par $\Gamma_{\mathcal{D}}$.

Coombes et Harbater [14] ont prouvé que le corps des modules est l'intersection de tous les corps de définition.

Couveignes [16] a montré qu'il existe des dessins pour lesquels le corps des modules n'est pas un corps de définition et qu'en genre 0, tout dessin admet un modèle sur une extension au plus quadratique de son corps des modules. En genre 0, le corps des modules est toujours corps de définition d'un dessin marqué.

c. Caractéristiques du corps des modules

Par définition, le degré du corps des modules est égal au nombre de dessins dans l'orbite sous l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. Son discriminant est nettement plus mystérieux, on se demande par exemple quels nombres premiers en sont des diviseurs.

Beckmann [4] a prouvé (dans un cadre plus général) que les facteurs premiers du discriminant sont des diviseurs de l'ordre du groupe de monodromie. La réciproque est bien évidemment fausse, mais on ne connait pas de caractérisation combinatoire qui réponde à cette question. †

d. L'action de Galois est fidèle

Le groupe $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ agit fidèlement sur les dessins. Cela signifie que pour tout élément $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, on peut construire un dessin sur lequel σ agit non trivialement. En d'autres termes, tout corps de nombres est le corps des modules d'un dessin.

Plus précisément, le groupe $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ agit fidèlement sur les dessins de genre 1. De plus, H.W. Lenstra a prouvé que l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ est fidèle sur les arbres (cf. [37, pp56-59]).

Cette propriété permet d'étudier $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ en étudiant les dessins d'enfants, en particulier les arbres. L'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur les dessins se compare à son action sur le corps des modules du dessin.

II.3.2 Invariants galoisiens

a. Orbites sous l'action de Galois

Pour l'étude de l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur les dessins, il est important de savoir déterminer si deux dessins sont conjugués. L'idéal serait de pouvoir n'utiliser que la définition combinatoire des dessins pour établir un critère décidant de l'appartenance ou non à la même orbite. On connait quelques invariants combinatoires pour séparer deux orbites, mais la seule méthode sûre est de calculer les fonctions de Belyi des dessins.

† Sauf quelques cas particuliers comme les arbres de diamètre 4.

b. Liste des valences

Nous allons introduire une notation pour la liste des valences d'un dessin, qui ressemble à la notation employée par Malle [29]. Si a_n (resp. b_n, c_n) est le nombre de zéros (resp. uns, faces) de valence n, le symbole

$$[n^{c_n}...2^{c_2}1^{c_1}; n^{a_n}...1^{a_1}; n^{b_n}...1^{b_1}]$$

représente l'ensemble des dessins ayant mêmes valences. Bien évidemment, on omettra les valences absentes et les exposants 1. Par exemple, le "petit bonhomme" de la figure II.5 a pour liste de valences $[7\,1; 4\,2\,1^2; 3^3\,1^2]$. Pour un dessin marqué, on placera en premier la face marquée.

L'action de Galois sur une fonction de Belyi ne modifie par la structure de la ramification. Deux dessins conjugués par l'action de Galois ont donc même liste de valences, mais la réciproque est fausse. La liste des valences est un invariant galoisien qui ne suffit pas à séparer les orbites.

On peut raffiner cet invariant en remarquant que si la monodromie d'un dessin est le triplet $(\sigma_0, \sigma_1, \sigma_\infty)$, alors l'action de Galois sur les dessins induit une action de $Inn(G)$ sur ces triplets.

c. Composition de dessins

Si un dessin est une composition de revêtements (voir II.3.3.b. pour plus de détails sur la composition de dessins), le groupe de Galois absolu agit sur chaque étage de la tour de revêtements. Nous avons ainsi un deuxième invariant galoisien. Par exemple, l'orbite galoisienne d'un dessin qui est un k-multiple ne contient donc que des k-multiples. L'invariant (ordre abélien) introduit par Pakovitch [36] est un autre cas particulier.

Ces deux critères combinatoires suffisent vraisemblablement à séparer les arbres en Y (cf. § IV.3.1).

d. Les fleurs de Leila

On connait des exemples, en particulier les "Fleurs de Leila", pour lesquels un critère supplémentaire est nécessaire. Cet invariant a été formalisé par Zapponi [49] d'après un travail expérimental de Kochetkov, et correspond à la signature d'une permutation.

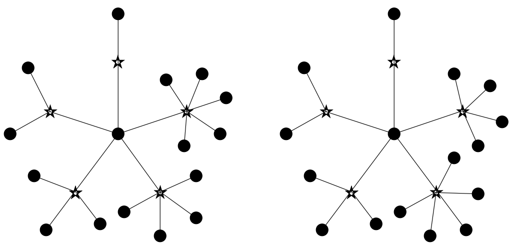


FIG. II.12 – *Fleurs de Leila*

II.3.3 Morphismes de dessins

a. Automorphismes d'un dessin

Certains dessins ont une certaine symétrie, qui correspond à un automorphisme du revêtement. Du point de vue de $\mathcal{P}_7$ un automorphisme du dessin est une permutation qui commute avec σ_0 et σ_1 (donc aussi avec σ_∞), c'est-à-dire un élément du centralisateur du groupe de monodromie dans $\mathfrak{S}_N$.

Si le dessin a des automorphismes, leur étude préalable simplifie beaucoup l'étude du dessin.

b. Composition de dessins

Nous cherchons à contruire un dessin à partir de dessins plus petits. Supposons que nous avons trois surfaces (ou courbes algébriques) X, Y et Z et deux revêtements ramifiés $\mathcal{D}_\beta : X \xrightarrow{\beta} Y$ et $\mathcal{D}_\lambda : Y \xrightarrow{\lambda} Z$. La composition $\mathcal{D}_\lambda \circ \mathcal{D}_\beta$ est le revêtement $X \xrightarrow{\lambda\circ\beta} Z$.

Lorsque ces trois revêtements sont des dessins d'enfants, nous parlons de "composition de dessins". C'est le cas si $Y = Z = \mathbb{P}_1$ et si $\lambda(\{0, 1, \infty\}) \subset \{0, 1, \infty\}$. Nous appelons **dessin gelé** un dessin de genre 0 (i.e. $\lambda : \mathbb{P}_1 \to \mathbb{P}_1$) dont nous avons fixé la fonction de belyi de telle sorte que les éléments $0, 1, \infty \in \mathbb{P}_1$ soient des points de type $\bullet$, $\bigstar$ ou $\circ$. Nous pouvons, sans perte de généralité, supposer que ∞ est une face, et nous représentons les dessins gelés en traçant un carré autour des valeurs 0 et 1. La figure II.13 donne deux exemples de composition par un dessin gelé.

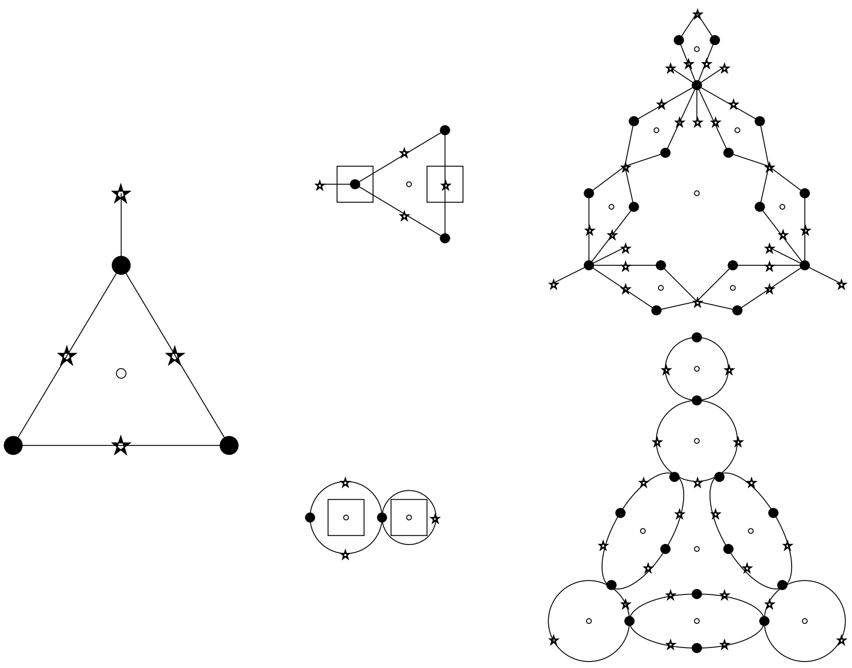


FIG. II.13 – *Exemples de composition de dessins*

On peut généraliser ceci au cas où $\mathcal{D}_\beta$ est un revêtement fini (mais pas un dessin) $X \to \mathbb{P}_1$ ramifié au dessus d'un ensemble R tel que $\lambda(R) \subset \{0, 1, \infty\}$. C'est ce qui est utilisé par Birch pour obtenir quelques exemples en genre 1 (cf. § III.2.1.a.).

c. Double, ou foncteur de Walsh

Nous avons défini $\mathcal{C}_2^+$ comme sous-groupe d'index 2 de $\mathcal{H}_2^+$, ce qui définit les dessins propres comme des cas particuliers de dessins d'enfants. On peut aussi regarder l'inclusion de $\mathcal{H}_2^+ = \Gamma(2)$ dans $\mathcal{C}_2^+ = \Gamma_0(2)$. Cela permet d'associer à tout dessin un dessin propre, que nous appelons son **double**.

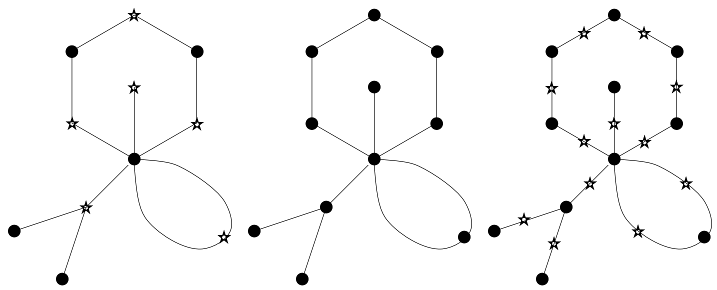


FIG. II.14 – *Doublement d'un dessin.*

Cette construction se fait en oubliant le type des sommets d'une carte bipartite, comme sur la figure II.14. C'est la composition par le dessin gelé de la figure ci-dessous, c'est à dire par la fonction $\lambda : \beta \mapsto 4\beta(1-\beta)$.

On voit donc que le calcul de la fonction de Belyi d'un dessin propre (de degré $2n$) qui est le double d'un autre dessin se réduit au calcul d'une fonction de Belyi de degré n. On verra (paragraphe III.1.2.d.) que le calcul d'une fonction de Belyi se simplifie aussi pour les dessins propres qui ne sont pas des doubles.

d. Autres foncteurs

L'inclusion de $\mathcal{C}_2^+ = \Gamma_0(2)$ dans $\mathcal{T}_2^+ = \Gamma(1)$ transforme un dessin propre en une triangulation à l'aide de $\lambda : \beta \mapsto 27\beta^2/(4-\beta)^3$. Tout ceci est développé en détail par Jones et Singerman [26, §7] ; c'est aussi un cas particulier de composition de dessins.

e. Autres multiples

Si on décompose chaque segment de la carte en k segments, on obtient un multiple du dessin. On peut remarquer que la factorisation de k permet de construire la k-multiplication comme une tour de revêtements.

Comme on le verra en IV.2.2, le polynôme λ_k pour le k-ième multiple est la composition $\Theta^{-1} \circ T_k \circ \Theta$ où T_k est le k-ième polynôme de Tchebitchev et $\Theta(x) = 1 - 2x$. Le triple est donc par exemple la composition par $\lambda : \beta \mapsto \beta(4\beta-3)^2$. Le quintuple est la composition par $\lambda : \beta \mapsto -\beta(16\beta^2 + 20\beta + 5)^2$.

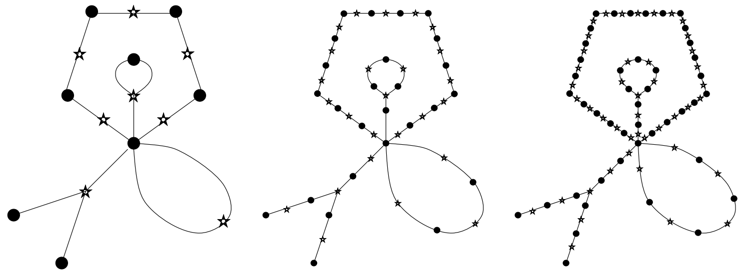


FIG. II.15 – *Dessin, triple et quintuple*

II.3.4 Énumération des dessins

a. Dessins réguliers et semi-réguliers

En genre 0, tous les dessins semi-réguliers sont galoisiens, et il est possible d'en donner la liste complète. Ce sont les dessins en étoile, de liste de valences $[n;\, n;\, 1^n]$, les cercles, de liste de valences $[n^2;\, 2^n;\, 2^n]$, et les solides réguliers : tétraèdre $[3^4;\, 3^4;\, 2^6]$, cube ou octaèdre $[4^6;\, 3^8;\, 2^{12}]$ et dodécaèdre ou icosaèdre $[5^{12};\, 3^{20};\, 2^{30}]$.

En genre 1, ce sont les quotients des réseaux réguliers carré ou triangulaire, sur les courbes $j = 0$ et $j = 1728$. En genre supérieur à 1, la formule de Riemann-Hurwitz donne une majoration de l'ordre du groupe de symétrie du dessin $(84(g-1))$; Adrinanov et Shabat [1] détaillent le sujet.

b. Arbres

Une formule d'énumération remontant apparemment à Tutte [46] s'applique aux dessins n'ayant qu'une face. On note $\hat{\#}[L]$ le nombre de dessins ayant pour liste de valence $[L]$, en comptant avec un poids $1/k$ les dessins ayant k automorphismes. Pour un arbre de liste de valences $[d; p_1^{a_1} \dots p_m^{a_m}; q_1^{b_1} \dots q_n^{b_n}]$,

$$\hat{\#}[L] = \frac{(a_1 + a_2 + \dots + a_m - 1)!}{a_1! a_2! \dots a_m!} \frac{(b_1 + b_2 + \dots + b_n - 1)!}{b_1! b_2! \dots b_n!}.$$

Cette formule donne facilement un majorant de la longueur de l'orbite du dessin sous l'action de Galois. Le paragraphe suivant donne une majoration plus précise.

c. Classes de conjugaison

À partir de la présentation $\mathcal{P}_7$ pour les dessins, nous posons $G \subset \mathfrak{S}_d$ le groupe egendré par $\langle \sigma_0, \sigma_1, \sigma_\infty \rangle$, qui est donc un groupe de permutations transitif sur d lettres. Nous nous intéressons aux classes de conjugaison c_i de $\sigma_0, \sigma_1, \sigma_\infty$ dans G.

Nous supposerons que ces classes de conjugaison sont rationnelles, c'est-à-dire que $c_i^* = c_i$, ce qui signifie que $\chi(c_i) \in \mathbb{Q}$. La longueur de l'orbite du dessin sous l'action de Galois est au plus le nombre $n_{\mathfrak{C}}$ ci-dessous, pour $k = 3$. Cette majoration est issue de la théorie de la rigidité et on la trouve chez Matzat [33] ou Serre [41, p68] (démontrée pour le cas où G n'a pas de centre). D'autres majorations, parfois plus fines, peuvent être construites de façon similaire.

$$n_{\mathfrak{C}} = |\mathcal{Z}(G)| \frac{1}{|G|^2} |c_1| \ldots |c_k| \sum_{\chi} \frac{\chi(c_1) \ldots \chi(c_k)}{\chi(1)^{k-2}}.$$

II.3.5 Rigidité

a. Motivation

La théorie de Galois, que nous avons évoquée au paragraphe I.1.2.c. pour les corps de nombres, se généralise aux extensions de corps de fonctions et aux revêtements algébriques. On cherche à résoudre le problème de Galois inverse sur $\mathbb{Q}$, c'est-à-dire qu'on veut prouver que tout groupe fini est groupe de Galois sur $\mathbb{Q}$. Ce problème est ouvert, mais il est possible d'en résoudre des cas particuliers en construisant des dessins d'enfants définis sur $\mathbb{Q}$ et de groupe de monodromie choisi. À partir de ce dessin, on calcule une extension (régulière) de $\mathbb{Q}(T)$ de même groupe de Galois, dont on déduit la propriété inverse de Galois sur $\mathbb{Q}$.

Nous aurons donc besoin de savoir, lorsque nous avons la description combinatoire d'un dessin, s'il est défini sur $\mathbb{Q}$. Une méthode est le calcul explicite de sa fonction de Belyi, mais il y a souvent plus rapide.

La borne sur la taille de l'orbite de Galois, donnée au paragraphe II.3.4.c., nous donne un critère de rationalité ($n_{\mathfrak{C}} = 1$), qui est un cas particulier du critère de rigidité donné par Serre [41] (voir le théorème 2 ci-dessous) qui est lui-même un cas particulier des critères plus généraux exposés par Matzat ([33], avec démonstrations dans son livre [32]) dont nous donnons un aperçu avec le théorème 3.

La rigidité, et la non rigidité, ont été un candidat pour une résolution générale du problème de Galois inverse sur $\mathbb{Q}$, et ces théories ont connu des nombreux développements. On peut notamment remarquer que si nous nous limitons dans cette thèse aux dessins d'enfants (et éventuellement aux revêtements de $\mathbb{P}_1$ ramifiés au dessus de $k > 3$ points), la théorie s'est étendue aux revêtements de surfaces (compactes orientées) de genre g ramifiés au dessus de k points et aux corps de fonctions à s variables.

b. Passage de $\mathbb{P}_1$ (revêtements) à $\mathbb{Q}$ (corps de nombres)

Une correspondance très riche entre revêtements et extensions donne la technique pour construire des extensions (régulières) de corps de fonctions de groupe de Galois fixé, à partir d'un revêtement dont on connait le groupe de Galois a priori.

Soit $\mathbb{L}$ une extension finie du corps $\mathbb{Q}(T)$ des fractions rationnelles sur $\mathbb{Q}$. On dit que cette extension est **régulière** si $\bar{\mathbb{Q}} \cap \mathbb{L} = \mathbb{Q}$, ce qui signifie que le produit tensoriel $\mathbb{L} \otimes \bar{\mathbb{Q}}$ est une extension finie de $\bar{\mathbb{Q}}(T)$ ayant la même structure. La régularité d'une extension permet d'avoir un parallèle entre l'aspect arithmétique (sur $\mathbb{Q}$) et l'aspect géométrique (sur $\bar{\mathbb{Q}}$ ou $\mathbb{C}$).

Si $\phi : X \to \mathbb{P}_1$ est un revêtement de courbes algébriques sur $\mathbb{Q}$, le corps $\mathbb{Q}(X)$ des fonctions rationnelles sur X est une extension régulière de $\mathbb{Q}(T)$. Réciproquement, si $\mathbb{L}$ est une extension finie régulière de $\mathbb{Q}(T)$, alors c'est le corps des fonctions d'une courbe projective lisse X. L'inclusion $\mathbb{Q}(T) \hookrightarrow \mathbb{L}$

définit un revêtement $X \to \mathbb{P}_1$. Si l'extension $\mathbb{L}/\mathbb{Q}(T)$ est galoisienne de groupe G, alors le revêtement correspondant est galoisien de groupe G.

Le **théorème d'irréducibilité** de Hilbert permet de transférer cette construction de $\mathbb{Q}(T)$ à $\mathbb{Q}$. En effet, si $f(T,X) \in \mathbb{Q}(T)[X]$ est un polynôme irréductible sur $\mathbb{Q}(T)$, il existe une infinité de spécialisations de la variable T, c'est-à-dire d'éléments $\tau \in \mathbb{Q}$ tels que le groupe de Galois de $f(\tau,X) \in \mathbb{Q}[X]$ sur $\mathbb{Q}$ soit égal au groupe de Galois de f sur $\mathbb{Q}(T)$.

c. Classification de Hurwitz

Nous posons $\bar{\Sigma} = \{(g_1,...,g_k) \in G^k \,|\, g_1...g_k = 1\}$ et Σ son sous-ensemble des k-uplets engendrant le groupe G.

Si nous fixons k places de $\mathbb{C}(T)$ (c'est-à-dire k valeurs de ramification dans $\mathbb{P}_1\mathbb{C}$) alors l'ensemble $\Sigma^a = \Sigma/\mathrm{Aut}(G)$ des orbites de Σ modulo les automorphismes de G classifie bijectivement les revêtements de $\mathbb{C}(T)$ de groupe de Galois G ramifiés au dessus de ces k points. C'est ce qu'on appelle la **classification de Hurwitz**.

Le problème de Galois sur $\mathbb{C}(T)$, et par la même sur $\bar{\mathbb{Q}}(T)$, est ainsi résolu puisqu'il existe des k-dessins de groupe G, pour tout groupe fini. Le problème de **rationalité** de ces k-dessins est la question de savoir s'ils sont définis sur $\mathbb{Q}$, ou de connaitre un corps de définition assez petit.

On considère k classes de conjugaisons $c_1,...,c_k$, non nécessairement distinctes. On note $\mathfrak{C} = \{(g_1,...,g_k) \in G^k \,|\, g_i \in c_i\}$ qu'on appelle une **structure de classes** de G et $\mathfrak{C}^* = \{(g_1,...,g_k) \in G^k \,|\, g_i \in c_i^*\}$ qu'on appelle une **structure de ramification**.

L'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur les revêtements conserve la structure de ramification. Nous pouvons donc étudier la restriction de la classification de Hurwitz à une certaine structure de ramification. Si cette restriction ne contient qu'un élément (modulo les automorphismes de G) alors l'orbite du revêtement sous $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ est réduite à un élément. C'est le critère de *rigidité*. La réciproque est fausse, et il existe d'autres critères (voir en particulier [33]).

d. Constantes de structure

On note comme Matzat $\mathfrak{C}^\circ$ qui vaut indifféremment $\mathfrak{C}$ ou $\mathfrak{C}^*$. Nous définissons les quatre ensembles $\bar{\Sigma}_{\mathfrak{C}^\circ} = \{(g_1,...,g_k) \in \mathfrak{C}^\circ \,|\, g_1...g_k = 1\}$ et $\Sigma_{\mathfrak{C}^\circ} = \{(g_1,...,g_k) \in \bar{\Sigma}_{\mathfrak{C}^\circ} \,|\, \langle g_1,...,g_k\rangle = G\}$. Sur ces ensembles opèrent les groupes $Inn(G)$ des automorphismes intérieurs de G et $Aut_{\mathfrak{C}^\circ}(G)$ des automorphismes conservant la structure de classes (ou de ramification).

Les objets qui nous intéressent sont les quotients $\Sigma^a_{\mathfrak{C}^\circ} = \Sigma_{\mathfrak{C}^\circ}/Aut_{\mathfrak{C}^\circ}(G)$ et $\Sigma^i_{\mathfrak{C}^\circ} = \Sigma_{\mathfrak{C}^\circ}/Inn(G)$. En particulier, $\Sigma^a_{\mathfrak{C}^*}$ énumère les revêtements ayant une structure de ramification donnée. Ces ensembles sont finis, et leurs cardinaux sont les nombres entiers $l^i_{\mathfrak{C}} = |\Sigma^i_{\mathfrak{C}}|$ et autres. Nous devons aussi définir le nombre $n_{\mathfrak{C}^\circ} = \bar{\Sigma}_{\mathfrak{C}^\circ}/Inn(G)$, qui est intervenu au paragraphe II.3.4.c. et que Matzat appelle **constante de structure normalisée**.

Ces entiers sont liés par les égalités $l^i_{\mathfrak{C}^*} = e_{\mathfrak{C}} l^i_{\mathfrak{C}}$ (l'entier $e_{\mathfrak{C}}$ est appelé indice cyclotomique) $l^i_{\mathfrak{C}^\circ} = a_{\mathfrak{C}^\circ} l^a_{\mathfrak{C}^\circ}$ (l'entier $a_{\mathfrak{C}^\circ}$ est égal au cardinal de $Out_{\mathfrak{C}^\circ}(G) = Aut_{\mathfrak{C}^\circ}(G)/Inn(G)$, ensemble des classes d'automorphismes extérieurs) et nous avons l'inégalité $l^i_{\mathfrak{C}^\circ} \leqslant n_{\mathfrak{C}^\circ}$ à cause de l'inclusion $\Sigma \subset \bar{\Sigma}$.

On voit donc que $n_{\mathfrak{C}^*} \geqslant l^i_{\mathfrak{C}^*} \geqslant l^a_{\mathfrak{C}^*}$ sont des majorants du nombre de conjugués galoisiens du dessin.

e. Rationalité et rigidité

Il n'est pas nécessaire de calculer toutes ces constantes. On dit qu'une classe $c \in C\ell(G)$ est $\mathbb{K}$-**rationnelle** si l'image de c par les caractères irréductibles $\chi \in X(G)$ est toujours dans $\mathbb{K}$. Il est équivalent de dire que $c^n = c$ pour tout $\sigma_n \in Gal(\mathbb{K}(\zeta_N)/\mathbb{K})$. En particulier, puisque $\mathbb{Q}^{ab}$ (on note ainsi l'extension abélienne maximale de $\mathbb{Q}$, parfois aussi notée $\mathbb{Q}^{cycl}$ car c'est l'extension cyclotomique maximale) contient tous les ζ_N, toute classe de conjugaison est $\mathbb{Q}^{ab}$-rationnelle. La $\mathbb{Q}$-rationalité de c est équivalente à l'égalité $c^* = c$.

On dit qu'un k-uplet $\mathfrak{C}$ de classes de conjugaisons est **rigide** si $l^i_{\mathfrak{C}} = 1$ et qu'il est strictement rigide si de plus $\Sigma_{\mathfrak{C}} = \bar{\Sigma}_{\mathfrak{C}}$. Dans le cas où G n'a pas de centre, la condition de rigidité devient $|\Sigma_{\mathfrak{C}}| = |G|$ (Serre [41, p70]).

Théorème 2 (D'après Serre) *Soit G un groupe fini de centre trivial. Si le k-uplet $(c_1, ..., c_k)$ de classes de conjugaisons de G est rigide et si toutes les c_i sont $\mathbb{K}$-rationnelles, alors il existe une extension régulière de $\mathbb{K}(T)$ de groupe de Galois G. Cette extension correspond à un revêtement de $\mathbb{P}_1$ défini sur $\mathbb{K}$ non ramifié hors d'un ensemble $\{p_1, ..., p_k\}$ de points $\mathbb{K}$-rationnels et dont la monodromie en p_i est engendrée par un élément de c_i.*

Ce revêtement est unique à G-isomorphisme près si on fixe les points p_i et si on choisit une racine primitive N-ième de l'unité dans $\mathbb{K}$, c'est-à-dire un facteur du polynôme cyclotomique dans $\mathbb{K}$.

Si $k = 3$ et $\{p_i\} = \{0, 1, \infty\}$, nous avons un dessin d'enfant. Le calcul de la correspondance de Grothendieck permet alors d'expliciter l'extension $\mathbb{L}/\mathbb{K}(T)$. Bien évidemment, ceci est surtout intéressant si $\mathbb{K} = \mathbb{Q}$, mais les conditions sur le k-uplet $(c_1, ..., c_k)$ sont trop sévères pour être souvent vérifiées. Serre [41, p84] cite une variante simple du théorème 2 où la $\mathbb{Q}$-rationalité de toutes les c_i n'est pas nécessaire pour avoir une extension de $\mathbb{Q}(T)$.

f. Un critère de rationalité

D'un point de vue bien plus général, nous pouvons avoir une version du théorème 2 où toutes les hypothèses sont affaiblies.

Le centre $\mathcal{Z}(G)$ du groupe G ne doit pas nécessairement être trivial. Il suffit que $\mathcal{Z}(G)$ ait un complément dans G. Cela signifie qu'il existe un sous-groupe H tel que tout élément $g \in G$ se factorise de façon unique en un produit uh où $u \in \mathcal{Z}(G)$ et $h \in H$.

L'hypothèse de rigidité est en fait une hypothèse sur la valeur de $n_{\mathfrak{C}}$. L'hypothèse de rationalité peut être généralisée en calculant l'entier $e_{\mathfrak{C}}$.

Théorème 3 (D'après Matzat) *Si le centre de G a un complément et si $l^i_{\mathfrak{C}} > 0$, il existe une extension régulière de $\mathbb{K}(T)$ de groupe de Galois G et de structure de ramification $\mathfrak{C}^*$.*

L'intersection $\mathbb{K}_0$ de $\mathbb{K}$ avec le corps engendré par les valeurs des caractères irréductibles sur les classes de $\mathfrak{C}$ est un corps abélien tel que $[\mathbb{K} : \mathbb{K}_0] \leqslant l^i_{\mathfrak{C}}$ et $[\mathbb{K}_0 : \mathbb{Q}] \leqslant e_{\mathfrak{C}}$.

Si $\mathfrak{C}$ est rigide, nous retrouvons le résultat de Serre : $\mathbb{K} = \mathbb{Q}$ lorsque $e_{\mathfrak{C}} = 1$, donc lorsque le k-uplet $\mathfrak{C}$ est invariant par élévation aux puissances n-ièmes, c'est-à-dire si les caractères sont globalement invariants sous l'action du groupe $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

Il existe d'autres critères de rationalité, utilisant par exemple l'action du groupe de tresses sur le lieu de ramification.

Chapitre III

Calcul de la fonction de Belyi

La correspondance de Grothendieck pose (entre autres) le problème de son calcul explicite. Étant donnée une paire de Belyi (X, β), Leila Schneps [37, p60] propose, dans le cas d'un dessin propre de genre 0, une méthode rigoureuse† pour calculer la monodromie $(\sigma_0, \sigma_1, \sigma_\infty)$ et la préimage de $[0, 1]$ par β. Cette méthode s'applique facilement au cas des dessins non nécessairement propres.

Pour le problème inverse, la méthode employée est souvent la résolution d'un système algébrique dont les inconnues sont les paramètres de la fonction de Belyi. Nous commencerons par présenter la construction d'un tel système. Nous énumérerons ensuite quelques autres méthodes de calcul d'une fonction de Belyi.

Nous concluons en donnant des résultats géométriques d'approximation, qui permettent d'aider le calcul en s'inspirant d'une intuition géométrique.

III.1 Le système algébrique

III.1.1 Paramètres de la paire de Belyi

a. Présentation du problème

Les données sont une description topologique du dessin, nous cherchons à calculer une paire de Belyi (X, β) définie sur un *petit* corps de nombres, son corps des modules, si possible.

Si nous occultons toutes les justifications théoriques, il s'agit de tracer un graphe bipartite sur une surface (compacte connexe de Riemann) X. On cherche à en déduire une fonction (méromorphe) β à valeurs dans $\mathbb{C} \cup \{\infty\}$ telle que la préimage de $[0, 1]$ dessine ce graphe sur la surface.

Il y a unicité de cette fonction, lorsqu'on impose certaines conditions. Nous donnons à la surface X une structure de courbe algébrique, et la fonction β est alors une fonction rationnelle sur X. Elle définit donc un revêtement $X \to \mathbb{P}_1$

† On obtient ce résultat en traçant $\beta^{-1}([0, 1])$ par résolution numérique de $y = \beta^{-1}(x)$ pour suffisamment de valeurs x. L'idée est de majorer β' et β'' pour être rigoureux.

ramifié au dessus de trois valeurs au plus. Celui-ci est unique, à isomorphisme de X et de $\mathbb{P}_1$ près.

D'après le théorème de monodromie, la préimage d'un chemin de $\mathbb{P}_1$ évitant les valeurs de ramification est un chemin de X. La préimage de $]0,1[$ est donc une réunion de segments de X ne se croisant pas. Le nombre de ces segments qui se touchent en un point de la préimage de $\{0,1\}$ est l'indice de ramification de ce point.

À partir de la description de la ramification, qu'on obtient en lisant la description combinatoire du dessin, on en déduit des propriétés contraignantes pour la fonction β. Ce sont des conditions sur les indices de ramification, qui suffisent souvent à définir un système n'ayant qu'un nombre fini de solutions, l'une d'entre elle correspondant au dessin considéré.

Il n'est pas facile de compléter ces conditions pour contraindre le calcul de la fonction de Belyi et obtenir l'unique (à automorphismes des courbes près) correspondant à une monodromie donnée. Cependant, si nous résolvons le système par approximation numérique, le choix d'une approximation initiale à l'aide d'une carte ayant la bonne monodromie dirigera souvent le résultat vers un dessin ayant cette monodromie.

b. Représentation du problème

Un courbe algébrique projective X peut être définie par m équations homogènes en $x_0, ..., x_m$. Les fonctions rationnelles de X (par exemple l'application de Belyi) sont des fractions rationnelles à m variables. Nous notons $\bar{x} = (x_0, ..., x_m)$.

Soit $\lambda \in \mathbb{P}_1$, la ramification de β en λ est donnée par la multiplicité des racines de $\beta - \lambda$ dans la courbe X. En pratique, si $\beta - \lambda = Q(\bar{x})/R(\bar{x})$ et si X est définie par des polynômes $P_i(\bar{x})$, les racines de $\beta - \lambda$ dans la courbe X se calculent comme solutions du système défini par les P_i et par Q.

Si nous connaissons la monodromie (σ_0, σ_1) du revêtement, la longueur des cycles de σ_0, σ_1, σ_∞ est la liste des valences du dessin, c'est-à-dire les indices de ramification au dessus de $0, 1, \infty$.

Regardons ceci sur un exemple : X est la courbe définie par $y^2 - 4(2x + 9)(x^2 + 2x + 9)$. La fonction $\beta(x, y)$ est le polynôme $x^2 + 4x + 18 + y$. Le point $(x, y) = (0, -18)$ est une racine quadruple de β sur X. Les points $(-3, 12)$ et $(9, -108)$ sont racines triple et simple de $\beta - 27$.

c. En genre 0

Lorsque X est de genre 0, c'est une courbe isomorphe (sur $\mathbb{C}$) à la sphère $\mathbb{P}_1$. le paramètre $\bar{x}$ de la courbe est tout simplement un nombre $x \in \mathbb{P}_1\mathbb{C}$ et la fonction de Belyi est une fraction rationnelle en x. Nous avons donc $\beta \in \mathbb{C}(X)$.

La condition de multiplicité des racines de $\beta - \lambda$ se traduit en une condition de multiplicité des racines de quelques polynômes. On pose $\beta = \frac{P(x)}{R(x)}$ et $Q = P - R$. Ces polynômes sont premiers entre eux. On a la correspondance suivante :

Ramification en 0 :	Racines de P que nous notons p_i
Ramification en 1 :	Racines de Q que nous notons q_i
Ramification en ∞ :	Racines de R que nous notons r_i

Connaissant la monodromie $(\sigma_0, \sigma_1, \sigma_\infty)$, les indices de ramification des trois valeurs critiques de β se lisent simplement : c'est la longueur des cycles de σ_0, σ_1 et σ_∞, c'est-à-dire la liste des valences du graphe représentant le dessin.

Il suffit de forcer les valeurs de ces indices de ramification pour être assuré que le revêtement n'a que trois valeurs critiques et pour savoir qu'il n'existe qu'un nombre fini de tels revêtements (à automorphismes près). La première propriété se déduit de la formule de la caractéristique d'Euler, la seconde propriété est une conséquence de l'énumération des graphes ayant des valences données.

III.1.2 Les dessins de genre 0

Cette définition du système algébrique n'est pas nouvelle. Elle vraisemblablement a été introduite par Atkin et Swinnerton-Dyer [2, p6]. Chaque auteur en donne une présentation différente : voir [7, p39], [17, p109] ou [37, p66].

a. Les données du système

Nous cherchons les coefficients d'une fonction de Belyi β dans un corps de définition $\mathbb{K}$ du dessin. Nous connaissons les indices de ramification du revêtement et nous savons que P, Q et R sont premiers entre eux. Notons a_n (resp. b_n et c_n) le nombre de sommets (resp. segments et faces) d'indice de ramification n. On note $a = \sum_{n>0} a_n$ le nombre total de sommets.

Quelques formules lient ces données : comme le dessin est de degré N, nous avons $\sum na_n = \sum nb_n = \sum nc_n = N$. La caractéristique d'Euler est $2 - 2g = \sum a_n + \sum b_n + \sum c_n - N$. Puisqu'il est de genre 0, nous avons donc $a + b + c = N + 2$.

b. Aspect de l'application de Belyi

La fonction de Belyi est une fraction rationnelle en $x \in \mathbb{P}_1\mathbb{C}$, définie à automorphisme de $\mathbb{P}_1\mathbb{K}$ près. Pour être rigoureux, nous devrions donc la formuler en coordonnées homogènes, modulo la composition à gauche par une homographie quelconque.

Il est plus simple de se libérer de cette présentation en fixant quelques paramètres qui vont déterminer l'homographie et en manipulant avec prudence des formules où $x \in \mathbb{C} \cup \{\infty\}$ au lieu de $\mathbb{P}_1\mathbb{C}$.

La fonction de Belyi a donc la forme suivante :

$$\beta(x) = \frac{P(x)}{R(x)} = 1 + \frac{Q(x)}{R(x)} \qquad P, Q, R \in \mathbb{K}[X].$$

L'égalité polynomiale III.1 induit l'égalité des coefficients des polynômes, ce qui définit un système de $N + 1$ équations dans $\mathbb{K}$ auquel la fonction de Belyi fournit une solution :

$$P(x) - R(x) = Q(x). \tag{III.1}$$

Mais si un triplet de polynômes (P, Q, R) est solution de cette égalité alors tout triplet (kP, kQ, kR) pour $k \in \mathbb{K}$ aussi. En particulier, le triplet $(0, 0, 0)$ est une solution que nous aimerions éviter. Nous modifions donc légèrement l'équation pour que P, Q et R soient unitaires, en faisant apparaître un paramètre $\lambda \in \mathbb{K}$. La fonction de Belyi a alors la forme

$$\beta(x) = \frac{P(x)}{\lambda R(x)} \qquad P, R \in \mathbb{K}[X] \quad \text{unitaires.}$$

La nouvelle forme de l'équation III.1 dépend du degré des polynômes P, Q et R. S'ils sont tous de degré N, cela signifie que l'infini n'est pas ramifié.

c. Cas où l'infini n'est pas ramifié

Pour tout dessin, il est possible de supposer que l'infini n'est pas ramifié sans perte de généralité (c'est-à-dire sans modifier le corps de définition de β). Si l'infini est ramifié, on choisit un rationnel θ non ramifié et on remplace x par $x/(x-\theta)$. Les degrés des polynômes P, Q et R sont tous égaux à N. Nous obtenons ainsi une égalité de degré $N-1$:

$$P(x) - \lambda R(x) = (1-\lambda)Q(x) \tag{III.2}$$

$$\text{où} \quad P(x) = \prod_{n>0} \left(x^{a_n} + \sum_{i=0}^{a_n-1} \alpha_{n,i} x^i \right)^n \qquad \text{et autres.}$$

L'égalité ci-dessus (III.2) nous donne un système de N équations, avec $N+3$ inconnues (les $\alpha_{n,i}$, $\beta_{n,i}$, $\gamma_{n,i}$ et λ), à solutions dans $\mathbb{K}$.

Nous savons que la variété solution a une composante de dimension 3 sur $\mathbb{K}$ qui correspond à l'application de Belyi que nous cherchons, à composition près par l'espace de dimension 3 des homographies $x \mapsto \frac{ax+b}{cx+d}$.

Mais cette variété a des composantes parasites qui correspondent aux cas où les polynômes P, Q et R ne sont pas premiers entre eux.

- Pour éliminer les solutions où $\lambda = 0$ ou $\lambda = 1$, on peut rajouter une variable μ et l'équation $\lambda(\lambda-1)\mu = 1$. C'est une astuce qui marche assez bien pour une résolution par base de Gröbner.

- Pour éliminer les autres cas où P, Q et R ont un facteur commun, on peut rajouter une collection d'équations et de variables supplémentaires. Mais ceci n'est pas pratiquable, le système devenant bien trop complexe.

Cet inconvénient est contourné à l'aide d'une *astuce de différentiation* très classique, dans le cas où l'infini est ramifié. Il est toujours possible de composer la fonction de Belyi par une homographie pour placer une ramification à l'infini, mais ceci est un marquage du dessin (cf. II.2.2.a.), qui peut changer le corps des modules du dessin. Différents choix donneront parfois différents corps de définition.

d. Placement d'un célibataire à l'infini

On appelle *célibataire* un point de ramification unique par sa valence. Il correspond donc à un polynôme $P_{[n]}$, $Q_{[n]}$ ou $R_{[n]}$ de degré 1, qui vaut donc $X+\eta$ où $\eta \in \mathbb{K}$ peut être placé à l'infini par une homographie qui ne change pas le corps de définition.

S'il existe un célibataire, nous supposerons que c'est une face dont la valence sera notée v_∞, nous avons donc $c_{v_\infty} = 1$, et on place cette face à l'infini. La fonction R est alors ramifiée de degré v_∞ à l'infini, ce qui signifie que $d^o(R) = N - v_\infty < N$. Notre système devient :

$$P(x) - \lambda R(x) = Q(x)$$

L'astuce de *différentiation* permet d'éliminer λ et d'éviter les composantes parasites de la solution du système III.2, en dérivant l'égalité $\beta = P/R = \lambda + Q/R$. On obtient alors :

$$P'R - PR' = Q'R - QR'.$$

Si on pose $\hat{P}$ le PGCD de P et P', avec $P = \hat{P}P_0$ et $P' = \hat{P}P_1$, on a (en simplifiant par $\hat{R}$).

$$\hat{P}(P_1R_0 - P_0R_1) = \hat{Q}(Q_1R_0 - Q_0R_1).$$

Nous remarquons que $\hat{P}$ et $\hat{Q}$ sont premiers entre eux et que le degré de $\hat{P}$ (qui est $N-a$) égale le degré de $Q_1R_0 - Q_0R_1$ (qui est $b+c-2$). On rappelle que v_∞ est la valence de la face à l'infini, nous avons donc le système † :

$$\begin{array}{rcl} P_1R_0 - P_0R_1 & = & v_\infty \hat{Q} \\ Q_1R_0 - Q_0R_1 & = & v_\infty \hat{P} \end{array} \tag{III.3}$$

Nous pouvons de la même façon obtenir l'équation :

$$Q_1P_0 - Q_0P_1 = \lambda v_\infty \hat{R} \tag{III.4}$$

Explicitons les formules définissant $\hat{P}$, P_0, P_1, etc. en fonction des $\alpha_{n,i}$, etc.

$$\begin{array}{ll} \text{on pose} & P_{[n]}(x) = \left(x^{a_n} + \sum_{i=0}^{a_n-1} \alpha_{n,i} x^i \right) \\ \text{on a} & P = \prod_{n>0} P_{[n]}^n \quad \text{et} \quad P' = \sum_{n>0} n P'_{[n]} P_{[n]}^{n-1} \prod_{m \neq n} P_{[m]}^m \\ \text{d'où} & \hat{P} = \prod_{n>0} P_{[n]}^{n-1} \quad , \quad P_0 = \prod_{n>0} P_{[n]} \quad \text{et} \quad P_1 = \sum_{n>0} n P'_{[n]} \prod_{m \neq n} P_{[m]} \end{array}$$

Le système : on va résoudre (III.3). Ce système a $N+1$ inconnues et $N+c-2$ équations et une solution de dimension 2. Cette redondance, de dimension $c-1$ (c'est-à-dire le nombre de faces ailleurs qu'à l'infini) est très utile pour la méthode des bases de Gröbner.

Si c'est un dessin propre : on a $\hat{Q} = Q_0$ et $\hat{Q}' = Q_1$. Nous pouvons donc facilement éliminer les β_{i_n} de la seconde équation de (III.3), ce qui donnera un système de $N/2$ inconnues et $N/2 + c - 2$ équations.

† NB : si nous n'avions pas placé de face à l'infini, l'astuce de différentiation aurait donné les formules ci-dessous, bien moins utiles, où les P_λ, Q_λ et R_λ sont des polynômes de degré 1, dépendants de λ.

$$\begin{array}{rcl} P_1R_0 - P_0R_1 & = & Q_\lambda \hat{Q} \\ Q_1R_0 - Q_0R_1 & = & P_\lambda \hat{P} \\ Q_1P_0 - Q_0P_1 & = & R_\lambda \hat{R} \end{array}$$

Position du dessin dans $\mathbb{P}_1\mathbb{C}$: Nous savons que la position d'un dessin est déterminée à homographie près. Dans le cas d'un dessin marqué, nous imposons $\infty \mapsto \infty$ et il reste deux paramètres.

Le plus simple est de choisir deux valeurs arbitraires qui imposeront la position du "centre de gravité" (translation) et l'échelle du dessin (homothétie). Pour que ce choix ne grossisse par le corps de définition, nous donnons donc certaines valeurs rationnelles à deux inconnues du système.

On décide donc que l'un des $\alpha_{n,0}$ vaut 0, ce qui fixe la translation. Si cette condition n'impose pas que tous les autres $\alpha_{n,0}$ (ou $\beta_{n,0}$ ou $\gamma_{n,0}$) sont nuls, on décide que l'un d'eux vaut 1, ce qui fixe l'homothétie. Voir aussi Couveignes [16, p10].

Cette approche (rudimentaire) suffit pour la plupart des calculs. Pour des dessins dont on sait que le calcul sera compliqué, une étude plus précise peut parfois accélérer la résolution du système.

III.1.3 Cas des arbres.

a. Polynômes de Shabat

Dans le cas où le dessin est un arbre, il y a une unique face de valence N qui est donc un célibataire que nous plaçons à l'infini. Nous avons donc $v_\infty = N$ et $R = \hat{R} = 1$. Le système (III.3) devient : $P_0 = N\hat{Q}$ et $Q_0 = N\hat{P}$.†

La fonction de Belyi est un polynôme. Shabat [42] définit ainsi un polynôme de Chebyshev généralisé comme un polynôme f dont les valeurs critiques sont $\{\pm 1\}$. Ils sont parfois appelés polynômes de Shabat. Il correspondent à la fonction de Belyi d'un arbre $\beta = \frac{1}{2}(f+1)$ ou à la fonction de Belyi d'un arbre propre $\beta = 1 - f^2$.

b. Recherche numérique des racines

Pour les arbres, il existe un système algébrique très simple ou les inconnues ne sont plus les coefficients des polynômes $P_{[n]}$ et $Q_{[n]}$ mais leurs racines [16] On note n_{p_i} (resp. n_{q_i}) la valence du sommet p_i (resp. du segment q_i).

Comme $\hat{R} = 1$, l'égalité (III.4) peut se réécrire (où Θ est un polynôme de degré $N+1$) :

$$\frac{Q_1}{Q_0} - \frac{P_1}{P_0} = \frac{\lambda v_\infty \hat{R}}{P_0 Q_0} \qquad \text{d'où} \quad \sum_{i=1}^{n_q} \frac{n_{q_i}}{x - q_i} - \sum_{i=1}^{n_p} \frac{n_{p_i}}{x - p_i} = \frac{1}{\Theta(x)}.$$

Un développement en l'infini (avec $x = 1/U$) nous donne la formule ci-dessous :

$$\sum_{i=1}^{n_q} \frac{n_{q_i} U}{1 - q_i U} - \sum_{i=1}^{n_p} \frac{n_{p_i} U}{1 - p_i U} = \mathcal{O}(U^{N+1}).$$

Les coefficients de U^2 à U^N de cette équation nous donnent :

$$\forall 1 \leqslant k \leqslant N-1 \qquad \sum_{i=1}^{n_p} n_{p_i} p_i^k = \sum_{i=1}^{n_q} n_{q_i} q_i^k. \tag{III.5}$$

† C'est le système $Y = nS$, $U = nR$ de Betrema et Zvonkine [9].

Comme (III.3), ce système a $N-1$ équations avec $N+1$ inconnues et ne fait pas intervenir λ. Mais les inconnues ne sont pas les mêmes et nous avons une plus grande stabilité numérique. En revanche, il est exclu d'utiliser ce système pour une résolution algébrique car a priori ses inconnues ne sont pas dans le corps de définition du dessin.

III.2 Autres méthodes

III.2.1 Méthodes directes

a. La projection d'une courbe elliptique sur la première coordonnée

Toute courbe de genre 1 est une courbe elliptique E, dont l'équation peut s'écrire $ZY^2 = V(X, Z)$ où V est un polynôme homogène de degré 4 ayant quatre racines sont distinctes. Nous avons alors le revêtement $\beta_V : E \to \mathbb{P}_1$, $(X : Y : Z) \mapsto (X : Z)$ qui a quatre valeurs de ramification d'ordre 2, l'ensemble R des racines de V.

Si nous composons ce revêtement avec une fonction de Belyi $\lambda : \mathbb{P}_1 \to \mathbb{P}_1$ telle que $\lambda(R) \subset \{0, 1, \infty\}$, nous obtenons un revêtement de genre 1, ramifié au dessus de $\{0, 1, \infty\}$.

Si la liste des valences du revêtement λ est $[r_1 ... r_c;\ p_1 ... p_a;\ q_1 ... q_b]$, on obtient la liste des valences du revêtement $\beta \circ \lambda$ en doublant les valences correspondant à R et répétant les autres. Par exemple, le double de $[\underline{3};\ \underline{21};\ 2\underline{1}]$ est $[6;\ 42;\ 222]$, le double de $[\underline{3};\ \underline{21};\ \underline{2}1]$ est $[6;\ 42;\ 411]$ et le double de $[\underline{43};\ 3\underline{22};\ 2221]$ est $[86;\ 4433;\ 22222211]$.

C'est la méthode utilisée par Birch [7] pour la plupart de ses exemples de dessins de genre 1, sous la forme du *double* d'un dessin de genre 0.

b. Construction de Belyi

Il ne s'agit pas ici de trouver la fonction de Belyi d'un dessin dont on connaît les degrés de ramification ou la monodromie, mais de trouver la fonction de Belyi d'un dessin de genre 0 pour lequel les points $\bullet$ et $\circ$ sont à une position prédéfinie. Plus précisément, nous cherchons une fonction non ramifiée hors de $\{0, 1, \infty\}$

$$\beta(x) = \prod_{i=1}^{n} (x - \lambda_i)^{r_i}$$

où les λ_i sont fixés et distincts et les $r_i \in \mathbb{Z}$ inconnus. Par construction, les points de ramification de cette fonction sont les zéros et pôles de sa dérivée logarithmique β'/β. Belyi [6] propose une solution dans le cas où les λ_i sont entiers.†

On calcule les déterminants de Vandermonde $W = \mathrm{Det}_{\mathrm{VdM}}(\lambda_1, \lambda_2, ..., \lambda_n)$ et $w_i = (-1)^{i-1} \mathrm{Det}_{\mathrm{VdM}}(\lambda_1, ..., \hat{\lambda}_i, ..., \lambda_n)$, où $n \geqslant 2$ et où $\hat{\lambda}_i$ signifie comme d'habitude qu'on omet λ_i. Ils sont liés par l'identité

$$\sum_{i=1}^{n} \frac{w_i}{x - \lambda_i} = W \prod_{i=1}^{n} \frac{1}{x - \lambda_i}$$

† Belyi prend des entiers premiers entre eux $\lambda_1 = 0 < \lambda_2 < ... < \lambda_n$, mais cela se généralise trivialement à n'importe quels entiers distincts.

d'où on déduit par exemple que $\sum_{i=1}^n w_i = 0$. Or il se trouve que $\frac{\beta'(x)}{\beta(x)} = \sum_{i=1}^n \frac{r_i}{x-\lambda_i}$. Si les λ_i sont entiers, les w_i aussi, ils permettent alors de construire β.

III.2.2 Séries de Puiseux

Nous commençons par étudier localement la fonction de Belyi. Nous choisissons une valeur de ramification parmi $\{0, 1, \infty\}$, par exemple 0, et un point (de ramification) $p \mapsto 0$ d'ordre n. Un voisinage de p dans la surface X est par exemple un disque centré en p, dans lequel la fonction de Belyi est équivalente à x^n. Sa réciproque est donc équivalente à une racine n-ième.

Pour reformuler ceci de façon plus canonique, nous introduisons comme dans [17] des uniformisantes $\Lambda_{\vec{f},n}$ pour chaque fléchette $\vec{f}$. La réciproque de la fonction de Belyi peut alors être exprimée localement comme une série en $\Lambda_{\vec{f},n}$.

Nous avons donc $6N$ formules locales. L'égalité de ces séries en des points qui sont dans l'intersection de leurs domaines de convergence peut être utilisée pour en déduire une description de X et de la fonction de Belyi.

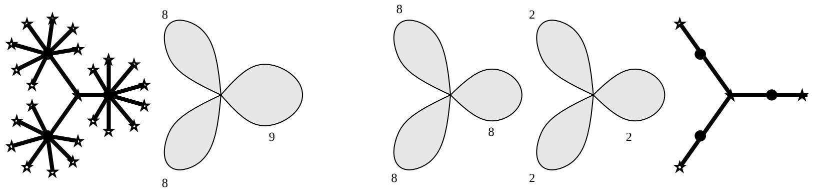
III.3 Approximation de dessins

III.3.1 Résolution par étapes dans $\mathbb{C}$

a. Idée générale

Pour utiliser une méthode numérique de résolution du système, nous devons trouver une première approximation du dessin, qui soit assez proche de la solution pour être dans la zone de convergence de l'algorithme de Newton. Comme on le voit dans [9] et dans le paragraphe IV.4.2, la géométrie d'un dessin a l'air de respecter une certaine régularité.

La généralisation des fonctions de Belyi sous la forme de différentielles de Strebel permet d'avoir une transformation continue d'un dessin vers un autre. En particulier, le dessin ci-dessous explique comment on peut raisonnablement supposer que le dessin de valences $[25; 3\,1^{22}; 9\,8^2]$ est proche du dessin de valences $[24; 3\,1^{21}; 8^3]$ qui est lui-même un multiple de $[6; 3\,1^3; 2^3]$.



Le principe est donc d'utiliser les positions des points de ramification d'un dessin dont la structure en tant que graphe est proche du dessin que nous voulons calculer. Notre méthode, qui repose sur l'intuition de l'utilisateur, effectue des calculs de fonctions de Belyi de dessins de plus en plus compliqués, et se ressemblant.

b. Suppression d'un sommet de valence 1

Si on considère un dessin (de genre 0) comme un graphe plan, nous pouvons nous demander ce qui se passe si on supprime un sommet de ce graphe, en particulier si c'est un sommet de valence 1. On remarque "expérimentalement" que les positions des sommets éloignés sont presque inchangées.

Le procédé inverse, qui consiste à rajouter un sommet à une position bien choisie, pour avoir ainsi une estimation de la position des sommets d'un dessin plus gros, a donc de bonnes chances de marcher. En effet, c'est ainsi que je réussis à calculer les exemples du chapitre IV.

c. Ajout d'un sommet de valence 1

Ce sont des considérations locales qui vont nous permettre de savoir où placer le point supplémentaire. On prouve facilement que les angles formés par les arêtes du dessin autour d'un point de ramification sont égaux, car la réciproque de la fonction de Belyi est une racine n-ième. Quant à la distance des sommets voisins d'un autre sommet, elle dépend principalement de leur valence.

Dans un premier temps, nous supposons que (localement au moins) le dessin est un arbre. Nous avons un sommet central et k voisins, de valences $(n_i)_{i=1..k}$. La distance du sommet numéro i est environ $\frac{n_i}{\sum_j n_j}$. Cette première estimation est assez précise. La figure IV.2 montre deux exemples de familles d'arbres, où on rajoute un sommet à chaque étape.

Dans un deuxième temps, nous étendons cette estimation au cas où un des sommets voisins est contigu à une face de valence 1, le dessin a une boucle. On peut appliquer la même estimation de distance, en considérant un poids ν_i au lieu de la valence n_i de chaque sommet. On pose $\nu_i = n_i - 1$ pour le sommet d'où part la boucle et $\nu_i = n_i + 1$ pour les autres. Cette estimation est elle-aussi assez efficace.

En règle générale, nous pouvons considérer chaque sommet comme une charge répulsive de valeur ν_i, telle que ν_i croît si le nombre de sommets voisins croît, et décroît s'il y a des boucles de petite longueur.

III.3.2 Résolution approchée dans $\mathbb{Q}_p$

Comme précisé en I.1.3, un tel calcul n'est envisageable que si nous savons qu'un corps $\mathbb{K}$ de définition du dessin est inclus dans un $\mathbb{Q}_p$ connu. Par exemple, Malle [29] a ainsi calculé un polynôme ayant groupe de Galois M_{22}. Il fallait calculer un dessin défini sur $\mathbb{Q}(\sqrt{-11})$, qui est inclus dans $\mathbb{Q}_{23}$. Après recherche par bases de Gröbner des solutions modulo 23, il utilise le lemme de Hensel pour avoir son résultat dans $\mathbb{Q}_{23}$. Comme $\mathbb{Q}(\sqrt{-11})$ est de degré 2, il utilise les fractions continues pour trouver une formule exacte du résultat. En degré supérieur à 2, nous pouvons utiliser LLL.

III.3.3 Approximation de revêtements ramifiés au dessus de 4 points

a. Pour le calcul d'un tel revêtement

Dans le cas de revêtement ramifiés au dessus de quatre points, le déplacement des valeurs de ramification donne un revêtement dont la description numérique est proche. Si on réunit deux ramifications distinctes, les propriétés algébriques sont radicalement changées, mais l'aspect numérique reste proche.

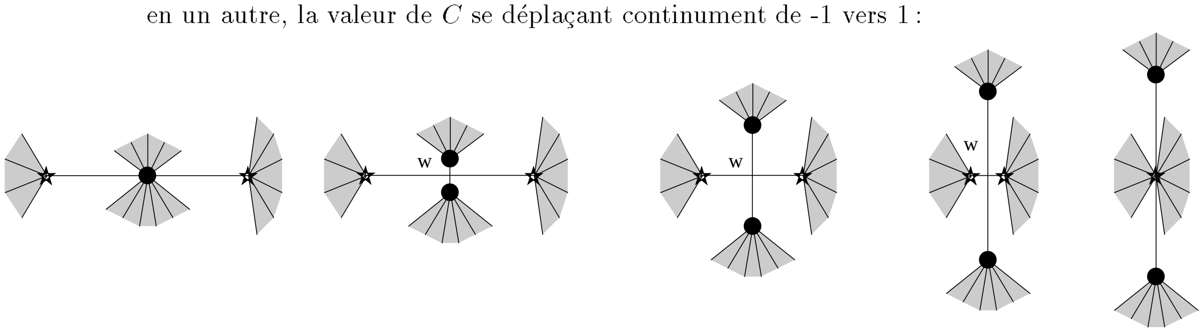
Ici aussi l'intuition géométrique joue un rôle fondamental, mais dans ce cas elle peut s'appuyer sur des théorèmes. Matzat [34] par exemple a montré comment il est possible de décrire algébriquement la collision (ou l'éclatement) de deux valeurs de ramification. En pratique, cela signifie qu'on peut ne regarder que la monodromie du revêtement et en déduire celle du revêtement dégénéré.

b. Pour le calcul d'un dessin

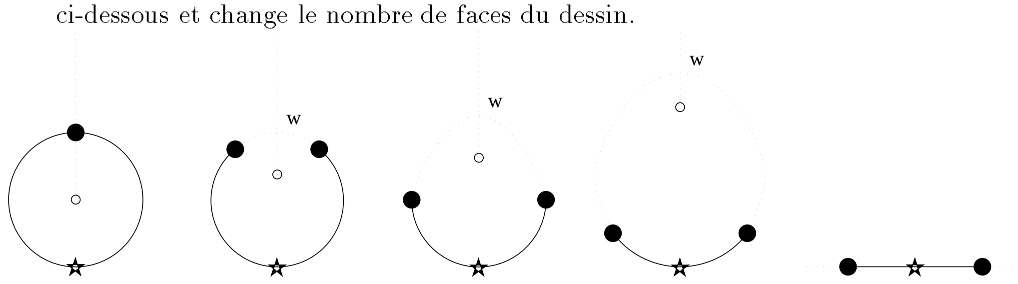
Le passage par un revêtement ramifié au dessus de quatre points est utilisé par Matiyasevich [31] pour automatiser le calcul des fonctions de Belyi des arbres.

Il appelle *polynôme quasi-généralisé de Tchebitchev* un polynôme ayant quatre valeurs critiques : -1, 1, ∞ et C, avec $-1 < C < 1$ et tel qu'il existe un seul point critique au dessus de C, de valence 2, noté w. Les polynômes quasi-généralisés de Tchebitchev de degré N définissent une famille de revêtements ramifiés au dessus de quatre valeurs, dont les revêtements dégénérés correspondent à tous les polynômes généralisés de Tchebitchev de degré N, c'est-à-dire tous les dessins d'enfants de degré N qui sont des arbres.

Matiyasevich effectue ainsi le calcul de tout arbre de degré N, en partant du polynôme généralisé de Tchebitchev $1 - 2x^N$ qui correspond à l'étoile à N branches. La séquence de dessins ci-dessous montre la transformation d'un arbre en un autre, la valeur de C se déplaçant continument de -1 vers 1 :



L'article de Matiyasevich peut facilement être généralisé au calcul de n'importe quel dessin de genre 0 : on définit les fonctions de quasi-Belyi comme ayant quatre valeurs de ramification 0, 1, ∞ et C, de telle sorte qu'il n'existe qu'un point critique au dessus de $C \in \mathbb{R}$, de valence 2. Le déplacement de C entre 0 et 1 correspond aux dessins ci-dessus, le déplacement de C entre 0 et ∞ au dessin ci-dessous et change le nombre de faces du dessin.



Chapitre IV

Exemples de calculs

IV.1 Matériel et méthodes

IV.1.1 Logiciels

Pour les calculs de bases de Gröbner, nous utilisons Maple V release 4 (logiciel payant), Mupad 1.3 (disponible sur `http://www.mupad.de/distrib.html`) ou GB v4 (dans `ftp://posso.ibp.fr/pub/softwares/GB`). Voir aussi l'annexe A.

Pour les calculs numériques, nous avons écrit un programme spécifique. Le calcul multiprécision est fait avec la bibliothèque Pari ou la bibliothèque NTL. L'algorithme LLL est celui de Pari, celui de NTL ou celui d'Antoine Joux. Le plus simple (et ce qui a servi pour nos estimations de temps de calcul) est d'utiliser NTL à chaque étape.

Pour mieux maîtriser l'aspect géométrique du dessin, nous avons programmé une interface graphique X11, pour les dessins en genre 0. Cette interface permet de tracer le dessin dans le plan, après en avoir calculé la position précise. Il est ensuite possible de lui faire subir les transformations intéressantes.

Pour tous les autres calculs de théorie des nombres, nous utilisons Pari-GP (version 2, voir `http://hasse.mathematik.tu-muenchen.de/ntsw/pari/Welcome`).

Pour les calculs dans des groupes de permutation, nous utilisons Gap (version 3.4, voir `http://wilton.anu.edu.au/research.groups/algebra/GAP/www/Info/`).

IV.1.2 Machines

Sauf mention contraire, les temps de calcul correspondent à une SparcStation 20/71. C'est une machine avec un processeur SuperSparc II à 75 MHz. Mais ces logiciels marchent sur la plupart des systèmes Unix.

IV.1.3 Méthode

Notre logiciel prend en entrée la liste des valences du dessin. Si c'est un arbre, il en déduit une majoration du nombre de conjugués.

À chaque itération de l'algorithme de Newton, il affiche les positions des racines de P, Q et R (qui sont donc sensées être proches des positions des points $\bullet$, $\bigstar$ et $\circ$). Cela permet de maîtriser la convergence du calcul, pour éviter les minima qui ne sont pas des zéros du système. À tout instant, on peut intervenir manuellement sur ces valeurs.

Une fois dans la zone de convergence, notre logiciel calcule la solution avec la précision qui devrait être suffisante. Puis l'algorithme LLL fournit un polynôme minimal pour chaque coefficient des polynômes.

IV.2 Exemples élémentaires

IV.2.1 Étoiles et étoiles doubles, cercles

Les dessins les plus simples sont les *étoiles*: dessins de genre 0 totalement ramifiés en 0 et en ∞. La fonction de Belyi d'une étoile de degré d est $\beta : x \mapsto x^d$. Presque aussi simples, nous avons les *étoiles doubles* qui servent dans la preuve de Belyi. Ce sont des arbres de type $[m+n; m\,n; 2\,1^{m+n-2}]$ et de fonction de Belyi $\beta : x \mapsto \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n$.

Les *cercles*, de type $[n^2;\ 2^n;\ 2^n]$ ont pour fonction de Belyi $\frac{(x^n-1)^2}{-4x^n}$.

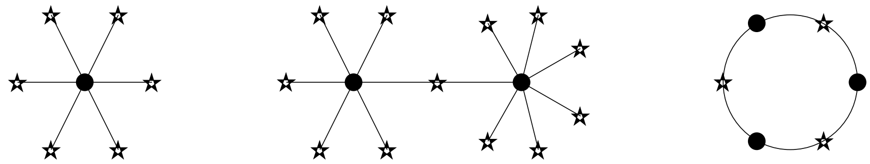


FIG. IV.1 – *Étoile, étoile double et cercle.*

IV.2.2 Lignes

On peut remarquer que les polynômes de Tchebitchev, définis par $T_n(x) = \cos(n \arccos(x))$, ont pour valeurs critiques ± 1.

La fonction $\Theta : x \mapsto 1 - 2x$ transforme ± 1 en $\{0, 1\}$, on en déduit que les arbres (linéaires) de type $[d = 2n;\ 2^{n-1}1^2;\ 2^n]$ et $[d = 2n+1;\ 2^n 1;\ 2^n 1]$ ont pour fonction de Belyi $\beta = \Theta^{-1} \circ T_d \circ \Theta$

IV.3 Les arbres en Y

IV.3.1 Classification

a. Énumération

On étudie la famille des arbres ayant un unique sommet de valence 3, tous les autres étant de valence 1 ou 2. Si les branches de l'arbre ont pour longueurs a, b, c, Pakovitch [36, chap. 2] les note $Y_{a,b,c}$. Nous les appelons *arbres en Y* ou *Y-arbres*.

Comme pour tous les arbres, nous séparons les sommets des arbres en Y en deux types $\bullet$ et $\bigstar$. Les types des trois sommets de valence 1 forment un invariant Galoisien qui détermine quatre familles d'arbres en Y. Nous supposons que le sommet de valence 3 est de type $\bullet$ et nous comptons le nombres d'arbres de chaque type avec la formule du paragraphe II.3.4. Ici, k est un entier naturel quelconque.

– [Type A] Extrémités de types $\bigstar$, $\bigstar$, $\bigstar$.

  Il y a $n_A(k) = \frac{(k+1)(k+2)}{6}$ dessins de type $[3+2k; 32^k; 2^k1^3]$.

– [Type B] Extrémités de types $\bullet$, $\bigstar$, $\bigstar$.

  Il y a $n_B(k) = \frac{(k+1)(k+2)}{2}$ dessins de type $[4+2k; 32^k1; 2^{k+1}1^2]$.

– [Type C] Extrémités de types $\bigstar$, $\bullet$, $\bullet$.

  Il y a $n_C(k) = \frac{(k+1)(k+2)}{2}$ dessins de type $[5+2k; 32^k1^2; 2^{k+2}1]$.

– [Type D] Extrémités de types $\bullet$, $\bullet$, $\bullet$.

  Il y a $n_D(k) = \frac{(k+1)(k+2)}{6}$ dessins de type $[6+2k; 32^k1^3; 2^{k+3}]$.

On remarque que si k est un multiple de 3, les nombres $n_A(k)$ et $n_D(k)$ ne sont pas entiers. La valeur $1/3$ correspond à l'arbre dont les trois branches sont de longueurs égales ($(2k+6)/3$ ou $(2k+3)/3$), qui admet un automorphisme d'ordre 3 (la rotation d'un tiers de tour).

b. Action de Galois

Voici ce qu'on peut conjecturer sur les orbites sous l'action de Galois. La preuve de la dernière conjecture est immédiate, car les branches des Y-arbres de type D sont de longueur paire. Ces conjectures font que les Y-arbres de type B ou C sont de bons candidats pour avoir des corps des modules† de degré assez élevé, ce qui permet de tester nos algorithmes.

– Les Y-arbres de type A sont les conjugués des $Y_{1,1,2k+1}$ et les multiples impairs de ces arbres (cette conjecture est vérifiée pour $k \leqslant 12$).

– Les Y-arbres de type B sont les conjugués des $Y_{1,1,2k+2}$ et les multiples impairs de ces arbres (cette conjecture est vérifiée pour $k \leqslant 10$).

– Les Y-arbres de type C sont les conjugués des $Y_{2,2,2k+1}$ et les multiples impairs de ces arbres (cette conjecture est vérifiée pour $k \leqslant 9$).

– Les Y-arbres de type D sont les doubles (au sens du § II.3.3.c.) d'un autre Y-arbre de degré moitié.

Nous appelons donc Y-arbre irréductible un arbre $Y_{1,1,N-2}$ ou un arbre $Y_{2,2,2k+1}$. Nous vérifions notre conjecture en calculant le degré des corps des modules des Y-arbres irréductibles.

† Si nous plaçons l'unique face à l'infini, le corps des modules d'un arbre est un corps de définition, que le calcul d'une fonction de Belyi donne assez directement.

IV.3.2 Résultats

a. Description des tables

La première table donne, pour les Y-arbres de type B, les temps et mémoire utilisés pour le calcul d'un polynôme P définissant le corps des modules. On voit que la méthode numérique est au moins aussi performante qu'une utilisation classique de bases de Gröbner.

Une seconde table donne, pour les Y-arbres de type A, B ou C la longueur des orbites galoisiennes. On donne le discriminant du corps des modules des Y-arbres irréductibles, ou un multiple de ce discriminant si le calcul est impraticable.

La troisième table donne les polynômes P obtenus par nos calculs. Lorsque le corps est de petit degré, nous donnons aussi un autre polynôme Q, unitaire, définissant le corps des modules de façon un peu plus canonique (voir l'algorithme `polred` [11, p166]).

Voici quelques précisions sur le calcul du polynôme P : pour les arbres de type B, on place le sommet $\bullet$ de valence 3 en 0, le sommet $\bullet$ de valence 1 en 1, et le polynôme P est le polynôme minimal de la somme des deux sommets $\bigstar$ de valence 1.

Pour les arbres de type C, on place le sommet $\bullet$ de valence 3 en 0, le sommet $\bigstar$ de valence 1 en 1, et le polynôme P est le polynôme minimal de la somme des deux sommets $\bullet$ de valence 1.

Pour les arbres de type A, si nous plaçons le sommet de valence 3 en 0 et si nous imposons la somme des sommets de valence 1 à 1, alors la somme des sommets de même type est toujours rationnelle. Le polynôme P est donc ici le polynôme minimal de la deuxième fonction symétrique des trois sommets de valence 1.

Le calcul de $d(\mathbb{K})$ est bien plus lent et ne peut être mené à terme que pour les petits corps de définition. Pour $B(5)$, le calcul de $d(\mathbb{K})$ à l'aide de Pari (algorithme Round 4) met 120 heures en utilisant 450 Mo de mémoire.

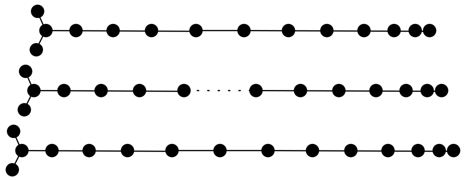
Il faut construire une base intégrale de $\mathbb{K}$, à partir d'un ordre que l'on grossit pour chaque nombre premier. Les algorithmes Round 4 et Round 2 implantés dans Pari partent de l'ordre engendré par une racine d'un polynôme P unitaire. Comme le coefficient dominant des polynômes que nous calculons a de nombreux petits facteurs, ces algorithmes perdent beaucoup de temps à éliminer ces facteurs. Il serait donc utile de développer une extension de ces algorithmes aux ordres engendrés par un P quelconque.

b. Le choix de l'approximation initiale

Pour le calcul par approximation se pose le problème du choix de la position initiale des sommets de l'arbre. Sa solution est ici très facile.

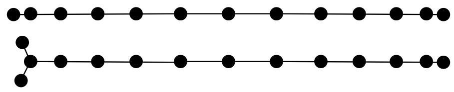
Une première approche est de calculer les propriétés de $Y_{1,1,n}$ en calculant successivement $Y_{1,1,1}$, $Y_{1,1,2}$, ..., $Y_{1,1,n-1}$ et $Y_{1,1,n}$, chacun s'obtenant par rajout d'un point dans la branche la plus longue du précédent.

Nos considérations sur l'aspect du tracé d'un dessin dans le plan suggèrent que la longueur de cette branche a peu d'influence sur ce qui se passe à ses extrémités. Nous choisissons donc de remplacer l'arête du milieu (qui est aussi la plus longue) par deux arêtes ayant cette longueur.



Une seconde approche est de remarquer que l'arbre $Y_{1,1,n}$ est "similaire" à la ligne avec $n+2$ sommets, dont on connaît bien la fonction de Belyi (polynôme de Tchebitchev).

Puisque nous savons qu'au voisinage d'un sommet de valence 3, les arêtes font un angle 1/3 de tour, nous remplaçons la dernière arête de la ligne par deux arêtes de même longueur, symétriques. Chacune de ces deux approches permet d'être dans la zone de convergence de l'algorithme de Newton.



c. Performance des différentes méthodes

sur SS20/71	B(5)	B(6)	B(7)	B(8)	B(9)	B(10)
Maple mini †	10s 2.2 Mo	84s 4.5 Mo	193s 4.5 Mo	28 min 8 Mo	162 min	
Maple standard	71s 3.4 Mo	4h21 25 Mo	*(>64h)* *(>320Mo)*	*(>36h)* *(>190Mo)*	*(>85h)* *(>140Mo)*	*(>55h)* *(>350Mo)*
MuPAD	37s 5.7 Mo	557s 6.3 Mo	7h 12 Mo			
GB modular	0.3s	0.5s	0.8s	1.9s	4.6s	71s
GB comput.	0.3s	0.6s	2.3s	5.8s	14s	110s
GB check	1.1s	2.3s	6.5s	17s	47s	200s
GB totolex	36s	213s	19 min	94 min	613 min	35h
GB mémoire	10 Mo	13 Mo	23 Mo	46 Mo	109 Mo	234 Mo
PAR APPROXIMATION						
convergence	78s	282s	513s	44 min	108 min	242 min
LLL	8s	48s	126s	9 min	35 min	114 min
précision	410 digits	850 digits	1100 digits	1900 digits	3200 digits	3900 digits
mémoire	6 Mo	11 Mo	15 Mo	30 Mo	52 Mo	56 Mo

d. Discriminant du corps de définition

- $n_A(0) = 1/3$ $\mathbb{Q}$.
- $n_A(1) = 1$ $\mathbb{Q}$.

† Sous Maple, les mêmes commandes ne donnent pas toujours les mêmes temps de calcul, car la recherche d'une base de Gröbner utilise un certain nombre d'heuristiques.

Par exemple, nous avons obtenu quatre comportements possibles pour un calcul de $B(5)$ (voir tableau ci-dessous). Le plus probable est celui que j'ai appelé *Moyen*. Le temps *Mini* est malheureusement exceptionnel, les deux autres assez rares. On remarque aussi que pour $B(6)$, cela peut mettre 85 secondes, 260 minutes, ou ne pas terminer au bout de 48 heures.

B(5)	mémoire	Ultra140	SS20/71	SS10/512
Mini	2.2 Mo	7.8–8.1 s	10–11 s	18–22 s
Court	2.9 Mo		42–44 s	70 s
Moyen	3.4 Mo	53–55 s	70–73 s	115–132 s
Long	6.5 Mo		549–555 s	897 s

- $n_A(2) = 2 \qquad d(\mathbb{K}) = 3\,7.$
- $n_A(3) = 3 + 1/3 \qquad d(\mathbb{K}) = -3^3 5.$
  L'orbite de longueur 1 est le triple de $A(0)$.
- $n_A(4) = 5 \qquad d(\mathbb{K}) = -3^3 5^2 7\, 11^3.$
- $n_A(5) = 7 \qquad d(\mathbb{K}) = 3^4 5^3 7^2 13^6.$
- $n_A(6) = 8 + 1 + 1/3 \qquad d(\mathbb{K}) = -3^7 5^7 7^3 11.$
  Les orbites de longueur 1 sont le quintuple de $A(0)$ et le triple de $A(1)$.
- $n_A(7) = 12 \qquad d(\mathbb{K}) = 3^8 5^5 7^4 11^2 13\, 17^{10}.$
- $n_A(8) = 15 \qquad d(\mathbb{K}) = -3^{12} 5^7 7^5 11^3 13^2 19^{13}.$
- $n_A(9) = 16 + 2 + 1/3 \qquad d(\mathbb{K}) = -3^{14} 5^7 7^{15} 11^4 13^3 17.$
  L'orbite de longueur 1 est le septuple de $A(0)$ et celle de longueur 2 le triple de $A(2)$.
- $n_A(10) = 22 \qquad d(\mathbb{K}) = 3^{18} 5^{11} 7^7 11^5 13^4 17^2 19\, 23^{19}.$
- $n_A(11) = 25 + 1 \qquad d(\mathbb{K}) = 3^{17} 5^{43} 7^9 11^6 13^5 17^3 19^2.$
  L'orbite de longueur 1 est le quintuple de $A(1)$
- $n_A(12) = 27 + 3 + 1/3 \qquad d(\mathbb{K}) = -3^{65} 5^{12} 7^9 11^7 13^6 17^4 19^3 23.$
  L'orbite de longueur 1 est le nonuple de $A(0)$ et celle de longueur 3 le triple de $A(3)$.

- $n_B(0) = 1 \qquad \mathbb{Q}.$
- $n_B(1) = 3 \qquad d(\mathbb{K}) = -2^2 3^3.$
- $n_B(2) = 6 \qquad d(\mathbb{K}) = 2^9 3^4 5^2.$
- $n_B(3) = 10 \qquad d(\mathbb{K}) = 2^8 3^6 5^{10} 7^2.$
- $n_B(4) = 14 + 1 \qquad d(\mathbb{K}) = 2^{20} 3^{13} 5^6 7^4.$
  L'orbite de longueur 1 est le triple de $B(0)$.
- $n_B(5) = 21 \qquad d(\mathbb{K}) = -2^{18} 3^{16} 5^8 7^{21} 11^2.^{\dagger}$
- $n_B(6) = 28 \qquad d(\mathbb{K}) = 2^{77} 3^{22} 5^{12} 7^8 11^4 13^2.$
- $n_B(7) = 33 + 3 \qquad d(\mathbb{K}) = -2^{28} 3^{57} 5^{14} 7^{10} 11^6 13^4.$
  L'orbite de longueur 3 est le triple de $B(1)$.
- $n_B(8) = 44 + 1 \qquad d(\mathbb{K}) f^2 = 2^{1550} 3^{646} 5^{43} 7^{118} 11^{88} 13^{78} 17^{34} N^2.$
  L'orbite de longueur 1 est le quintuple de $B(0)$.
- $n_B(9) = 55 \qquad d(\mathbb{K}) f^2 = -2^{1796} 3^{1046} 5^{332} 7^{166} 11^{281} 13^{104} 17^{68} 19^{38} N^2.$

† C'est l'exemple de [16], mais la valeur du discriminant de $\mathbb{K}$ y est fausse.

- $n_B(10) = 60+6 \qquad d(\mathbb{K})f^2 = -2^{3292}3^{122}5^{352}7^{230}11^{132}13^{130}17^{102}19^{76}N^2.$
  L'orbite de longueur 6 est le triple de $B(2)$.

- $n_C(0) = 1 \qquad \mathbb{Q}.$
- $n_C(1) = 3 \qquad d(\mathbb{K}) = -2^2 3\, 7^2.$
- $n_C(2) = 6 \qquad d(\mathbb{K}) = 2^4 3^{10} 5.$
- $n_C(3) = 10 \qquad d(\mathbb{K}) = 2^8 3^7 5^2 7\, 11^8.$
- $n_C(4) = 15 \qquad d(\mathbb{K}) = 2^{12} 3^{10} 5^5 7^2 13^{12}.$
- $n_C(5) = 20+1 \qquad d(\mathbb{K}) = -2^{16} 3^{19} 5^{20} 7^3 11.$
  L'orbite de longueur 1 est le triple de $C(0)$.
- $n_C(6) = 28 \qquad d(\mathbb{K}) = 2^{24} 3^{22} 5^{11} 7^6 11^2 13\, 17^{24}.$
- $n_C(7) = 36 \qquad d(\mathbb{K})f^2 = 2^{3364}3^{592}5^{197}7^{121}11^{45}13^{32}19^{140}N^2.$
- $n_C(8) = 42+3 \qquad d(\mathbb{K})f^2 = -2^{4560}3^{81}5^{255}7^{42}11^{64}13^{51}17^{19}N^2.$
  L'orbite de longueur 3 est le triple de $C(1)$.
- $n_C(9) = 55 \qquad d(\mathbb{K})f^2 = -2^{7884}3^{1352}5^{461}7^{233}11^{85}13^{72}17^{40}19^{21}23^{270}N^2.$

e. Polynômes caractérisant les corps de définition

$A(3)$ $Q = x^3 + 3x - 1,$

$P = 3x^3 + 12x^2 + 27x + 5.$

$A(4)$ $Q = x^5 - x^4 - 9x^3 + 3x^2 - 9,$

$P = 361x^5 - 4474x^4 - 38273x^3 - 65627x^2 - 41455x - 4325.$

$A(5)$ $Q = x^7 - 2x^6 - 15x^5 - 17x^4 + 406x^3 - 1185x^2 + 1528x - 797,$

$P = 54289x^7 - 282278x^6 - 3283899x^5 - 31969477x^4 - 78654736x^3 - 65823135x^2 - 20988650x - 1404125.$

$A(6)$ $Q = x^8 - x^7 - 8x^6 + 47x^5 - 65x^4 - 7x^3 + 217x^2 - 154x + 91,$

$P = 289x^8 - 4885x^7 - 46400x^6 - 342915x^5 - 1089480x^4 - 1739622x^3 - 996660x^2 - 214785x - 10305.$

$A(7)$ $P = 98207651161x^{12} + 870318338439x^{11} - 225964214871x^{10} - 120603046889300x^9 - 1641468242003715x^8 - 8545487217454683x^7 - 23874722290036452x^6 - 38144830567619007x^5 - 35366172814693935x^4 - 18277692100532150x^3 - 4874726982487875x^2 - 585383786486250x - 19309256928125.$

$A(8)$ $P = 870144924171961x^{15} - 31272534505579827x^{14} + 3409826827410834x^{13} + 1631528313606604292x^{12} + 25545284053437227001x^{11} + 265781178080254774527x^{10} + 1656478912849790418811x^9 + 6206289995712665940813x^8 + 14144169927465834515019x^7 + 20094178519992806367157x^6 + 17902864566095038971675x^5 + 9866732665267344460200x^4 + 3223408046591823300500x^3 + 576457341066342065625x^2 + 48553143846669318750x + 1206449284005015625.$

$A(9)$ $P = 92811821263x^{16} + 2185900990315x^{15} + 45151781389620x^{14} + 529427232145945x^{13} + 4647506123797600x^{12} + 28962371220779367x^{11} + 128594938811688720x^{10} + 406119437724414015x^{9} + 902761895287107765x^{8} + 1392468619368942000x^{7} + 1462963566390250932x^{6} + 1022154080759090055x^{5} + 457850422093506750x^{4} + 123967037149475625x^{3} + 18361060568707500x^{2} + 1270568722106250x + 25781283703125.$

$A(10)$ $P = 5110967574223205916281508 1x^{22} - 1222855031957479455016606244x^{21} + \ldots + 891721888539814605911620527 34375x + 1366808126272895577235041015625.$

$A(11)$ $P = 220285971278677899180643 21x^{25} - 1570978381221509566911226 85x^{24} + \ldots + 266306914994407378687794743366260x + 336085679651063762186725941 2161.$

$A(12)$ $P = 62988609009298392434369403x^{27} - 23325513470798812154712197 64x^{26} + \ldots + 1422986981521391200555139707031250x + 15522928406114874760081689453125.$

$B(1)$ $Q = x^3 + 2,$

$P = 25x^3 - 42x^2 + 12x + 8.$

$B(2)$ $Q = x^6 - 2x^5 - x^4 + 6x^3 - 2x^2 - 4x - 1,$

$P = 192x^6 + 1600x^5 + 5488x^4 + 8464x^3 + 5960x^2 + 1784x + 137.$

$B(3)$ $Q = x^{10} - 5x^9 - 10x^8 - 330x^7 + 3780x^6 - 23538x^5 + 146520x^4 - 900210x^3 + 4617195x^2 - 8099745x - 6066414,$

$P = 288x^{10} + 4920x^9 + 37400x^8 + 154160x^7 + 379100x^6 + 574424x^5 + 534980x^4 + 295250x^3 + 89690x^2 + 12950x + 563.$

$B(4)$ $P = 5120x^{14} + 149504x^{13} + 2014208x^{12} + 15777280x^{11} + 79923712x^{10} + 275166208x^9 + 658361216x^8 + 1101880256x^7 + 1283578112x^6 + 1023671040x^5 + 541541472x^4 + 180018720x^3 + 34297616x^2 + 3188528x + 92633.$

$B(5)$ $P = 24883200x^{21} + 1158312960x^{20} + 25502867712x^{19} + 341618429376x^{18} + 3109936201344x^{17} + 20392715344064x^{16} + 99638796203968x^{15} + 370504764844224x^{14} + 1062741483903680x^{13} + 2370640833511888x^{12} + 4128644196255936x^{11} + 5614827771514976x^{10} + 5942714032340512x^{9} + 4860315116093808x^{8} + 3036961695710128x^{7} + 1425822458726372x^{6} + 491072052205560x^{5} + 119836481716252x^{4} + 19663328827436x^{3} + 1993132055040x^{2} + 106550236828x + 2000024111.$

$B(6)$ $P = 513684799488000x^{28} - 34901212948070400x^{27} + 1137545530142883840x^{26} - 23094430990658961408x^{25} + 326698815564602671104x^{24} - 3421329382195643547648x^{23} + 27523540095132109897728x^{22} - 174305408754660243668992x^{21} + 883931948169484761563136x^{20} - 3633243437315754018471936x^{19} + 12208911396657704553414656x^{18} - 33740348646985795280830464x^{17} + 76979469564829984977911808x^{16} - 145292021332525428824211456x^{15} + 226960358645737432122753024x^{14} - 293120952934211895334699008x^{13} + 312191481069764390293626880x^{12} - 273058909744499620720631808x^{11} + 194957884663016060566106112x^{10} - 112699121083547276423794688x^{9} + 52176655480973862044680704x^{8} - 19071337921265203163214336x^{7} + 5399626220939144567968512x^{6} - 1154053132723323568606464x^{5} + 179599504361044758896448x^{4} - 19299434128448598021184x^{3} + 1315528871847908959392x^{2} - 486306933596563742 40x + 658418172827465249.$

$B(7)$ $P = 128450560000x^{33} - 11707809792000x^{32} + 515906676326400x^{31} - 14320455719649280x^{30} + 280278666945232896x^{29} - 4112010196865513472x^{28} + 46962642048178507264x^{27} - 428236816106298382848x^{26} + 3174061201133603157504x^{25} - 19372769702192537887488x^{24} + 98305223546172769210368x^{23} - 417686500832906293682688x^{22} + 1493724878756594616210432x^{21} - 4512769265396529128088576x^{20} + 11546134536650775044859648x^{19} - 25052844127927284357151488x^{18} + 46120547173023714432494592x^{17} - 72002596612591111053052800x^{16} + 95199167018173601085387456x^{15} - 106357485558642750786858048x^{14} + 100078973730597608483119488x^{13} - 78970049026910168467295136x^{12} + 51958955637812070724883328x^{11} - 28299178126805457249292896x^{10} + 12640465685125959112475328x^{9} - 4575645926936732962787328x^{8} + 1321740712875893316349680x^{7} - 298567190658186756100976x^{6} + 51320083437219286364736x^{5} - 6461987207673914870592x^{4} + 563746426651493261606x^{3} - 31198295910054895890x^{2} + 932905167417746466x - 10118390704879427.$

$B(8)$ $P = 9394859377925554176x^{44} - 117338811135249560371 2x^{43} + 7144807732888287471 2064x^{42} - 27800159265999944763 31008x^{41} + \ldots - 66656693571608222649303393 18368x^{3} + 2499313015801108062887218939 36x^{2} - 5235606039815235509102372752x + 4205310339771802512967 3369.$

$B(9)$ $66586065841047365222400000000x^{55} - 10780627559211573832581120000000x^{54} + \ldots + 2601172009221349492583064091221971 97946x - 1638075168736052964113158952499236561.$

$B(10)$ $146357576070007357440000000000x^{60} + 2861715112497504898252800000000x^{59} + \ldots + 19018388052875975899050853234577100131 0144x + 10437184579716588277390655645856232 35937.$

$C(1)$ $Q = x^3 - x^2 + 5x + 1,$

$P = 45x^3 + 273x^2 + 791x + 427.$

$C(2)$ $Q = x^6 - 3x^5 + 4x^3 + 3x^2 - 9x - 8,$

$P = 175x^6 + 2430x^5 + 19017x^4 + 64068x^3 + 96849x^2 + 65502x + 14103.$

$C(3)$ $P = 4465125x^{10} + 114448950x^9 + 1717178265x^8 + 13590342216x^7 + 64780856250x^6 + 190045721668x^5 + 345207245482x^4 + 376373703112x^3 + 232122416801x^2 + 72368288630x + 8271649661.$

$C(4)$ $P = 46414974375x^{15} + 1935912990375x^{14} + 47642771951775x^{13} + 679387553811135x^{12} + 6409498796289459x^{11} + 41441755477203315x^{10} + 186714655833929691x^9 + 592398220222283579x^8 + 1329789279364354133x^7 + 2109332508307537877x^6 + 2342269666378397405x^5 + 1783536720101601725x^4 + 896749201669458449x^3 + 278709535385588177x^2 + 47252708713917161x + 3194956880159369.$

$C(5)$ $P = 33990957x^{20} + 2066170260x^{19} + 74666366110x^{18} + 1631856979620x^{17} + 24611630588625x^{16} + 266019245095440x^{15} + 2109653107162920x^{14} + 12489093935915280x^{13} + 55920663405670730x^{12} + 190918816431017880x^{11} + 498880666211503668x^{10} + 997491312345752120x^9 + 1519957436433127770x^8 + 1751012290740378960x^7 + 1506000289549705640x^6 + 949210838451943632x^5 + 426524139389956425x^4 + 131002511542763380x^3 + 25680204113378910x^2 + 2831323762830660x + 128953327629845.$

$C(6)$ $P = 12714083695698776015625x^{28} + 1120748524109664262312500x^{27} + \dots +$
$407530111261671567203245308353428x + 12528354714335602493796372103577.$

$C(7)$ $438120013555654794702228515625x^{36} +$
$52159336887503771380534767187500x^{35} +$
$\dots +$
$7049731770073321764690143539043276665428876x +$
$158320694832222900012097032628451757776249.$

$C(8)$ $19978981326387509765625x^{42} +$
$2983185126665458558593750x^{41} +$
$\dots +$
$27879339953976590435166859062127141462x +$
$488342166322371232909880230533140041.$

$C(9)$ $3943988517696329309474874414036059896739501953125x^{55} +$
$778311923110674963236504321809947069645837158203125x^{54} +$
$\dots +$
$1339528345709395891100601544080319508719136732164912389838408109507.$

IV.3.3 Remarques

a. Groupe de monodromie

Nous pouvons assez facilement calculer le groupe de monodromie de ces arbres ; pour les arbres irréductibles c'est le groupe alterné (pour $A(k)$ et $C(k)$ avec k pair) ou le groupe symétrique (pour $B(k)$ et les autres $A(k)$ et $C(k)$).

Si nous notons G_N le groupe engendré par les deux permutations $(1, 2, ..., N)$ et $(1, 2, 3)$, ce groupe est $\mathfrak{S}_N$ si N est pair et $\mathcal{A}_N$ si N est impair. Nous montrons ci-dessous que le groupe de monodromie de tout Y-arbre irréductible contient G_N, et la signature de σ_0 et σ_1 permet de conclure.

Pour les $Y_{1,1,N-2}$, la permutation σ_∞ est un cycle de longueur N, par exemple $(1, 2, ..., N)$ et la permutation σ_0^2 est alors le cycle $(1, 2, 3)$. Pour les $Y_{2,2,2k+1}$, si $\sigma_\infty = (1, 2, ..., 2k+5)$, alors σ_0^2 est le cycle $(1, 3, 5)$. Comme la longueur de σ_∞ est impaire, $\sigma_\infty^2 = (1, 3, 5, ...)$ est aussi un cycle de longueur $2k+5$. On voit d'ailleurs que cette construction ne marche pas avec les $Y_{2,2,2k}$, pour lesquels la longueur du cycle de σ_∞ est un nombre pair. Ce sont des Y-arbres de type D dont le groupe de monodromie est le carré du groupe de monodromie de $Y_{1,1,k}$.

b. Les arbres $Y_{1,1,2k+1}$

Pour $k \leqslant 12$, le nombre premier 2 ne se ramifie pas dans le corps des modules. Cette particularité n'a pas de preuve élémentaire.

IV.4 Divers dessins

IV.4.1 Dessins *esthétiques*

Le plus célèbre est sans conteste le *bonhomme* dont il existe deux variantes : un dessin propre de degré 14 et un dessin de degré 8 (le *petit bonhomme* de la figure II.5).

Les 10 dessins de même valence que le bonhomme de degré 14 sont conjugués, ils sont définis sur un corps de discriminant $d(\mathbb{K}) = 2^8 3^5 5^2 7^1 11^2 13^8$, $P = 1323x^{10} - 119826x^9 + 6988572x^8 - 222996780x^7 + 4891137480x^6 - 43596377072x^5 + 170896287880x^4 - 348444339716x^3 + 374432911288x^2 - 155498695280x + 25675962256$ (voir aussi le polynôme unitaire de [37, p76]).

IV.4.2 Distance entre sommets adjacents

Les familles d'arbres ci-dessous montrent la ressemblance géométrique entre des dessins ayant une ressemblance combinatoire.

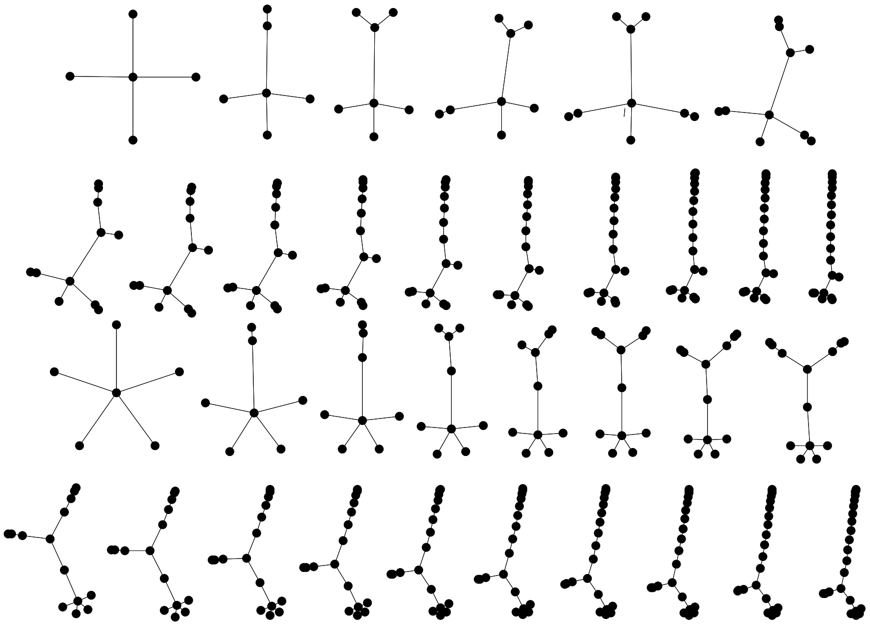
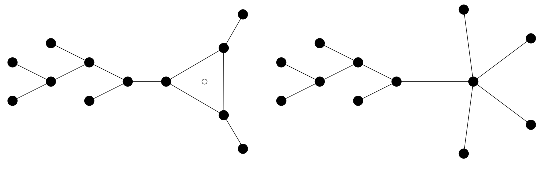


FIG. IV.2 – *Familles d'arbres*

Les deux dessins ci-desssous (vrai et faux extraterrestre) sont presque superposables (voir figure IV.3). Leur structure combinatoire est en effet assez proche, mais leurs propriétés algébriques sont radicalement différentes. Ce type de ressemblance reste mystérieux.



IV.4.3 Exemple résistant à la résolution formelle

L'exemple ci-dessous (figure IV.4) que j'appelle le *Bouddha* (voir aussi figure I.2), m'a été fourni par N. Magot. Il se résout très simplement en quatre étapes.

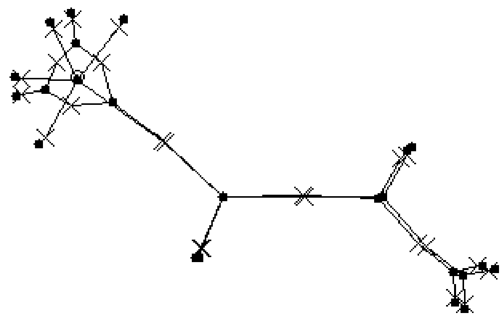


FIG. IV.3 – *Mélange du vrai et du faux extraterrestre.*

Je calcule un dessin de valences $[3\,1\,4^2;\,4^3;\,2^5 1^2]$ plutôt que le dessin de valences $[1\,3\,4^2;\,4^3;\,2^5 1^2]$ (remarquer le changement du choix de la face à l'infini) pour une meilleure stabilité numérique.

Le système III.3 résiste à une résolution par bases de Gröbner car la variété a des composantes parasites.

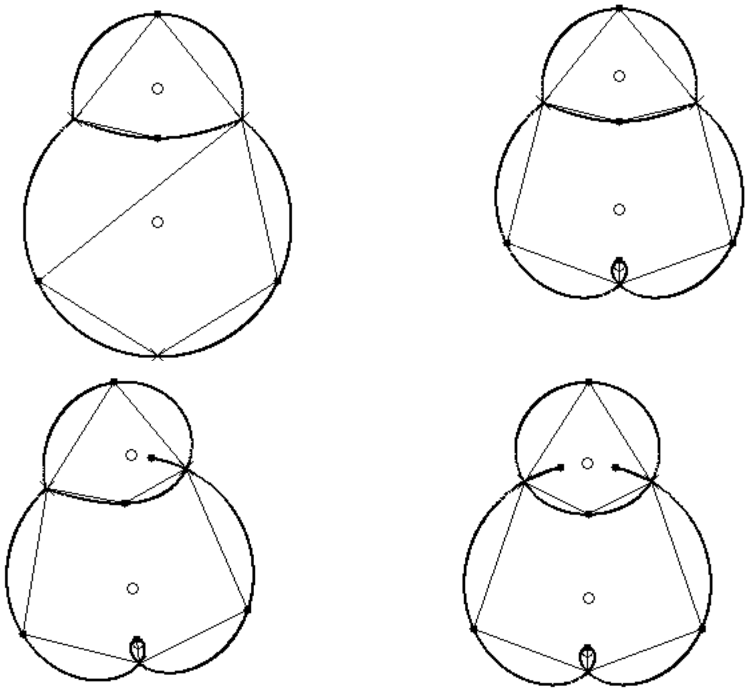


FIG. IV.4 – *Bouddha : les quatre étapes du calcul.*

Son corps des modules est défini par $x^4 - 2x^3 - 2x + 1$, il est de discriminant $-2^6 3^3$ (remarquer que ce corps de degré 4, qui est aussi $\mathbb{Q}(\sqrt[4]{12})$, n'est pas dans la liste de Malle [30]).

IV.5 Les groupes de Mathieu

IV.5.1 Contexte

Les propriétés axiomatiques définissant un groupe fini sont élémentaires et pourtant la classification des objets vérifiant ces propriétés est vraisemblablement le théorème le plus touffu des mathématiques. On commence par considérer les sous-groupes distingués (ceux qui sont stables par conjugaison). Il reste à classifier les groupes sans sous-groupes distingués, qu'on appelle **groupes simples**. Ceux-ci sont les groupes cycliques d'ordre premier, les groupes alternés (de degré 5 ou plus), les groupes de Chevalley et groupes de Chevalley "twisted", le groupe de Tits et les 26 groupes **sporadiques**.

Les cinq groupes de Mathieu (M_{11}, M_{12}, M_{22}, M_{23} et M_{24}) sont des groupes sporadiques. On peut en trouver des définitions comme groupes de permutations dans [45] et [12].

IV.5.2 Dessin correspondant à $Aut(M_{22})$

J'ai calculé par ma méthode numérique le revêtement utilisé par Malle [29] pour réaliser $Aut(M_{22})$ comme groupe de Galois sur $\mathbb{Q}(T)$. Ce calcul a été un peu plus difficile que les précédents car il y a de nombreuses étapes pour construire ce dessin. Il faut choisir soigneusement la façon dont on rajoute des points pour ne pas déséquilibrer la géométrie des étapes intermédiaires. Voir figures IV.10, IV.11, IV.12 et IV.13. Le temps de calcul est négligeable, puisque le dessin final (marqué avec une face à l'infini) est défini sur $\mathbb{Q}(\sqrt{-11})$.

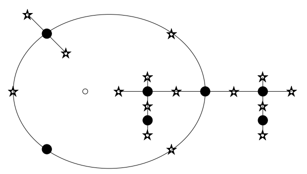


FIG. IV.5 – *$Aut(M_{22})$: aspect combinatoire du dessin.*

On peut facilement vérifier sur la figure IV.5 que la monodromie $(\sigma_\infty, \sigma_0, \sigma_1)$ du revêtement est dans les classes $11A$, $4C$ et $2B$ et engendre bien le groupe $Aut(M_{22})$.

$\sigma_\infty = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)(12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22)$,

$\sigma_0 = (1, 9, 3, 2)(4, 8, 17, 21)(5, 20, 19, 6)(12, 22, 16, 13)(7, 18)(10, 11)(14, 15)$,

$\sigma_1 = (3, 8)(4, 20)(6, 18)(7, 17)(9, 11)(13, 15)(16, 21)(1)(2)(5)(10)(12)(14)(19)(22)$.

IV.5.3 Dessins correspondant à M_{24}

"The group M_{24} is one of the most remarkable of all finite groups" [13], en particulier parce qu'il intervient dans la structure des autres groupes sporadiques. On s'intéresse donc au calcul de dessins dont la monodromie engendre M_{24}.

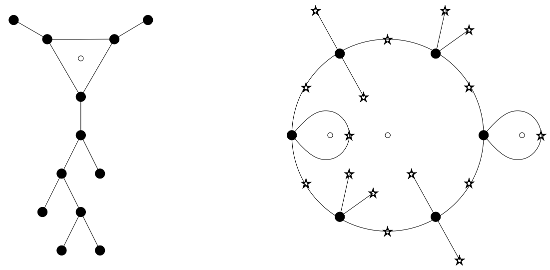


FIG. IV.6 – M_{24} : *extraterrestre et dessin de Conder.*

Le premier dessin (propre) de la figure IV.6, que Zvonkine a appelé *extraterrestre*, définit une extension de $\mathbb{Q}(T)(\sqrt{-7})$ de groupe de Galois M_{24}. La monodromie est :

$\sigma_\infty = (1,2,3)(4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24)$,

$\sigma_0 = (1,7,5)(2,4,23)(3,22,8)(9,21,19)(10,18,12)(13,17,15)$,

$\sigma_1 = (1,4)(2,22)(3,7)(5,6)(8,21)(9,18)(10,11)(12,17)(13,14)(15,16)(19,20)(23,24)$.

Conder [12] donne une définition de M_{24} qui correspond à un revêtement de genre 0 défini sur le corps de degré 5 de discriminant $-2^3 11^3 23$ et de polynôme générateur $X^5 - X^4 - X^2 - 4X + 4$. Le dessin correspondant est le second de la figure IV.6.

IV.5.4 Revêtement correspondant à M_{24}

a. Rationalité

Matzat [33] a prouvé, à partir de calcul dus à F. Häfner, qu'il existe une extension régulière de $\mathbb{Q}(T)$ de groupe de Galois M_{24}, ramifiée au dessus de quatre points. Il n'avait pas réussi à le calculer explicitement, ce que nous avons mené à bien (voir l'article [23]).

La preuve de l'existence d'un modèle rationnel de ce revêtement est compliquée, elle permet de savoir que le calcul explicite du revêtement peut effectivement aboutir à un modèle rationnel, mais elle n'est pas nécessaire pour mener ces calculs à terme.

Comme le revêtement correspondant à cette extension de $\mathbb{Q}(T)$ n'a pas de célibataire, nous obtiendrons d'abord un modèle sur $\mathbb{Q}(i)$. Nous en déduisons ensuite un modèle sur $\mathbb{Q}$, le polynôme $P \in \mathbb{Q}(T)[u]$ ci-dessous :

$$P(u) = (1+u^2)B(u)^2 + (T - A(u))^2$$

avec $A(u) =$
$115641803437317009004628044535281448962593335543045088145221615616u^{12} +$
$626355604609903799744911431879812361696225381618360944350772330496u^{11} +$
$857783185877096409511863319468234125688211122856849368609978318848u^{10} +$
$880807408611151325465045992722903978345973433532263965887299584 00u^9 -$
$204436057943295143469297637444439470087926257167240991358642431590 4u^8 -$
$547514372289055882188598064185449906818636190525525070386730074112 0u^7 -$
$791509819476082182314254656935347211621995489777715556924768738508 8u^6 -$
$860626148589107016085701786430019544933089591341674867206096771686 4u^5 -$

$6892242684910426245304385038953482144305957644307673212590062039792u^4-$
$4211432359386694117643177642371531969039977445473402080794314842304u^3-$
$1872082062997662285544516575637661132224190147802824412182076667540u^2-$
$535658851956460224909548877202498831723299104598077260690473552648u-$
$10539752687297944130116169432500844400960251281699137159101902851925/108$
et $B(u)=$
$497930855073541362607491227688032103381849370443591345788311044096u^{10}+$
$2247466124279729012772791671105119975141086793312284796250730004480u^9+$
$4511506352550421307509247841822653344621269494040738994345402695680u^8+$
$6412425694206308627270788749164116952920226584905116935357763420160u^7+$
$6416753127617241617644191979736728938801492606944566101914795376640u^6+$
$4464975149990471124875637674124629993019905811395113462955040856064u^5+$
$2003277439178423819468870064822584402702435670423637216226474276864u^4+$
$1387773461012475714244303645318594139233416068249978437106475427 84u^3-$
$3809562734971144467315146327392108281779107480309715398124321834 56u^2-$
$2815102872986447180702587652581905306098845966627302221930003120 96u-$
$6557975116213973228922906510377485833875923610261918314466448071 6.$

b. Éclatement de la singularité

Nous connaissons la monodromie $(\sigma_a, \sigma_b, \sigma_c, \sigma_d)$ du revêtement. Nous en déduisons la monodromie $(\sigma_a, \sigma_t = \sigma_b\sigma_c, \sigma_d)$ d'un revêtement dégénéré, où les valeurs de ramification correspondant à b et c sont confondues.

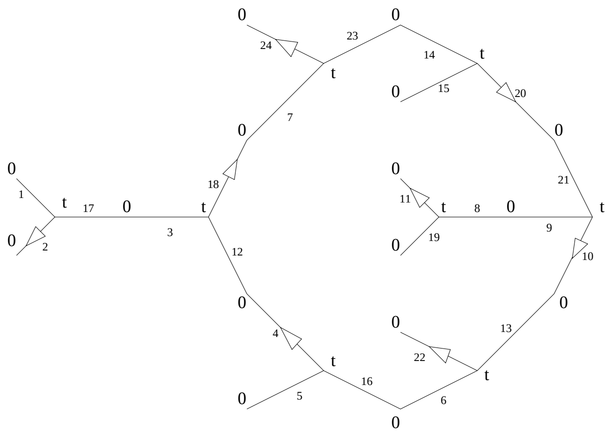


FIG. IV.7 – M_{24} : $\tilde{\varphi}^{-1}([0,t])$ *pour un revêtement dégénéré, avec flèches indiquant la direction d'éclatement des singularités*

Lorsque nous "éclatons" la singularité en t, chaque point au dessus de la valeur de ramification t se sépare en plusieurs points de ramification au dessus de b ou c. Leur nombre dépend de leurs valences, et la direction de l'iclatement est une conséquence de la façon dont sont mélangées les orbites des permutations σ_b et σ_c.

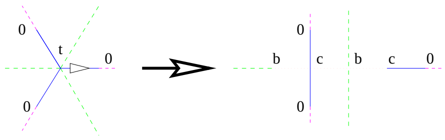


FIG. IV.8 – *Éclatement des singularités.*

c. Calcul de nombreuses solutions

Le paramètre (non rationnel) de la famille de Hurwitz le plus simple à manipuler est la position relative des quatre valeurs de ramification. Nous pourrions utiliser le birapport de ces valeurs, mais il est encore plus simple, et pas moins efficace, de fixer une de ces valeur à ∞ et de bouger (presque) indifféremment les trois autres.

Sachant que 144 (c'est ici la valeur de $l^i_{\mathfrak{C}}$) revêtements correspondent à chaque position des valeurs de ramification, nous faisons agir (progressivement) le groupe de tresses à quatre brins pour obtenir la description de tous ces revêtements. En pratique, nous fixons un des trois points mobile, nous faisons tourner les deux autres l'un autour de l'autre, puis nous changeons de point fixé.

d. Recherche d'un paramètre de la famille de revêtements

La méthode décrite au paragraphe I.3.4.e. permet de trouver un paramètre rationnel d'une courbe. Mais, dans le cas qui nous intéresse, lorsque nous avons fixé $0 \to 0$, la variété solution du système est de dimension 2. L'un des degrés de liberté correspond au paramètre de la famille de Hurwitz, l'autre à l'échelle du dessin.

Pour trouver le paramètre qui nous intéresse, nous supprimons l'influence du paramètre d'échelle en ne considérant que des fonctions ξ des variables du système qui soient invariantes par changement d'échelle.

Nous avons construit une fonction ξ_P et une fonction ξ_Q, fonctions symétriques des variables correspondant aux points de ramification d'ordre 2 (pour ξ_P) ou 1 (pour ξ_Q). Une relation polynomiale de degré 4 définit la courbe où vit le couple (ξ_P, ξ_Q). Nous trouvons un paramètre ζ de cette courbe.

Ensuite, nous avons choisi une fonction $\tilde{\xi}_P$ qui rompt la symétrie de la construction de ξ_P. Nous trouvons une relation polynomiale entre ζ et $\tilde{\xi}_P$ qui, après désingularisation, donne un paramètre t. C'est un paramètre rationnel du revêtement.

Il suffit donc de donner une valeur rationnelle à t et de calculer le revêtement correspondant pour avoir un point rationnel de la famille, et donc une extension de $\mathbb{Q}(T)$.

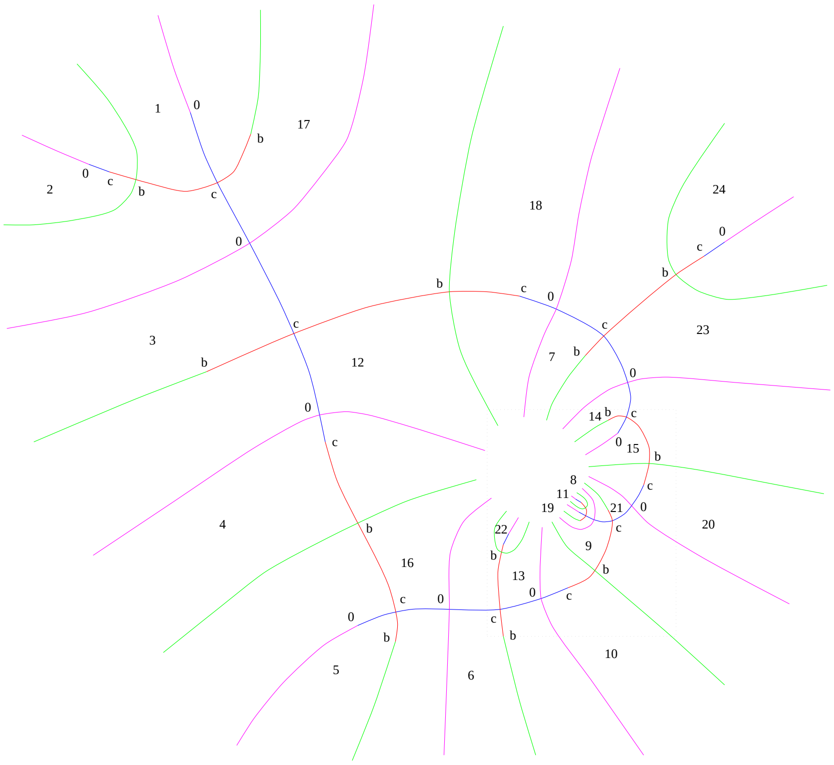


FIG. IV.9 – M_{24} : *le revêtement final*

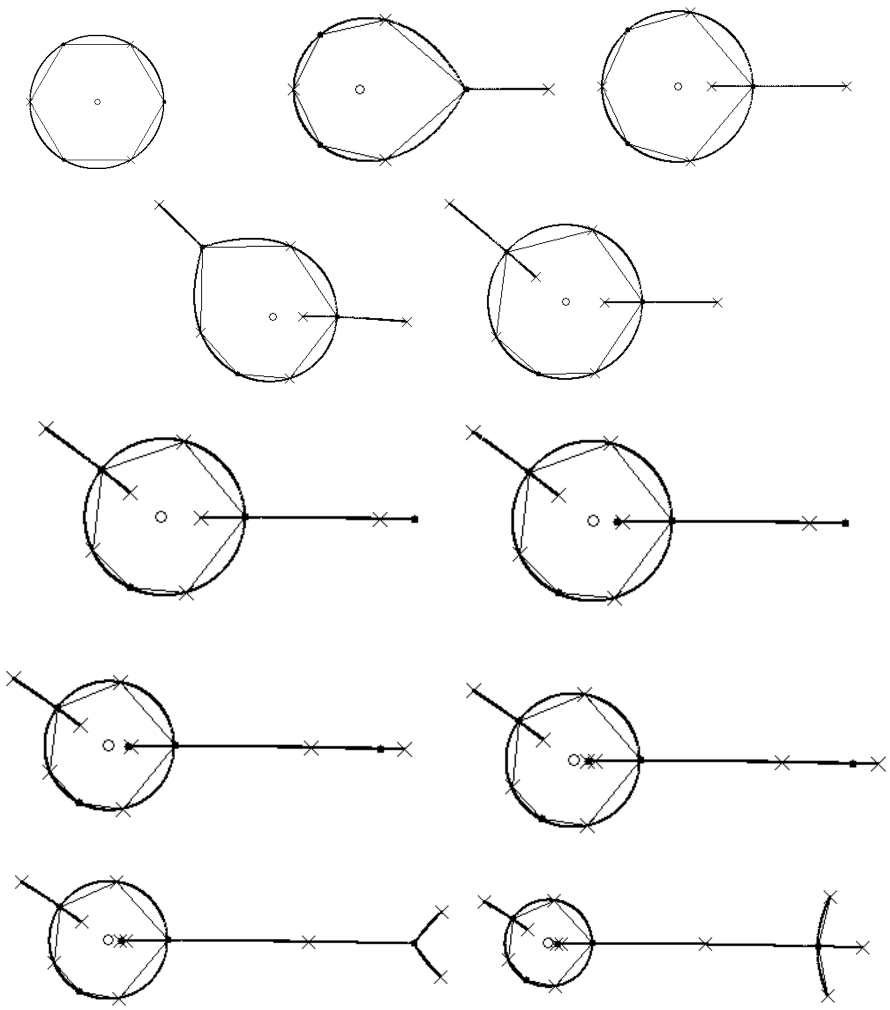


FIG. IV.10 – $Aut(M_{22})$: *onze premières étapes.*

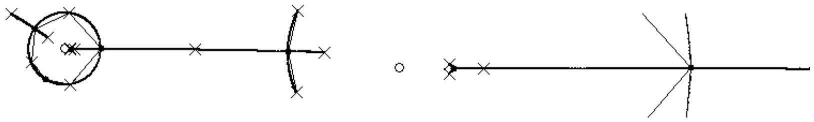


FIG. IV.11 – $Aut(M_{22})$: *douzième étape avec angrandissement du centre.*

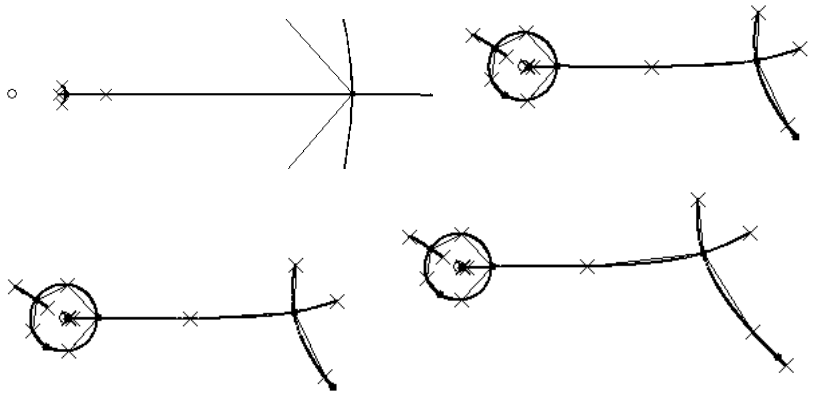


FIG. IV.12 – $Aut(M_{22})$: *treizième à seizième étapes.*

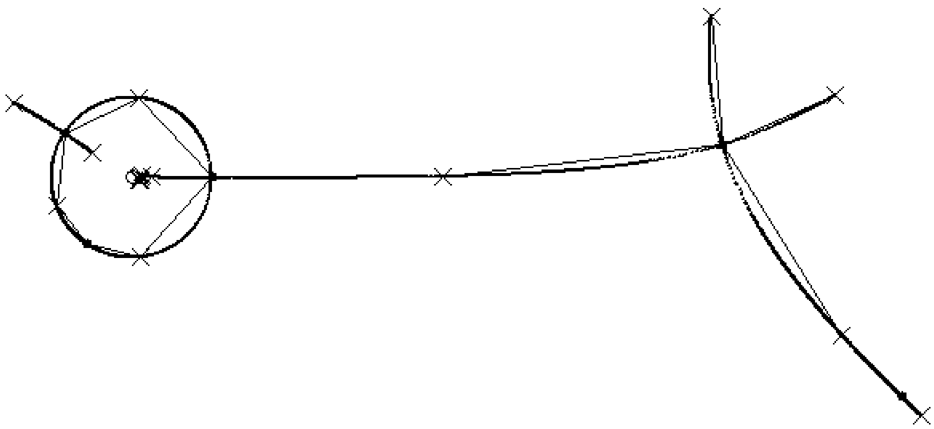


FIG. IV.13 – $Aut(M_{22})$: *dessin final.*

Annexe A

Logiciels de calcul de bases de Gröbner

A.1 Calcul du système

a. Avec Maple

Le fichier `dessins.mp` ci-dessous définit la procédure `systeme` qui calcule les équations du système III.3 à partir de la factorisation des polynômes P, Q et R.

La commande `gbasis` du package `grobner` résout ensuite ce système. La solution se présente sous la forme d'une liste dont chaque élément décrit une composante irréductible, sous forme triangulaire.

```
systeme := proc (Pv, Qv, Rv)
local v, P, Q, R, P0, Q0, R0, P1, Q1, R1,
      eq0, eq1, sys, i;
description `Calcul pour un dessin de genre 0`;
  P:=mul(Pv[i*2-1]^Pv[i*2],i=1..(nops(Pv)/2));
  Q:=mul(Qv[i*2-1]^Qv[i*2],i=1..(nops(Qv)/2));
  R:=mul(Rv[i*2-1]^Rv[i*2],i=1..(nops(Rv)/2));
  v:=degree(P);
  P0:=mul(Pv[i*2-1],i=1..(nops(Pv)/2));
  Q0:=mul(Qv[i*2-1],i=1..(nops(Qv)/2));
  R0:=mul(Rv[i*2-1],i=1..(nops(Rv)/2));
  P1:=factor(diff(P,x))*P0/P:
  Q1:=factor(diff(Q,x))*Q0/Q:
  R1:=factor(diff(R,x))*R0/R:
  eq0:=collect(P1*R0-P0*R1-v*Q/Q0,x):
  eq1:=collect(Q1*R0-Q0*R1-v*P/P0,x):
  sys:=[coeffs(eq0,x),coeffs(eq1,x)]:
end:
```

b. Avec MuPAD

La syntaxe est proche de celle de Maple. Le système est résolu avec la commande `gbasis` du package `groebner`. On demande une résolution pour l'ordre lexicographique (`LexOrder`) qui fournit un système triangulaire.

Dans le fichier **dessins.mb** ci-dessous, nous devons redéfinissons **Factor** qui est buggué dans la version 1.3 de MuPAD.

```
FFactor := proc (pol)
begin
  if (pol = 0) or (pol = 1) or (pol = -1)
  then pol:
  else Factor(pol):
  end_if:
end_proc:

MkPol := proc (v)
local p, q, i;
begin
  p := 1: q := 1: i := 1:
  while i < nops(v) do
    p := p * v[i]^v[i+1]:
    q := q * v[i]:
    i := i + 2:
  end_while:
  [p,q]:
end_proc:

systeme := proc (Pv, Qv, Rv)
local v, P, Q, R, P0, Q0, R0, P1, Q1, R1,
      eq0, eq1, sys, mk;
begin
  mk:=MkPol(Pv): P:=mk[1]: P0:=mk[2]:
  mk:=MkPol(Qv): Q:=mk[1]: Q0:=mk[2]:
  mk:=MkPol(Rv): R:=mk[1]: R0:=mk[2]:
  v:=degree(P):
  P1:=FFactor(diff(P,x))*P0/P:
  Q1:=FFactor(diff(Q,x))*Q0/Q:
  R1:=FFactor(diff(R,x))*R0/R:
  eq0:=P1*R0-P0*R1-v*Q/Q0:
  eq1:=Q1*R0-Q0*R1-v*P/P0:
  sys:=[coeff(eq0,[x]),coeff(eq1,[x])]:
end_proc:
```

c. Avec GB

Les équations du système sont calculées avec Maple par exemple. Dans la session GB, on calcule d'abord avec **tgroebner** une base pour l'ordre du degré, qui est ensuite transformée avec **totolex** en un système triangulaire.

A.2 Application aux arbres en Y de type B

a. Formalisation

Ce sont les dessins dont la liste des valences est $[2n+4;\ 3\,2^n 1;\ 2^{n+1}1^2]$ (voir aussi § IV.3). Il y a $2n+5$ inconnues qui sont les coefficients des polynômes P et Q.

$$P(x) \quad = \quad (x+p_a)^3(x+p_b)(x^n+p_cx^{n-1}+...)^2$$

$$Q(x) \quad = \quad (x^2 + q_a x + q_b)(x^{n+1} + q_c x^n + ...)^2$$

Pour fixer la position du dessin dans $\mathbb{P}_1\mathbb{C}$, nous imposons la position de deux célibataires : le sommet $\bullet$ de valence 3 est en 0 et le sommet $\bullet$ de valence 1 est en 1. Nous fixons donc $p_a = 0$ et $p_b = -1$.

b. Calcul de $B(5)$ avec MuPAD

Il y a 21 arbres ayant cette liste de valences. Le calcul montre que tous sont conjugués.

```
   *----*    MuPAD 1.3  ---  Multi Processing Algebra Data Tool
  /|   /|
 *----* |    Copyright (c) 1992-96 by B. Fuchssteiner, Automath
 | *--|-*    University of Paderborn.  All rights reserved.
 |/   |/
 *----*      Demo version, please register with
             MuPAD-distribution@uni-paderborn.de
>> read("dessins.mb"):
>> sys:=systeme(
&> [x,3, x-1,1, x^5+pc*x^4+pd*x^3+pe*x^2+pf*x+pg,2],
&> [x^2+qa*x+qb,1, x^6+qc*x^5+qd*x^4+qe*x^3+qf*x^2+qg*x+qh,2],
&> []):
>> time((sol:=groebner::gbasis(sys,LexOrder)));
                                   37000
>> degree(sol[2]);
                                    21
```

c. Calcul de $B(5)$ avec Maple

```
    |\^/|     Maple V Release 4 (Ecole normale superieure)
._|\|   |/|_. Copyright (c) 1981-1996 by Waterloo Maple Inc. All rights
 \  MAPLE  /  reserved. Maple and Maple V are registered trademarks of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
> read `dessins.mp`;
> sys:=systeme(
> [x,3, x-1,1, x^5+pc*x^4+pd*x^3+pe*x^2+pf*x+pg,2],
> [x^2+qa*x+qb,1, x^6+qc*x^5+qd*x^4+qe*x^3+qf*x^2+qg*x+qh,2],
> []):
bytes used=1000256, alloc=851812, time=0.66
> sol:=grobner[gsolve](sys):
bytes used=2001020, alloc=1179432, time=1.69
bytes used=3001316, alloc=1376004, time=3.17
(...)
bytes used=41264396, alloc=2948580, time=41.59
bytes used=42298668, alloc=2948580, time=41.99
> lprint(degree(sol[1][13]));
21
```

d. Calcul de $B(8)$ avec GB

Il y a 45 arbres ayant cette liste de valences. L'un d'entre eux est le quintuple de $B(0)$. Le calcul montre que les 44 autres sont conjugués.

On a calculé les équations du système avec Maple par exemple.

```
> read `dessins.mp`;
> sys:=systeme(
> [x,3, x-1,1, x^8+pa*x^7+pb*x^6+pc*x^5+pd*x^4+pe*x^3+pf*x^2+pg*x+ph,2],
```

```
> [x^2+qa*x+qb,1,
>    x^9+qc*x^8+qd*x^7+qe*x^6+qf*x^5+qg*x^4+qh*x^3+qi*x^2+qj*x+qk,2],
> []):
```

La session GB ressemble à ce qui suit.

```
Grobner Basis Computations (C++ version) (ASAP)
Author:Jean-Charles Faugere ***  CNRS & Universite Paris 6/LITP - IBP ***
Working directory /users/grecc/granboul
GB> S1:=-3*ph-20*qk;
GB> S2:=-20*qj-5*pg+4*ph;
GB> S3:=-19+18*pa-20*qc;
GB> S4:=16*pb-17*pa-20*qd;
GB> S5:=14*pc-20*qe-15*pb;
GB> S6:=-20*qf-13*pc+12*pd;
GB> S7:=-11*pd-20*qg+10*pe;
GB> S8:=-20*qh+8*pf-9*pe;
GB> S9:=-20*qi+6*pg-7*pf;
GB> S10:=2*qb*qj+qa*qk;
GB> S11:=4*qb*qi+3*qa*qj+2*qk;
GB> S12:=18*qb-20*pb+17*qa*qc+16*qd;
GB> S13:=-20*pc+15*qa*qd+14*qe+16*qb*qc;
GB> S14:=12*qf+13*qa*qe+14*qb*qd-20*pd;
GB> S15:=-20*pe+11*qa*qf+10*qg+12*qb*qe;
GB> S16:=8*qh-20*pf+9*qa*qg+10*qb*qf;
GB> S17:=8*qb*qg-20*pg+7*qa*qh+6*qi;
GB> S18:=5*qa*qi+6*qb*qh+4*qj-20*ph;
GB> S19:=19*qa-20*pa+18*qc;
GB>
GB> D:=HDMP([qk,ph,qj,pg,qi,pf,qh,pe,qg,pd,qf,pc,qe,pb,qd,qa,pa,qc,qb],INT);
GB> S:List(D)
GB> S:=[S1,S2,S3,S4,S5,S6,S7,S8,S9,S10,S11,S12,S13,S14,S15,S16,S17,S18,S19];
GB>
GB> g:=tgroebner(S);
(...)
End of modular computation (5.75 sec)
(...)
End of gbasis computation (1.60 sec)!
End of minimal gbasis computation !
    a) done in 1.93 sec + 5.75 sec
b) Check that input polynomials are in gbasis ...done in 0.00 sec
c) Check that gbasis is a groebner basis
(...)
End of gbasis computation (17.24 sec)!
    c) done in 17.28 sec
GB>
GB> dimension(g)
       45
                   Type: Integer
GB>
GB>
GB> h:=totolex(g);
(...) [94 minutes et 46 Mo]
GB> size(h)
       19
                   Type: Integer
GB> h.19
(...) [un polynôme de degré 45]
```

Ensuite, ce polynôme est factorisé en 6 minutes et 18 Mo avec Pari-GP. Ses facteurs sont de degré 1 et 44.

Bibliographie

[1] Adrianov (N.) et Shabat (G.). – Singularities of moduli spaces, Galois cartography and finite projective geometry. In *Geometric Galois Actions, vol. 1* [39].

[2] Atkin (A.) et Swinnerton-Dyer (H.). – Modular forms on non-congruence subgroups. In *Proc. Symp. Pure Math. XIX*, pp. 1–25. – AMS, 1971.

[3] Bauer (M.) et Itzykson (C.). – Triangulations. In *The Grothendieck theory of Dessins d'Enfants* [38], pp. 179–236.

[4] Beckmann (S.). – Ramified primes in the field of moduli of branched covering of curves. *J. Algebra*, vol. 125, 1989, pp. 236–255.

[5] Belyi (G.). – On Galois extensions of the maximal cyclotomic field. *Izvestiya Ak. Nauk. SSSR, ser. mat.*, vol. 43, n° 2, 1979, pp. 269–276. – (en russe. Version américaine : *Math. USSR Izv.* vol. 14, 1979, pp. 247–256).

[6] Belyi (G.). – *Another proof of three points theorem.* – Rapport interne, MPI 97-46, Max Planck Institute, Bonn, avril 1997.

[7] Birch (B.). – Noncongruence subgroups, covers and drawings. In *The Grothendieck theory of Dessins d'Enfants* [38], pp. 25–46.

[8] Bétréma (J.), Péré (D.) et Zvonkin (A.). – *Plane trees and their Shabat polynomials (catalog).* – Rapport interne, LABRI 92-75, Bordeaux, 1992.

[9] Bétréma (J.) et Zvonkin (A.). – La vraie forme d'un arbre. In *Proc. TAPSOFT'93*, éd. par Gaudel (M.) et Jouannaud (J.-P.), pp. 599–612.

[10] Buchberger (B.). – Gröbner bases : an algorithmic method in polynomial ideal theory. In *Multidimensional systems theory*, éd. par Bose (N.-K.), chap. 6, pp. 184–232. – D. Reidel Pub. Co., 1985, *Mathematics and its Applications* 16.

Reprenant les idées de sa thèse : *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, U. Innsbruck, Autriche, 1965.

[11] Cohen (H.). – *A course in computational algebraic number theory.* – Springer, 1993, *GTM* 138.

[12] Conder (M.). – Generating the Mathieu groups and associated Steiner systems. *Discrete Mathematics*, vol. 112, 1993, pp. 41–47.

[13] Conway (J. H.), Curtis (R. T.), Norton (S. P.), Parker (R. A.) et Wilson (R. A.). – *Atlas of finite groups.* – Clarendon Press, 1985.

[14] Coombes (K.) et Harbater (D.). – Hurwitz families and arithmetic Galois groups. *Duke Math. J.*, vol. 52, 1985, pp. 821–839.

[15] Cori (R.). – *Un code pour les graphes planaires et ses applications.* – SMF, 1975, *Astérisque* 27.

[16] Couveignes (J.-M.). – Calcul et rationalité de fonctions de Belyi en genre 0. *Annales de l'Institut Fourier*, vol. 44, n° 1, janvier 1994, pp. 1–38.

[17] Couveignes (J.-M.) et Granboulan (L.). – Dessins from a geometric point of view. In *The Grothendieck theory of Dessins d'Enfants* [38], pp. 79–113.

[18] Dieudonné (J.). – *Éléments d'analyse – Tome III, Chapitre XVI: Variétés différentielles.* – Gauthier-Villars, 1970.

[19] Faugère (J.-C.). – *GB algebraic system.*

[20] Faugère (J.-C.), Gianni (P.), Lazard (D.) et Mora (T.). – Efficient computation of zero-dimensional gröbner bases by change of ordering. *J. Symbolic Computation*, vol. 16, 1993, pp. 329–344.

[21] Fulton (W.). – *Algebraic curves – An introduction to Algebraic Geometry.* – W.A. Benjamin, Inc., 1969, *Math. Lecture Notes.*

[22] Giovini (A.), Mora (T.), Niesi (G.), Robbiano (L.) et Traverso (C.). – One sugar cube please — or selection strategies in the Buchberger algorithm. In *Proc. ISSAC'91*, pp. 49–54.

[23] Granboulan (L.). – Construction d'une extension régulière de $\mathbb{Q}(T)$ de groupe de Galois M_{24}. *Experimental Math.*, vol. 5, n° 1, 1996, pp. 3–14.

[24] Grothendieck (A.). – Esquisse d'un programme. In *Geometric Galois Actions, vol. 1* [39]. 1984.

[25] Hironaka (H.). – Resolution of singularities of an algebraic variety over a field of characteristic zero. *Ann. Math.*, vol. 79, 1964, pp. 109–326.

[26] Jones (G.) et Singerman (D.). – Maps, hypermaps and triangle groups. In *The Grothendieck theory of Dessins d'Enfants* [38], pp. 115–145.

[27] Lazard (D.). – Solving zero-dimensional algebraic systems. *J. Symbolic Computation*, vol. 13, 1992, pp. 117–131.

[28] Lenstra (A. K.), Lenstra (H. W.) et Lovász (L.). – Factoring polynomials with rational coefficients. *Math. Ann.*, vol. 261, 1982, pp. 515–534.

[29] Malle (G.). – Polynomials with Galois groups $\mathrm{Aut}(M_{22})$, M_{22} and $\mathrm{PSL}_3(\mathrm{F}_4)$ over $\mathbb{Q}$. *Math. Comp.*, vol. 41, n° 184, oct. 1988, pp. 761–768.

[30] Malle (G.). – Fields of definition of some three point ramified field extensions. In *The Grothendieck theory of Dessins d'Enfants* [38], pp. 147–168.

[31] Matiyasevich (Y.). – Calculation of generalized chebishev polynomials on computer. *Vestnik Moskovskogo Universiteta*, n° 6, 1996, pp. 59–61. – (en russe).

[32] Matzat (B. H.). – *Konstruktive Galoistheorie.* – Springer Verlag, 1987, *Lecture Notes in Math.* 1284.

[33] Matzat (B. H.). – Rationality criteria for Galois extensions. In *Galois groups over* $\mathbb{Q}$, éd. par Ihara (Y.), Ribet (K.) et Serre (J.-P.), pp. 361–383. – Springer Verlag, 1989, *MSRI Publications* 16.

[34] Matzat (B. H.). – Braids and Decomposition Groups. In *Séminaire de Théorie des Nombres, Paris, 1991–1992*, éd. par David (S.), pp. 179–189. – Birkhäuser, 1993, *Progress in mathematics* 116.

[35] Neumaier (A.). – *Interval methods for systems of equations.* – Cambridge University Press, 1990, *Encycl. of Math. and its Applications* 37.

[36] Pakovitch (F.). – *Combinatoire des arbres planaires et arithmétique des courbes hyperelliptiques.* – Thèse de doctorat, Université de Grenoble I, 1997.

[37] Schneps (L.). – Dessins d'enfant on the Riemann sphere. In *The Grothendieck theory of Dessins d'Enfants* [38], pp. 47–77.

[38] Schneps (L.) (éditeur). – *The Grothendieck theory of Dessins d'Enfants.* – Cambridge University Press, 1994, *Lecture Notes in Math.* 200.

[39] Schneps (L.) et Lochak (P.) (éditeurs). – *Geometric Galois Actions, vol. 1 — Around Grothendieck's* Esquisse d'un Programme. – Cambridge University Press, 1997, *Lecture Notes in Math.* 242.

[40] Schneps (L.) et Lochak (P.) (éditeurs). – *Geometric Galois Actions, vol. 2 — Anabelian Geometry.* – Cambridge University Press, 1997, *Lecture Notes in Math.* 243.

[41] Serre (J.-P.). – *Topics in Galois theory.* – Jones and Bartlett, 1992, *Research Notes in Math.* 1. Notes written by Henri Damon.

[42] Shabat (G.). – On the classification of plane trees by their galois orbits. In *The Grothendieck theory of Dessins d'Enfants* [38], pp. 169–177.

[43] Shabat (G.) et Voevodsky (V.). – Drawing curves over number fields. In *The Grothendieck Festschrift, Vol III*, pp. 199–227. – Birkhäuser, 1990, *Progress in Math* 88.

[44] Strebel (K.). – *Quadratic differentials.* – Springer, 1984.

[45] Todd (J. A.). – Abstract definitions for the Mathieu groups. *Quart. J. Math. Oxford*, vol. 21, 1970, pp. 421–424.

[46] Tutte (W. T.). – The number of planted plane trees with a given partition. *Amer. Math. Monthly*, vol. 21, 1964, pp. 272–277.

[47] Wolfart (J.). – The *obvious* part of Belyi's theorem and Riemann surfaces with many automorphisms. – août 1995. preprint.

[48] Zapponi (L.). – On dessins d'enfants of genus one. In *Geometric Galois Actions, vol. 2* [40].

[49] Zapponi (L.). – Un invariant galoisien pour une famille d'arbres. – 1997. – à paraître.

Résumé

Cette thèse est découpée en quatre chapitres. Le premier chapitre est consacré à deux méthodes de résolution de systèmes d'équations algébriques. La première repose sur le calcul de base de Gröbner, à base de manipulations exactes de polynômes. Pour la seconde méthode on approche numériquement la solution, puis on reconstitue sa définition algébrique. On utilise en particulier l'algorithme LLL de réduction de réseaux.

Le second chapitre est plus théorique. Après une brève présentation informelle, et une longue série de définitions mathématiques, nous définissons formellement les dessins en insistant sur leurs deux visages, et la correspondance (de Grothendieck) entre les deux : nous regroupons d'une part les définitions liées à leur aspect combinatoire et d'autre part celles concernant leur aspect algébrique. Nous insistons sur les nombreuses variantes et généralisations des dessins d'enfants.

Le troisième chapitre expose la principale méthode pour le calcul explicite de la correspondance de Grothendieck. Nous partons de la description combinatoire du dessin, nous définissons un système algébrique dont les solutions décrivent les propriétés algébriques et arithmétiques du dessin. Nous exposons quelques autres méthodes, appliquées dans certains cas particuliers, puis nous détaillons les avantages de la résolution numérique du système par rapport à des techniques plus algébriques.

Le quatrième chapitre donne des exemples de calculs explicites de dessins. Il commence avec les dessins les plus élémentaires, qui servent à visualiser les plus simples de ces objets, puis il continue en décrivant une série de calculs d'"arbres en Y", qui servent de prétexte à une comparaison des techniques de calcul. Nous montrons ensuite quelques dessins ayant un intérêt particulier, et nous concluons avec des calculs servant à la résolution d'instances du problème de Galois inverse.

Mots clés :

Systèmes d'équations algébriques. Réduction de réseau. Dessins d'enfants. Galois inverse.

Abstract

This document is divided in four chapters. The first chapter describes two methods for the resolution of systems of algebraic equations. They make use of elementary algebra. We begin with the definitions, stressing the problem of approximating algebraic numbers. The first method is the now classical Gröbner basis calculus. The other method computes an approximation of the solution and goes back to the (exact) algebraic properties with the help of LLL reduction.

The second chapter gives an introduction to the "dessins d'enfants". We recall quickly some basic definitions of group theory, geometry or graph theory. Then we give formal definitions of the "dessins", stressing the "Grothendieck's correspondance" between combinatoric and algebraic properties. We list the usual variants and generalisations of the dessins d'enfants.

The third chapter explains how we can build an algebraic system from the visual description of a dessin. Its solutions describe the algebraic properties of the dessin. This system can be solved with Gröbner basis, but we prefer to compute successive approximations of dessins. With that technique, we can take advantage of the geometric nature of the dessins.

The fourth chapter begins with the most simple of all dessins, as toy examples. Then we give a conjecture and computations of the number of conjugates of some specific dessin called "Y-trees". These computations show that the numeric approach for solving the systems is really competitive. We continue with some nice examples, we conclude with computations of dessins that represent regular extensions of Galois group some Mathieu group.