An introduction to dessins d'enfants

Hang Chen and Haoda Li

May, 2022

Abstract

The ideas about dessins d'enfants are originally outlined by Alexander Grothendieck in his famous program *Esquisse d'un programme*, we introduce some developments of it in this paper. Dessins d'enfants are topological and combinatorial objects that reflects rich geometric and arithmetic information. The first five sections are devoted to give an overview of the theory of dessins d'enfants. They cover topics like Belyi's theorem and the Grothendieck correspondence, along with Galois action on dessins; which shed light on the geometric and arithmetic feature of dessins d'enfants. Examples and applications are given in Section 6 and Section 7, respectively. The prerequisites needed to read the applications in Section 7 are partly covered in the appendices.

Contents

1 Introduction

The theory of dessins d’enfants is considered by Grothendieck as one of the most important discoveries he made in his mathematical career, according to Grothendieck himself in the *Esquisse d’un programme* [3]. As easily seen in the Definition 2.0.1 given in Section 2, such objects are purely of topological and combinatorial data. However, these objects contain rich geometric and arithmetic information. For example, as we shall see in Section 5 and Section 7.3, they yield interesting descriptions of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and its representations (see Corollary 5.1.4 and Theorem 7.3.2, for example). Heuristically speaking, they lead to comparisons between arithmetic Galois groups and geometric fundamental groups, which are somewhat highly nontrivial since naturally the arithmetic fundamental group is an extension of the arithmetic Galois group and the geometric fundamental group. Moreover, the theory of dessins d’enfants is considered as the starting point of the study of anabelian geometry.

An important feature of dessins d’enfants is that they correspond to étale coverings of $\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash\{0,1,\infty\}$, in particular the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on them. More precisely, the category of dessins d’enfants is equivalent to the category $\mathbf{F\acute{E}t}_{\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash\{0,1,\infty\}}$ of finite étale coverings of $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}$, which is equivalent to the category $\mathbf{FTopCov}^{\mathrm{Gal}(\mathbb{C}/\overline{\mathbb{Q}})}_{\mathbb{P}^1_{\mathbb{C}}\backslash\{0,1,\infty\}}$ of finite topological ramified coverings of $\mathbb{P}^1_{\mathbb{C}}$ defined over $\overline{\mathbb{Q}}$ and branching only at some points in $\{0,1,\infty\}$ (by Grothendieck’s Riemann existence theorem and that $\mathbb{P}^1_{\mathbb{C}}\backslash\{0,1,\infty\}$ is integral as a scheme, see [14] for details). This is called the Grothendieck correspondence, a topological constructive proof is given in Section 3.2, another proof via the cartographical group is given in Section 3.3, see Section 3 for details.

Using the topological and combinatorial datum, we may define the automorphism group $\mathrm{Aut}(\mathcal{D})$ and the monodromy group $\mathrm{Mon}(\mathcal{D})$ of a dessin $\mathcal{D}$, they coincide with the automorphism group $\mathrm{Aut}(f_{\mathcal{D}})$ and the monodromy group $\mathrm{Mon}(f_{\mathcal{D}})$ of the ramified cover $f_{\mathcal{D}}$ obtained via the Grothendieck correspondence, see Section 4 for details. They are both interesting invariants of dessins, as they are direct to compute and invariant under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, in particular they can be used to check whether two dessins are in the same Galois orbit. It is also worth mentioning that $\text{Aut}(\mathcal{D})$ is in fact isomorphic to the centralizer $Z(\text{Mon}(\mathcal{D}))$ of $\text{Mon}(\mathcal{D})$ in S_n.

There are many interesting applications of the theory of dessins d'enfants. For example, it yields a new perspective of Davenport's bound on $f^3 - g^2$, leading to a clean and short new proof of Zannier's main result in [13]. Also, we may use Belyi's theorem to show that the *abc*-conjecture implies Faltings theorem. For details, see Section 7.

2 The definition of Dessin d'enfants

Definition 2.0.1. A *dessin d'enfant*, or simply a dessin, is a pair $(X, \mathcal{D})$, where X is an oriented compact topological surface, and $\mathcal{D} \subset X$ is a finite graph such that:

(1) $\mathcal{D}$ is connected.

(2) $\mathcal{D}$ can be put a bipartite structure, namely the vertices can be marked with two distinct marks in such a way that the direct neighbors of any given vertex are all of the opposite mark.

(3) $X \setminus \mathcal{D}$ is the union of finitely many topological discs, which is called the faces of $\mathcal{D}$.

Definition 2.0.2. A clean dessin is a dessin where all the vertices with a particular mark have degree 2. And it's to be understood that in the definition of the dessin the condition (2) is removed. For a graph satisfying the conditions (1) and (3), a dessin is associated by giving all the vertices the same mark and placing a new vertex with a different mark in the middle of each edge.

Note that a dessin is more than a mere abstract graph, since it's equipped with a certain embedding in a given topological surface. The genus of a dessin $(X, \mathcal{D})$ is simply the genus of the topological surface X. When the topological surface X is clear from the context, we will denote the dessin simply by $\mathcal{D}$.

3 Grothendieck correspondence

3.1 Belyi's theorem

There's a one-one correspondence between dessin d'enfants and Belyi functions, which is the main reason why we consider the theory of dessin d'enfants. Belyi's celebrated theorem states that a Riemann surface has a Belyi's function on it if and only if it's defined over $\overline{\mathbb{Q}}$, and Belyi's functions are defined over $\overline{\mathbb{Q}}$.

Definition 3.1.1. A morphism $f : X \to \mathbb{P}^1_{\mathbb{C}}$ all of whose critical values lie in $\{0, 1, \infty\}$ is called a *Belyi morphism*. We call f clean if all the ramification orders over 1 are equal to 2.

Definition 3.1.2. If X is an algebraic curve defined over $\overline{\mathbb{Q}}$ and f is a Belyi function on it, we call the couple (X, f) a *Belyi pair*. Two Belyi pairs are said to be *equivalent* if they are equivalent as ramified coverings.

Theorem 3.1.3 (Belyi's theorem)**.** *Let S be a compact Riemann surface, then the following statements are equivalent:*

(a) X is defined over $\overline{\mathbb{Q}}$.

(b) There exists a non-constant holomorphic function $f : X \to \mathbb{P}^1_{\mathbb{C}}$ all of whose branch values lie in $\{0, 1, \infty\}$, i.e., a Belyi function.

Full proof is given in appendix, here we just prove $(a) \Rightarrow (b)$ as the construction is useful in creating some dessins. And a partly proof of $(b) \Rightarrow (a)$(different from the approach taken in appendix) is given based on a main criterion just to show maybe some insights of the theorem.

Lemma 3.1.4. *Let f be a morphism from Riemann surface S to $\mathbb{P}^1_{\mathbb{C}}$ and all critical values of f lie in $\overline{\mathbb{Q}} \cup \{\infty\}$. Then there exists a function $P : \mathbb{P}^1_{\mathbb{C}} \mapsto \mathbb{P}^1_{\mathbb{C}}$ such that $g = P \circ f$ is a Belyi function. Moreover, P can be chosen to be a polynomial.*

Proof. A general observation is given first that the following equation holds.

$$\text{Branch}(g \circ f) = \text{Branch}(g) \cup g(\text{Branch}(f)) \tag{3.1.4.1}$$

Step 1: Constructing a function only ramifies in rational numbers.

Let S be the set of all critical values of f and all their conjugates under $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If $S \in \mathbb{Q}$, go to the next step. If not, set $m_1(z) = \prod_{s \in S}(z - s) \in \mathbb{Q}[z]$. The branch values of $m_1 \circ f$ are contained in $S_1 = m_1(\{\text{roots of } m_1' \cup \{0, \infty\})$ by equation 3.1.4.1. Since $m_1' \in \mathbb{Q}[z]$, S_1 contains all the conjugates of S_1 under $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus, set $m_2(z) = \prod_{s \in S_1}(z - s) \in \mathbb{Q}[z]$, then we have $\deg m_2 \leq \deg m_1' < \deg m_1$. So we can construct $m_i \in \mathbb{Q}[z]$ recursively, and the degrees of m_i decrease successively until for some $n, \deg(m_n) = 0$. Let $h = m_{n-1} \circ m_{n-2} \circ \cdots \circ m_1 \circ f$, then all the branch values are contained in $\mathbb{Q}$.

Step 2: If there's a branch value $m/(m + n) \in \mathbb{Q} \cap (0, 1)$

Consider the *Belyi polynomial*

$$P_{m,n}(z) = \frac{(m + n)^{m+n}}{m^m n^n} z^m (1 - z)^n \tag{3.1.4.2}$$

which transforms both 0 and 1 to 0, and $m/(m + n)$ to 1. It ramifies only at the points $x = 0, 1, m/(m + n), \infty$. Hence, $\text{Branch}(P_{m,n} \circ h) = \text{Branch}(h) - \{m/(m + n)\}$. We can reduce branch values by one in $\mathbb{Q} \cap (0, 1)$ by composing h with a Belyi polynomial.

Step 3: If there are branch values in $\mathbb{Q} - [0, 1]$

Composing Möbius transformation $M(z) = 1/z$ or $M(z) = 1 - z$ can help to transform some branch values to $[0, 1]$.

After finishing step 1, we can use step 2 and step 3 alternately to obtain the wanted Belyi function. □

Proof of (a)⇒(b). Let $S = S_F$ be a compact Riemann surface where $F(X,Y) = p_0(X)Y^n + p_1(X)Y^{n-1} + \cdots + p_n(X)$. Considering the function $\mathbf{x}$: $(x,y) \mapsto x$, then $\mathrm{Branch}(\mathbf{x}) \subset \{\text{roots of } p_0\} \cup \{\text{first ordinates of common roots of } F_Y \text{ and } F\}$. By Bézout's theorem, the branch values of $\mathbf{x}$ are all in $\overline{\mathbb{Q}}$. Then by Lemma 3.1.4, the proof of this half is done. □

This approach can be applied to construct some Belyi morphisms, and then by Grothendieck correspondence some dessins.

For (b)⇒(a), a criterion for definability over $\overline{\mathbb{Q}}$ is given without proof.

Theorem 3.1.5. *Let S be a compact Riemann surface, the following conditions are equivalent:*

- *S is defined over $\overline{\mathbb{Q}}$.*
- *The family $\{S^\sigma\}_{\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})}$ contains only finitely many isomorphism classes of Riemann surfaces.*

Proof of (a)⇒(b) based on the criterion. From this criterion the proof of Belyi theorem is quickly accessed. If $f : S \to \mathbb{P}^1_{\mathbb{C}}$ is a Belyi function, then for arbitrary $\sigma \in \mathrm{Gal}(\mathbb{C})$, the degree of $f^\sigma : S^\sigma \to \mathbb{P}^1_{\mathbb{C}}$ unchanged. σ acts trivially on set $\{0, 1, \infty\}$, then f and f^σ have the same branch values. So the monodromies of f^σ have only finite possibilities when σ goes through $\mathrm{Gal}(\mathbb{C})$, which shows f^σ are in finite equivalent classes of coverings. Then apply theorem 3.1.5 to finish the proof. □

3.2 A proof via a topological construction

In the original work of Grothendieck, he only considered the clean dessins and proves the correspondence of the clean dessins and clean belyi pairs. But the proof of construction also works for the general situations. In the next section, we will introduce another proof of Grothendieck correspondence of clean dessins d'enfants by considering action of cartographical group on the set of flags of a dessin, which can also be modified to suit non-clean case.

We first construct a dessin from a Belyi pair. For a given Belyi pair (S, f), let $\mathcal{D}_f = f^{-1}[0,1]$, where $[0,1]$ is the segment of the real line on $\mathbb{P}^1_{\mathbb{C}}$, the vertices of the graph are $f^{-1}(0)$ and $f^{-1}(1)$ with different marks which equip the graph a bipartite structure. Then $(S, \mathcal{D}_f)$ is a dessin.

Proposition 3.2.1. *The dessin $(S, \mathcal{D}_f)$ satisfies the following properties:*

(1) $\mathcal{D}_f$ is a dessin d'enfant.

(2) Each face of the dessin has exactly one point in $f^{-1}(\infty)$.

(3) Each of the sets $f^{-1}[0,1]$, $f^{-1}[0,\infty]$ and $f^{-1}[1,\infty]$ is a union of topological segments. All of them together are the complete set of edges of a triangle decomposition $\mathcal{T}(\mathcal{D}_f)$ of S. This shows $\mathcal{D}_f$ satisfies the condition (1) and (3) of the definition of dessins.

(4) $\deg(f)$ *agrees with the number of edges of* $\mathcal{D}_f$*.*

(5) The multiplicity of f *at a vertex* v *of* $\mathcal{D}_f$ *coincides with the degree of the vertex. The multiplicity of a point in the set* $f^{-1}(\infty)$ *agrees with half the valency of the face where the point is.*

(6) If f *is clean,* $\mathcal{D}_f$ *is clean.*

Next, we are going to construct a Belyi pair from a given dessin $(X, \mathcal{D})$, including equipping the topological surface X with a Riemann surface structure. Suppose the two marks on the dessin are $\circ$ and $\bullet$, and the edges of the dessin are labelled with numbers from 1 to n.
Step 1: We shall first construct a triangle decomposition $\mathcal{T} = \mathcal{T}(\mathcal{D})$ of X associated to $\mathcal{D}$. Choose a *centre* in each of the faces of $\mathcal{D}$ and mark them with $\star$. For each pair (v, A) where v is a vertex in the boundary of a face A, draw a segment γ_A^v that starts at v and ends at the centre of A, and it's not allowed to meet any edge except at v it self. Then the γ_A^v divide X into some triangles, satisfying following properties:

- Every triangle contains one vertex of each type $\circ, \bullet$ and $\star$.
- For an edge numbered j, there are two triangles T_j^+ and T_j^- of which j is a common edge. A triangle of which j is an edge is denoted by T_j^+ if the circuit $\circ \to \bullet \to \star \to \circ$ follows the positive orientation of δT_j^+, and by T_j^- otherwise.

Step 2: For a triangle T_j^+, we can construct a homeomorphism f_j^+ from the triangle T_j^+ to $\bar{\mathbb{H}}^+ := \mathbb{H} \cup \mathbb{R} \cup \infty$ satisfying the following condition:

$$f_j^+ : \begin{cases} \partial T_j^+ \longrightarrow & \mathbb{R} \cup \infty \\ \circ \longmapsto & 0 \\ \bullet \longmapsto & 1 \\ \star \longmapsto & \infty \end{cases} \tag{3.2.1.1}$$

And similarly construct f_j^- from the adjacent triangle T_j^- to $\bar{\mathbb{H}}^- := \hat{\mathbb{C}} \setminus \mathbb{H}$ that coincides with f_j^+ in the intersection $T_j^+ \cap T_j^-$ and verifies also equation 3.2.1.1. To ensure the compatibility condition on the boundary, we can first construct the homomorphisms on ∂T_j^δ $(\delta \in \{+, -\})$ and extend them to T_j^δ. Since these two homeomorphisms agree on $T_j^+ \cap T_j^-$, we say they can be *glued together*.

Glue together the collection of homeomorphisms $f_j^\pm : T_j^\pm \to \bar{\mathbb{H}}^\pm$ to construct a continuous function $f_{\mathcal{T}(\mathcal{D})} : X \to \hat{\mathbb{C}}$ whose restriction on $X^* = X \setminus f_{\mathcal{T}(\mathcal{D})}^{-1}\{0, 1, \infty\} \to \hat{\mathbb{C}} \setminus \{0, 1, \infty\}$ is a topological covering. So X^* inherits from $\hat{\mathbb{C}}$ a unique Riemann surface structure such that $f_j^\pm$ is holomorphic. Furthermore X can be converted into a compact Riemann surface denoted $S_{\mathcal{T}(\mathcal{D})}$ such that $f_{\mathcal{T}(\mathcal{D})}$ becomes a morphism from $S_{\mathcal{T}(\mathcal{D})}$ to $\hat{\mathbb{C}}$.

Moreover, it can be checked that for a different triangle decomposition $\mathcal{L}(\mathcal{D})$, $(S_{\mathcal{L}(\mathcal{D})}, f_{\mathcal{L}(\mathcal{D})})$ and $(S_{\mathcal{T}(\mathcal{D})}, f_{\mathcal{T}(\mathcal{D})})$ are in the same equivalent class of covering, which means that modulo the equivalence of coverings, the pair $(S_{\mathcal{L}(\mathcal{D})}, f_{\mathcal{L}(\mathcal{D})})$ depends only on the dessin $(X, \mathcal{D})$. Therefore, we shall write $(S_{\mathcal{D}}, f_{\mathcal{D}})$ instead of $(S_{\mathcal{T}(\mathcal{D})}, f_{\mathcal{T}(\mathcal{D})})$.

The following proposition is direct from the above construction procedure.

Proposition 3.2.2. *The pair $(S_{\mathcal{D}}, f_{\mathcal{D}})$ satisfies the following properties:*

(1) $(S_{\mathcal{D}}, f_{\mathcal{D}})$ is a Belyi pair.

(2) The same number equations as in Proposition 6.

(3) $f_{\mathcal{D}}^{-1}([0,1]) = \mathcal{D}$.

It's easy to check the two correspondences given above are mutually inverse.

Theorem 3.2.3. *The two correspondences*

$$\begin{array}{rcl} \{\textit{Equiv. classes of dessins}\} & \longrightarrow & \{\textit{Equiv. classes of Belyi pairs}\} \\ (X, \mathcal{D}) & \longmapsto & (S_{\mathcal{D}}, f_{\mathcal{D}}) \\ (S, \mathcal{D}_f) & \longleftarrow\!\shortmid & (S, f) \end{array}$$

are mutually inverse.

Definition 3.2.4. A function $R : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ is called Belyi extending if it satisfies the following conditions:

(1) R is a Belyi function.

(2) R is defined over the rationals.

(3) $R(\{0, 1, \infty\}) \subset \{0, 1, \infty\}$.

If (S, f) is a Belyi pair and R is a Belyi extending, then $R \circ f$ is still a Belyi function. It will be shown in the section 6 that Belyi-extendings can be used to create new invariants of Galois action.

Take $R = 1/4z(1-z)$. If f^c denote $R \circ f$, $\mathcal{D}^c$ denote the dessin corresponding to f^c, then f^c is a clean Beiyi function and therefore $\mathcal{D}^c$ is a clean dessin. Actually, $\mathcal{D}^c$ can be obtained by changing all the vertices of $\mathcal{D}$ white and adding a black vertex in the middle of each edge.

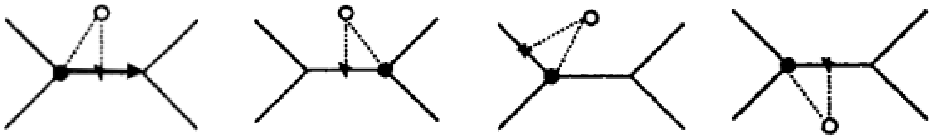
Take $R = 1/z$. Let $\mathcal{D}$ be a clean dessin and f is the corresponding clean Belyi function. The dual dessin formed from the preimages of the line segment $[1, \infty]$ corresponds to the $R \circ f = 1/f$.

3.3 Cartographical group and clean dessin

Definition 3.3.1. The cartographical group C_2 is generated by σ_0, σ_1 and σ_2 with the relations $\sigma_0^2 = \sigma_1^2 = \sigma_2^2 = 1$ and $(\sigma_0\sigma_2)^2 = 1$. The oriented cartographical group C_2^+ is the subgroup of index 2 of C_2 containing all even words of C_2, generated by $\rho_0 = \sigma_1\sigma_0$, $\rho_1 = \sigma_0\sigma_2$ and $\rho_2 = \sigma_2\sigma_1$, with the relations $\rho_1^2 = 1$ and $\rho_0\rho_1\rho_2 = 1$.

Definition 3.3.2. Let $\mathcal{D}$ be a clean dessin with marking as above, and the vertices marked $\bullet$ are of degree 2. Then the *flag set* $F(\mathcal{D})$ is the set of triangles in the triangle decomposition $\mathcal{T}(\mathcal{D})$, the elements of which are called flags, and the *oriented flag set* is the collection of all T_j^+.

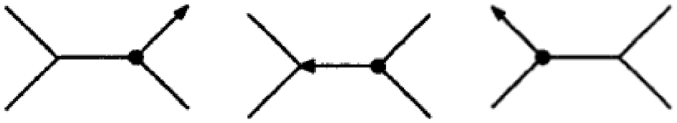
The action of the group C_2 on $F(\mathcal{D})$ is defined as in Figure 1.



(a) F (b) $\sigma_0(F)$ (c) $\sigma_1(F)$ (d) $\sigma_2(F)$

Figure 1: The action of $\sigma_0, \sigma_1, \sigma_2$ on a flag F

Only the group element in C_2^+ preserves the orientation. And the oriented flags can be uniquely determined by a vertex $\circ$ and an edge coming out of the vertex. In this view, the actions given by $\rho_0(F)$, $\rho_1(F)$ and $\rho_2(F)$ are shown by Figure 2.



(a) $\rho_0(F)$ (b) $\rho_1(F)$ (c) $\rho_2(F)$

Figure 2: The action of ρ_0, ρ_1, ρ_2 on a flag F

Definition 3.3.3. Let $B_{F,D}$ be the set of elements of C_2^+ fixing a flag F, which is a subgroup of finite index in C_2^+. Since C_2^+ acts transitively on $F^+(\mathcal{D})$, for any other flag F', $B_{F',D}$ is conjugate to $B_{F,D}$ in C_2^+.

Theorem 3.3.4. *There is a bijection between the isomorphism classes of clean dessins and the conjugacy classes of subgroups of C_2^+ of finite index.*

Proof. By Lemma 3.3.3, a dessin can be associated with a conjugacy class of subgroups of C_2^+ of finite index by the stabilizer of a flag. Then our only task is to construct a dessin from a subgroup of C_2^+ of finite index fitting this correspondence.

If B be the set of elements of C_2^+ fixing a flag F, then the action of C_2 on the flag set is isomorphic to its action on the coset space $H = C_2/B$. So imagine the elements in the coset space $H = C_2/B$ be flags with three vertices marked with $\circ, \bullet, \star$ respectively. A flag is positively oriented if and only if it's contained in C_2^+/B. By the definition of the action of σ_0, two flags have the common $\circ - \star$ edge if and only if they are in the same σ_0-obit. The $\bullet - \star$ and $\circ - \star$ edges can be identified in the similar way. Thus, we can glue the flags together in a unique way such that the dessin obtained corresponds to conjugacy class of B. □

The fundamental group of $\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$ is denoted by π_1, generated freely by loops γ_0, γ_1 around 0 and 1. Recall the classical results:

Lemma 3.3.5. *There is a bijection between the conjugacy classes of subgroups of finite index of π_1 and isomorphism classes of finite coverings X of $\mathbb{P}^1_{\mathbb{C}}$ ramified only over $0, 1, \infty$.*

For the clean type, let $\pi_1' = \pi_1/\langle\gamma_1^2\rangle$, then we have the following:

Corollary 3.3.6. *There is a bijection between the conjugacy classes of subgroups of finite index of π_1' and isomorphism classes of finite coverings X of $\mathbb{P}^1_{\mathbb{C}}$ ramified only over $0, 1, \infty$ such that the ramification over 1 is of degree at most 2.*

Theorem 3.3.7. *There is a bijection between the set of equivalent classes of clean dessins and the set of equivalent classes of clean Belyi pairs.*

This theorem is an immediate consequence of Lemma 3.3.6 and Theorem 3.3.4.

Remark 3.3.8. Actually, the actions ρ_1, ρ_2 defined here are consistent with σ_0, σ_1 in the next section, and the argument above can be adopted in the non-clean general case, which is related with the Fuchsian group description of Belyi pairs.

Let p, q be the order of the actions of ρ_1, ρ_2 on flag set. $\Pi_{p,q}$ denotes the hyperbolic regular q-gon with angles $2\pi/p$ in $\mathbb{H}$, and $\Gamma_{p,q} \subset PSL_2(\mathbb{R})$ is the group generated by two hyperbolic rotation β, γ. β is the rotation of $\Pi_{p,q}$ about the centre of angle $2\pi/p$, and γ is the rotation of $\mathbb{H}$ about a vertex of $\Pi_{p,q}$ of angle $2\pi/p$. β, γ satisfies the relations $\beta^q = \gamma^p$.

Then the homomorphism $\phi : C_2^+ \to \Gamma_{p,q} : \rho_1 \mapsto \beta, \rho_2 \mapsto \gamma$ is well defined. Set $\Gamma_{\mathcal{D},F} = \phi(B_{\mathcal{D},F})$. Since the conjugate class of $\Gamma_{\mathcal{D},F}$ is independent of the choice of F, so we may denote it by $\Gamma_{\mathcal{D}}$.

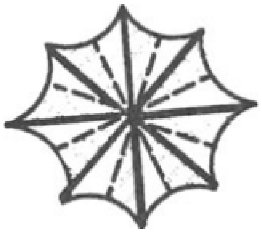


Figure 3: $\Pi_{p,q}$

The actions of β, γ on $\Gamma_{p,q}/\Gamma_{\mathcal{D},F}$ are isomorphic to the actions of ρ_1, ρ_2 on $C_2^+/B_{\mathcal{D},F}$. Thus, the Belyi pair $(S_{\mathcal{D}}, f)$ isomorphic to $(\mathbb{H}/\Gamma_{\mathcal{D}}, \pi)$ where π is the natural projection $\mathbb{H}/\Gamma_{\mathcal{D}} \to \mathbb{H}/\Gamma_{p,q}$. And the triangles in Figure 3 maps to flags by the projection $\mathbb{H} \to \mathbb{H}/\Gamma_{\mathcal{D}}$.

And obviously this also can be done in non-clean case with some adjustment.

4 Permutation representation pair

From now on, we assume a dessin is marked with white and black color such that the corresponding Belyi function sends white vertices to 0 and black vertices to 1.

Definition 4.0.1. Let $(X, \mathcal{D})$ be a dessin. If the dessin has n edges, label the edges of the dessin with integer $\{1, 2, \dots, n\}$. Consider two element σ_0, σ_1 in the permutation group S_n. Since the edges of the dessin is labelled, we can define the action of σ_0, σ_1 on the set of edges. σ_0 permutes an edge i to the following edge under positive rotation around the white vertex of i, and σ_1 permutes an edge i to the next edge by positive rotation around the black vertex of i. Then (σ_0, σ_1) is called the *permutation representation pair* of the dessin.

Proposition 4.0.2. *The permutation representation pair satisfies the following properties:*

(1) The circles of the σ_0 is in one-one correspondence with the white vertices of the dessin. And the degree of the corresponding vertex agrees with the length of the circle.

(2) The circles of the σ_0 is in one-one correspondence with the black vertices. And the degree of the corresponding vertex agrees with the length of the circle.

(3) The circles of the $\sigma_1\sigma_0$ is in one-one correspondence with the faces.

$$\begin{aligned} \#\{\textit{cycles of } \sigma_0\} &= \#\{f_{\mathcal{D}}^{-1}(0)\}, \\ \#\{\textit{cycles of } \sigma_1\} &= \#\{f_{\mathcal{D}}^{-1}(1)\}, \\ \#\{\textit{cycles of } \sigma_1\sigma_0\} &= \#\{f_{\mathcal{D}}^{-1}(\infty)\}. \end{aligned}$$

(4) The genus of the dessin can be calculated by the formula

$$2 - 2g = \#\{\textit{cycles of } \sigma_0\} + \#\{\textit{cycles of } \sigma_1\} - n + \#\{\textit{cycles of } \sigma_1\sigma_0\}.$$

(The Euler-Poincare characteristic of X corresponding to the polygonal decomposition)

(5) the group $\langle\sigma_0, \sigma_1\rangle$ acts transitively on the edges.

Proof. The first three properties can be easily viewed by the definition of (σ_0, σ_1), for the obit of an edge i under the action of σ_0 is just all the edges that have the common white vertex with i, similar for σ_1. The statement of the faces needs slightly more thoughts to consider the rotation of the triangle introduced in section 3.2.

Based on the first three propositions, the fourth one comes from the Grothendieck correspondence, and the fifth is an application of the Riemann-Hurwitz formula. The last one is because a dessin is a connected graph. □

If we label the edges of the dessin in a different way, and get a new permutation representation pair (σ_0', σ_1'), then there's a permutation in S_n that conjugate σ_0 to σ_0' and σ_1 to σ_1'. Actually, dessins are in one-one correspondence with permutation representation pairs up to conjugation. The way to construct a dessin from a given pair is to be discussed next, and the uniqueness is due to the relationship between the permutation representation pair and monodromy of corresponding Belyi function.

Proposition 4.0.3. *Let $\sigma_0, \sigma_1 \in S_n$, and $\langle\sigma_0, \sigma_1\rangle$ is a transitive subgroup. There exists a dessin of n edges whose permutation representation pair is precisely (σ_0, σ_1).*

One possible idea is to construct the faces first. Starting from an arbitrary edge i, the sequence $i, \sigma_0 i, \sigma_1\sigma_0 i, \sigma_0\sigma_1\sigma_0 i, \cdots$ iterates through the edges of a face containing i in counterclockwise direction. The common vertex of i and $\sigma_0(i)$ is marked white, and the common vertex of i and $\sigma_1(i)$ is marked black. When we have all faces constructed and all vertex marked, we can glue the same edge together such that the white vertices are glued to white ones and black to black. Then a dessin has been constructed now and obviously (σ_0, σ_1) is the dessin's permutation representation pair.

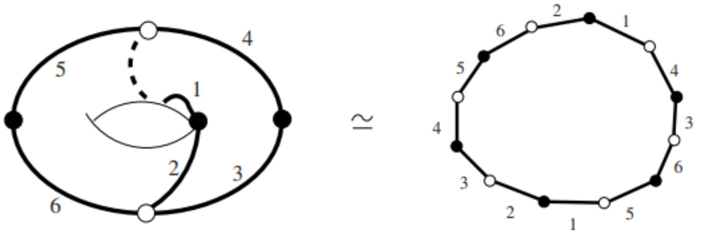


Figure 4: $\sigma_0 = (1,5,4)(2,6,3), \sigma_1 = (1,2)(3,4)(5,6)$

4.1 Monodromy of dessins

The fundamental group $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}, y)$ is a rank 2 free group. Let $y = 1/2$, then $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}, y)$ is generated by γ_0, γ_1 that are the loops based at $y = 1/2$ and turning counterclockwise once around the points 0 and 1 respectively. $\sigma_\gamma \in \mathrm{Bij}(f^{-1}(1/2))$ is defined as follows. If $x \in f^{-1}(1/2)$, then we can lift γ to a path $\tilde{\gamma}$ with the initial point x and the point $x' \in f^{-1}(1/2)$. Set $\sigma_\gamma(x) = x'$.

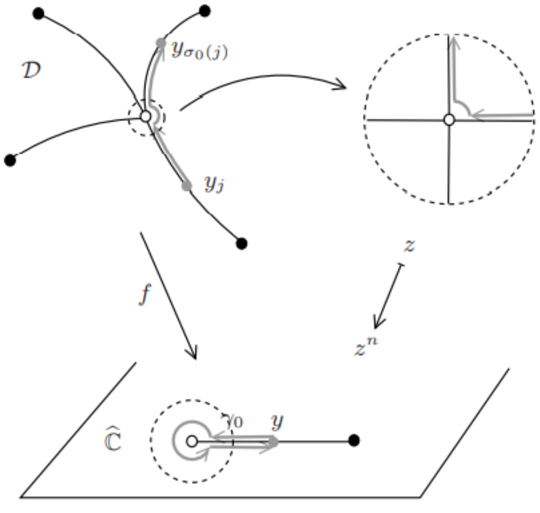


Figure 5: Lift of γ_0

As every edge of the dessin has exactly one point in the inverse image of $1/2$, $\sigma_{\gamma_0}, \sigma_{\gamma_1}$ can be thought to act on the set of edges of the dessin. Then it can be known easily from the construction of the Grothendieck correspondence that $\sigma_{\gamma_0} = \sigma_0$, $\sigma_{\gamma_1} = \sigma_1$.

Proposition 4.1.1. *The permutation representation pair of a dessin and the monodromy of the corresponding Belyi pair are determined by each other.*

Definition 4.1.2. The permutation group generated by σ_0 and σ_1 is called the monodromy group of the dessin, denoted by $\mathrm{Mon}(\mathcal{D})$.

4.2 Automorphisms of dessins

Definition 4.2.1. Let $(X, \mathcal{D})$ be a dessin. $\mathrm{Homeo}^+(X, \mathcal{D})$ is defined to be the set of orientation-preserving homeomorphisms of X that preserve $\mathcal{D}$ as a bicoloured graph. We set

$$\mathrm{Aut}(\mathcal{D}) = \mathrm{Homeo}^+(X, \mathcal{D}) / \sim,$$

where $H_1 \sim H_2$ if $H_1 \circ H_2^{-1}$ preserves setwise every edge of $\mathcal{D}$, called the *automorphisms of the dessin.*

It's clear that an element of $\mathrm{Aut}(\mathcal{D})$ is determined by how it permutes the edges of the dessin, then an element of $\mathrm{Aut}(\mathcal{D})$ can be represented by a permutation in S_n (If we label the edges of a dessin with $\{1, 2, \cdots, n\}$).

As the Grothendieck correspondence, the automorphisms of dessins correspond to automorphisms of the associated Belyi covers. Obviously, an automorphism of Belyi cover can be thought as an element of $\mathrm{Aut}(\mathcal{D})$. The following gives a brief description of why all element in $\mathrm{Aut}(\mathcal{D})$ can be constructed in this way.

Proposition 4.2.2. *The map $\mathrm{Aut}(f_{\mathcal{D}}) \to \mathrm{Aut}(\mathcal{D}) : H \mapsto H$ is an isomorphism of group.*

The inverse map can be obtained by the following lemma.

Lemma 4.2.3. *Let $\mathcal{T}(\mathcal{D})$ be a triangle decomposition for the dessin $(X, \mathcal{D})$, and $(S_{\mathcal{T}}, f_{\mathcal{T}})$ is the Belyi pair given by $\mathcal{T}(\mathcal{D})$. $H \in \mathrm{Homeo}^+(X, \mathcal{D})$, then there exits $H_1 \in \mathrm{Aut}(f_{\mathcal{T}})$ such that $H \sim H_1$.*

Proof. The triangle decomposition $H(\mathcal{T}(\mathcal{D}))$ provides x another Riemann surface structure. Due to the uniqueness of corresponding Belyi pair as coverings, there exists an isomorphism of Riemann surface F such that $f_{\mathcal{D}} \circ F = f_{H(\mathcal{D})}$. Then $H_1 = F \circ H$ satisfies $f_{\mathcal{T}} \circ H_1 = f_{\mathcal{T}}$ and equivalent to H. □

$\mathrm{Aut}(\mathcal{D})$ can be easily described by $\mathrm{Mon}(\mathcal{D})$ as shown next. An element of $\mathrm{Aut}(\mathcal{D})$ can be described by an permutation in S_n. And since it's a orientation-preserving homeomorphism preserving the bicolored structure, the corresponding permutation commutes with σ_0 and σ_1 (σ_0 is the rotation positively around white vertex and σ_1 around black vertex). Then we're going to explain that all the permutations with σ_0 and σ_1 are in $\mathrm{Aut}(\mathcal{D})$.

Proposition 4.2.4. *Assume $\sigma \in S_n$ commutes with σ_0 and σ_1, then there exists $H \in \mathrm{Aut}(\mathcal{D})$ making σ the corresponding permutation.*

Proof. Let $\mathcal{T}$ be a triangle decomposition associated with the dessin. As before, we first construct H_i^δ on the triangle $T_i^\delta(\delta \in \{+,-\})$, and then glue them together to get H. Take $H_i^\delta = (f_{\sigma(i)}^\delta)^{-1} \circ f_i^\delta$. To check they can glue, it's enough to check the boundary compatibility conditions. Take H_i^+ for instance:

$$H_i^+ = H_i^- \text{ on } T_i^+ \cap T_i^-$$

$$H_i^+ = H_{\sigma_0(i)}^- \text{ on } T_i^+ \cap T_{\sigma_0(i)}^-$$

$$H_i^+ = H_{\sigma_1(i)}^- \text{ on } T_i^+ \cap T_{\sigma_1(i)}^-$$

The first one comes from the compatibility of f_j^+ and f_j^-. The equation

$$\begin{aligned} H_{\sigma_0(i)}^- = (f_{\sigma(\sigma_0(i))}^-)^{-1} \circ f_{\sigma_0(i)}^- &= (f_{\sigma_0(\sigma(i))}^-)^{-1} \circ f_{\sigma_0(i)}^- \\ &\quad (\text{ on } T_i^+ \cap T_{\sigma_0(i)}^-) \\ &= (f_{\sigma(i)}^+)^{-1} \circ f_i^+ = H_i^+ \end{aligned}$$

shows the remained ones follow from that σ commutes with σ_0 and σ_1. Also, this construction ensured the glued morphism H having the corresponding permutation σ. □

Theorem 4.2.5. $\mathrm{Aut}(\mathcal{D})$ *is isomorphic to* $Z(\mathrm{Mon}(\mathcal{D}))$*, the centralizer of the monodromy group of* $\mathcal{D}$ *in* S_n*.*

The definition of regular dessin parallels the concept of Galois covering.

Definition 4.2.6. A dessin $(X, \mathcal{D})$ is called regular if $\mathrm{Aut}(\mathcal{D})$ acts transitively on the edges of $\mathcal{D}$.

Theorem 4.2.7. *Let $(X, \mathcal{D})$ be a dessin, and (S, f) be the corresponding Belyi pair. The following statements are equivalent.*

(1) $\mathcal{D}$ is regular.

(2) $f : S \to \mathbb{P}_{\mathbb{C}}^1$ is a Galois covering.

(3) $\#\mathrm{Mon}(\mathcal{D}) = \#\{\text{edges of } \mathcal{D}\} = \deg(f)$

From the Proposition 4.2.4, that the dessin is regular is totally the same with that the corresponding Belyi morphism is a Galois covering. And the last one comes from the results of Galois covering and is used to identify whether a dessin is regular.

If a dessin is regular, $\mathrm{Aut}(\mathcal{D}) \cong Z(\langle \sigma_0, \sigma_1 \rangle)$ acts transitively on the edges of $\mathcal{D}$, then the circles of σ_0 have the same length, the same for σ_0, $\sigma_1\sigma_0$. So all white vertices of the dessin have the same degree, and the same is true for black vertices and faces, and with these propertied a dessin is called uniform. But notice that a uniform dessin is not necessarily regular.

5 Galois action on dessins

We examine the action of the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of dessins of genus 0, 1, and ≥ 2, respectively.

We first describe the natural action of $G_{\mathbb{Q}}$ on the set of dessins.

Definition 5.0.1 (Transform of a dessin)**.** Let $\mathcal{D}$ be a dessin, σ be an element in $G_{\mathbb{Q}}$. Then the *transform (by σ) $\mathcal{D}^\sigma$* of a dessin $\mathcal{D}$ is defined by the composition

$$\begin{tikzcd}
\mathcal{D} \arrow[r, dashed] \arrow[d] & \mathcal{D}^\sigma \\
(S_{\mathcal{D}}, f_{\mathcal{D}}) \arrow[r, "\sigma"] & (S^\sigma_{\mathcal{D}}, f^\sigma_{\mathcal{D}}) \arrow[u]
\end{tikzcd}$$

where the vertical arrows are given as in Theorem 3.2.3.

The following basic properties of the action are by direct verification.

Proposition 5.0.2. *Let $\mathcal{D}$ be a dessin. The following quantities of $\mathcal{D}$ are invariant under the action of $G_{\mathbb{Q}}$:*

(a) The number of edges.

(b) The number of white vertices, black vertices and faces.

(c) The degree of the white vertices, black vertices and faces.

(d) The genus.

(e) The monodromy group.

(f) The automorphism group.

The main result of this section is the faithfulness of the action of $G_{\mathbb{Q}}$ on the set of dessins of any fixed genus:

Theorem 5.0.3 (Faithfulness of Galois action)**.** *For any $g \in \mathbb{Z}_{\geq 0}$, the action of $G_{\mathbb{Q}}$ on the set of dessins of genus g via $\sigma \mapsto (\mathcal{D} \mapsto \mathcal{D}^\sigma)$ is faithful.*

We will examine the three cases $g = 0, 1$, $g \geq 2$ separately.

5.1 Galois action on genus 1 dessins

Recall that the j-invariant classifies Riemann surfaces of genus 1 up to isomorphism, we have

Proposition 5.1.1. *The action of* $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ *on the isomorphism classes of compact Riemann surfaces of genus* 1 *is faithful.*

Proof. Let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ be an element not fixing a $z \in \mathbb{C}$. Choose a λ with $j(\lambda) = z$. Then $C_\lambda^\sigma = C_{\lambda^\sigma}$ has j-invariant

$$j(\lambda^\sigma) = j(\lambda)^\sigma = \sigma(z) \neq z,$$

therefore it cannot be isomorphic to C_λ. □

Corollary 5.1.2. *The action of $G_\mathbb{Q}$ on the set of dessins of genus 1 is faithful.*

From this we easily deduce:

Theorem 5.1.3. *The action of $G_\mathbb{Q}$ on the fundamental group $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \backslash \{0, 1, \infty\}, x)$ is faithful.*

Corollary 5.1.4. *There is an injective homomorphism*

$$\rho : G_\mathbb{Q} \to \mathrm{Out}(\hat{F}_2),$$

from the absolute Galois group $G_\mathbb{Q}$ to the outer automorphism group of the profinite completion of the free group $F_2 = \langle a, b \rangle = \langle a, b, c \mid abc = 1 \rangle$.

Proof. By a corollary of Grothendieck's Riemann existence theorem (see [11]), the étale fundamental group $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}, x)$ is isomorphic to the profinite completion of the topological fundamental group $\pi_1(\mathbb{P}^1_\mathbb{C} \setminus \{0, 1, \infty\}, x) \simeq F_2$, now by an easy check on the action of $G_\mathbb{Q}$ on the fundamental group $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}, x)$, we see that the preimage of $\mathrm{Inn}(\hat{F}_2)$ of the embedding

$$\tilde{\rho} : G_\mathbb{Q} \to \mathrm{Aut}(\hat{F}_2)$$

is trivial, giving rise to an embedding

$$\rho : G_\mathbb{Q} \to \mathrm{Out}(\hat{F}_2)$$

as desired. □

5.2 Galois action on genus ≥ 2 dessins

We first recall a classical result of Riemann surfaces.

Proposition 5.2.1. *Two hyperelliptic Riemann surfaces are isomorphic to each other if and only if there is a Möbius transformation relating the branch set of the respective hyperelliptic involutions.*

Proof. This follows directly from the fact that the hyperelliptic involution J of a hyperelliptic Riemann surface S is the only automorphism of order 2 satisfying $S/\langle J \rangle \cong \mathbb{P}^1$. □

From this we may even deduce the faithfulness of the action of $G_\mathbb{Q}$ on the set of hyperelliptic curves of genus g.

Theorem 5.2.2. *Let $\sigma \in G_{\mathbb{Q}}$ be a nontrivial element in $G_{\mathbb{Q}}$, and $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number not fixed by σ. For an integer $n \in \mathbb{Z}_{\geq 0}$, let C_n be the curve given by*

$$y^2 = (x-1)(x-2)\cdots(x-(2g+1))(x-(\alpha+n)).$$

Then, there is an n such that C_n^σ is not isomorphic to C_n.

Sketch of proof. Assume otherwise, then invoking Proposition 5.2.1 gives a family $\{f_n\}_{n\in\mathbb{Z}_{\geq 0}}$ of Möbius transformations in which only finitely many are distinct. We may choose three distinct natural numbers n_i $(i = 1, 2, 3)$ such that the three f_{n_i} are identical (denote by f from now on) and we have

$$f_{n_i}(\alpha + n_i) = \sigma(\alpha) + n_i$$

for each i. Then the Möbius transformation $g(z) := f(\alpha + z) - \sigma(\alpha)$ fixes all the n_i hence is identity, giving

$$f(z) = z + \sigma(\alpha) - \alpha.$$

Now

$$k + (\sigma(\alpha) - \alpha) = f(k) = l_k \in \{1, 2, \ldots, 2g+1\}$$

for each $k \in \{1, 2, \ldots, 2g+1\}$, but then

$$\sigma(\alpha) - \alpha = l_1 - 1 = l_2 - 2 = \cdots = l_{2g+1} - (2g+1)$$

must be 0, contradicting $\sigma(\alpha) \neq \alpha$. □

Corollary 5.2.3. *For any $g \geq 2$, the action of $G_{\mathbb{Q}}$ on the set of dessins of genus g is faithful.*

5.3 Galois action on genus 0 dessins

Notation 5.3.1. We call polynomial Belyi morphisms $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ *Shabat polynomials*, as often used in the literature. Two Shabat polynomials f_1, f_2 are called *linearly equivalent* if they are the same up to a linear change of variables, i.e. $f_1(x) = f_2(ax+b)$ for some $a, b \in \mathbb{C}$. It is direct to check that two Shabat polynomials are linearly equivalent if and only if they are in the same $\mathrm{PSL}_2(\mathbb{C})$-orbit.

We will use the following elementary technical lemma:

Lemma 5.3.2. *(1) Let H_1, H_2 be two monic polynomials of the same degree whose constant terms are 0. Assume that there are polynomials G_1, G_2 with $G_1 \circ H_1 = G_2 \circ H_2$. Then $H_1 = H_2$.*

(2) Let H_1, H_2 be arbitrary polynomials of the same degree such that $G_1 \circ H_1 = G_2 \circ H_2$ for some polynomials G_1, G_2. Then there are constants c, d such that $H_2 = cH_1 + d$.

Proof. See Leila's paper [8]. □

Theorem 5.3.3. *The action of $G_{\mathbb{Q}}$ on the set of linearly equivalent classes of Shabat polynomial is faithful.*

Proof (Lenstra). Let $\sigma \in G_{\mathbb{Q}}$ be a nontrivial element in $G_{\mathbb{Q}}$, and $\alpha \in \overline{\mathbb{Q}}$ not fixed by σ. Set

$$f_\alpha(x) = \int x(x-1)^2(x-\alpha)^3 \in \mathbb{Q}(\alpha)[x],$$

then f_α is a polynomial ramified exactly at $\{0, 1, \alpha\}$ and the ramification indices are distinct. Applying Belyi's algorithm now yields a polynomial $g \in \mathbb{Q}[x]$ such that $h_\alpha = g \circ f_\alpha$ is a Shabat polynomial.

Suppose h_α and h_α^σ are linearly equivalent, then

$$g(f_\alpha(az+b)) = f_\alpha(az+b) = f_\alpha^\sigma(z) = g(f_{\sigma(\alpha)}(z))$$

for some $a, b \in \mathbb{C}$, therefore by Lemma 5.3.2

$$f_\alpha(az+b) = cf_{\sigma(\alpha)}(z) + d$$

for some $c, d \in \mathbb{C}$. Now by our choice of f_α, the map $(z-b)/a$ maps $0, 1, \alpha$ to $0, 1, \sigma(\alpha)$ respectively, forcing $b = 0$ and $a = 1$ therefore $\sigma(\alpha) = \alpha$, leading to a contradiction. □

Corollary 5.3.4. *The action of $G_{\mathbb{Q}}$ on the set of dessins of genus 0 is faithful.*

6 Examples

Some dessins of genus 0:

All genus 0 Riemann surfaces are isomorphic to $\hat{\mathbb{C}}$, then in genus 0 case, we may assume $S = \hat{\mathbb{C}}$.

Example 6.0.1. The two dessins given by $f(z) = z^n$ and Chebyshev polynomial $f(\cos t) = \cos(nt)$ are star-like and chain-like trees as shown in Figure 6.

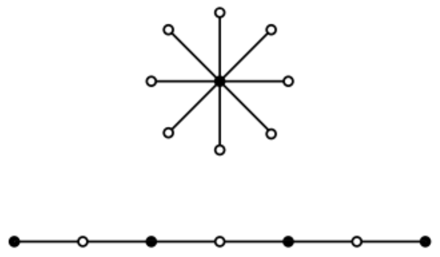


Figure 6: Star-like and chain-like trees

Example 6.0.2. The two dessins shown in Figure 7 are both with six edges and white vertices of degrees 2,2,1,1 and black vertices of degrees 4,1,1. The permutation representation pair of $\mathcal{D}_1$ is $\sigma_0 = (1,5)(6,3)$ and $\sigma_1 = (1,2,3,4)$. The permutation representation pair of

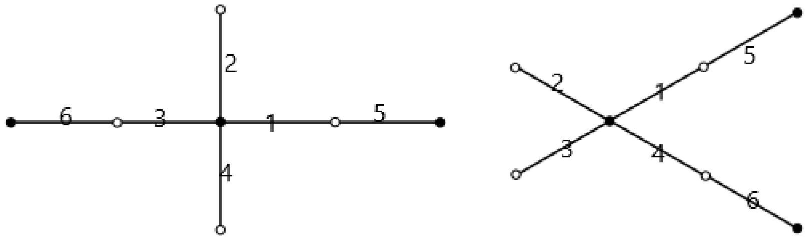


Figure 7: $\mathcal{D}_1$ and $\mathcal{D}_2$

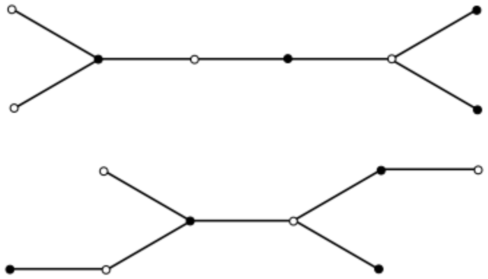


Figure 8: $\mathcal{D}_3$ and $\mathcal{D}_4$

$\mathcal{D}_2$ is $\sigma_0 = (1,5)(6,4)$ and $\sigma_1 = (1,2,3,4)$. Then $\#\,\mathrm{Mon}(\mathcal{D}_1) = 48$, $\#\,\mathrm{Mon}(\mathcal{D}_2) = 120$, and $\mathrm{Aut}(\mathcal{D}_1) = \langle(1,3)(2,4)(5,6)\rangle$, $\mathrm{Aut}(\mathcal{D}_2) = \langle(1)\rangle$. Since the monodromy group and automorphism group are invariants under the action of the absolute Galois group, therefore $\mathcal{D}_1$ and $\mathcal{D}_2$ can not be Galois conjugated.

But for dessins $\mathcal{D}_3$ and $\mathcal{D}_4$ shown in Figure 8, they have the same degree sets and monodromy group and automorphism group. But the monodromy group of $\mathcal{D}_3^c$ and $\mathcal{D}_4^c$ are different, then they are not Galois conjugated.

If R is a Belyi extending, the monodromy group and automorphism group of $R \circ f$ are also invariant under Galois group action. This example shows this method can construct some new invariants. Finding invariants of dessins which completely identify their $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits is a problem concerned in the theory of dessins d'enfants.

Example 6.0.3. This is an example of calculating the corresponding Belyi function from the dessin considered in the paper [15]. The dessin $\mathcal{D}$ shown in Figure 9 is a clean dessin(all vertices are the preimages of 0, and there's a middle point in each edge being a preimage of 1). Since it has three vertices of degree 2 and two vertices of degree 3, the numerator be f should be of the form:

$$(x^2 + ax + b)^3(x^3 + cx^2 + dx + e)^2 \tag{6.0.3.1}$$

The dessin have three faces of valencies 3,4,5, then the denominator of f should be $(x - f)^3(x - g)^4(x - h)^5$. As $\mathcal{D}$ is clean, $1 - f$ has 6 roots and the multiplicity of each root is 2.

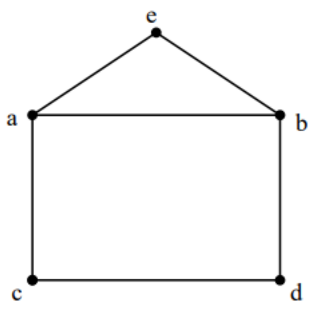


Figure 9: A dessin with 6 edges

So we have:

$$f(x) = k\frac{(x^2+ax+b)^3(x^3+cx^2+dx+e)^2}{(x-f)^3(x-g)^4(x-h)^5} \tag{6.0.3.2}$$

$$f(x) - 1 = k\frac{(x^6+mx^5+nx^4+px^3+qx^2+ux+v)^2}{(x-f)^3(x-g)^4(x-h)^5} \tag{6.0.3.3}$$

The above two equations reaches a system of equations including 15 unknowns and 12 equations. The remaining 3 degrees is because of the automorphism group of $\mathbb{P}^1_{\mathbb{C}}$. More the related results of finding the equation of Belyi function from a clean dessin in genus 0 case can be found in the article [8]

A dessin of genus 1:

Example 6.0.4. Let S be the Riemann surface $\{y^2 = x(x-1)(x-\sqrt{2})\} \cup \{\infty\}$. By the method proposed in the proof of $(a) \Rightarrow (b)$ of Belyi's theorem, we can construct a Belyi function on S: $f = -4(x^2-1)/(x^2-2)^2$:

$$x \xrightarrow{t \mapsto t^2-2} x^2-2 \xrightarrow{t \mapsto -1/t} -1/(x^2-2) \xrightarrow{t \mapsto 4t(1-t)} -4(x^2-1)/(x^2-2)^2 \tag{6.0.4.1}$$

By computing the preimage of $[0,1]$ step by step, the dessin corresponding to f can be obtained as Figure 10.

The only $\sigma \in \mathrm{Gal}(\mathbb{C})$ may act non-trivially on the dessin is $\sigma(\sqrt{2}) = -\sqrt{2}$. $S^\sigma = \{y^2 = x(x-1)(x+\sqrt{2})\} \cup \{\infty\}$, $f^\sigma = -4(x^2-1)/(x^2-2)^2$. And we can obtain the corresponding dessin $\mathcal{D}^\sigma$ by the same means as shown in Figure 11.

The permutation representation pair of $\mathcal{D}$ is $\sigma_0 = (1,7,5,3)(4,8), \sigma_1 = (1,2,3,4,5,6,7,8)$. The permutation representation pair of $\mathcal{D}^\sigma$ is $\sigma_0 = (2,4,6,8)(3,7), \sigma_1 = (1,2,3,4,5,6,7,8)$. They are not conjugate, so $\mathcal{D}$ and $\mathcal{D}^\sigma$ are not isomorphic dessin. Actually, $j(\sqrt{2}) \neq j(-\sqrt{2})$ (j denotes the classical j-invariant) shows that S and S^σ are not isomorphic Riemann surface. Hence, there are two dessins in the orbit of $\mathcal{D}$.

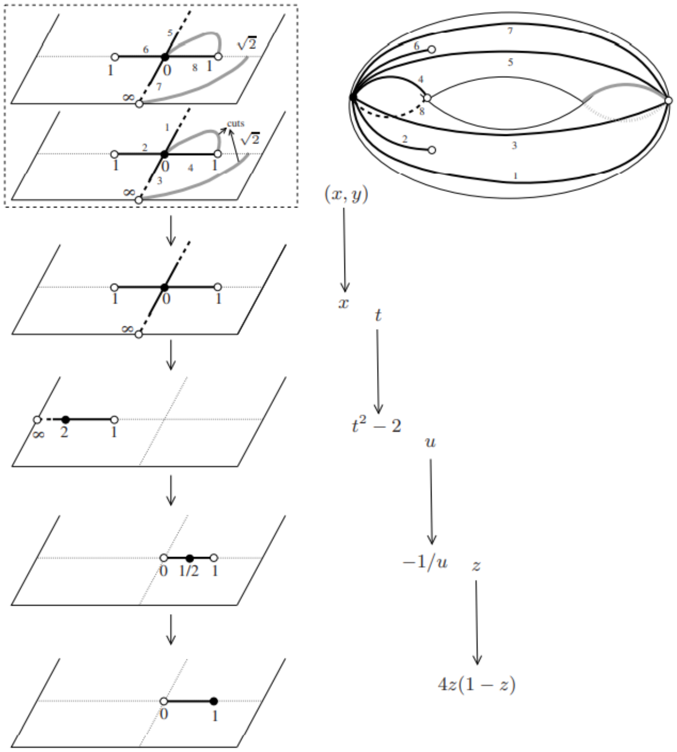


Figure 10: The procedure of finding the dessin

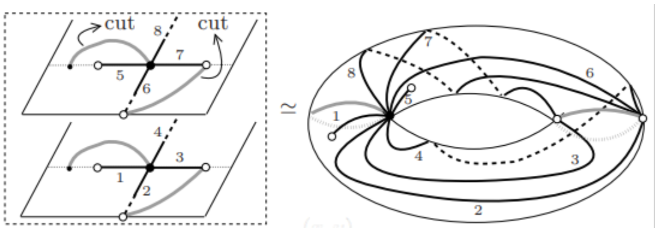


Figure 11: Dessin $\mathcal{D}^\sigma$

7 Applications

7.1 Minimal degree of $f^3 - g^2$

To state our main result in simpler terms, we introduce the following definitions.

Convention 7.1.1. All graphs are thought to be simple in this section, and by a *binary tree* we mean a tree whose vertices are all of degree 1 or 3.

Example 7.1.2. The graph in Figure 12 is a binary tree in the sense of 7.1.1.

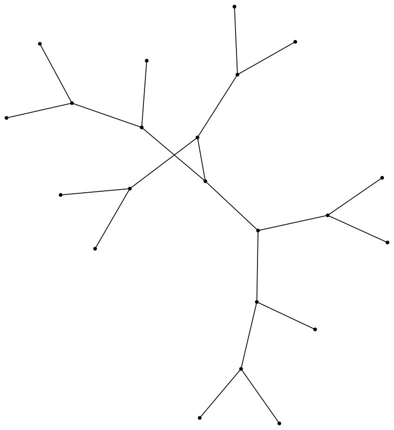


Figure 12: A binary tree

Definition 7.1.3 (Tacosad)**.** A graph Γ is a *tacosad*, if there is a surjection of graphs

$$\pi : \coprod_{i \in I} \gamma_i \to \Gamma$$

that is a bijection on the set of edges, where I is a finite index set, and each γ_i is isomorphic to K_3, such that any loop of Γ is generated by $\{\pi(\gamma_i)\}_{i \in I}$. We call these $\pi(\gamma_i)$ *faces* of the tacosad Γ.

Remark 7.1.4. It is straight-forward to check that any tacosad is the dual graph of a binary tree, and that the dual graph of any binary tree is a tacosad.

Example 7.1.5. The graph in Figure 13 is a tacosad. In fact, it is the dual graph of the binary tree in Example 7.1.2.

Definition 7.1.6 (Orientation of a tacosad)**.** An *orientation* of a tacosad Γ is a map that associates each face of Γ an orientation.

Definition 7.1.7 (Oriented binary tree)**.** An *oriented binary tree* is a pair $(\mathcal{T}, \varphi)$, where $\mathcal{T}$ is a binary tree, and φ is an orientation of the dual graph of $\mathcal{T}$, in the sense of Definition 7.1.6.

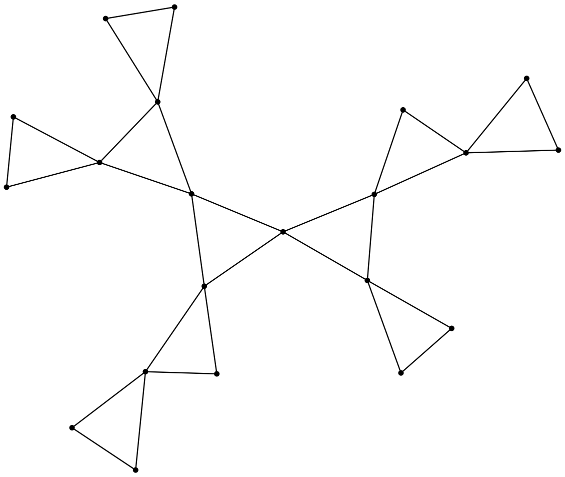


Figure 13: A tacosad

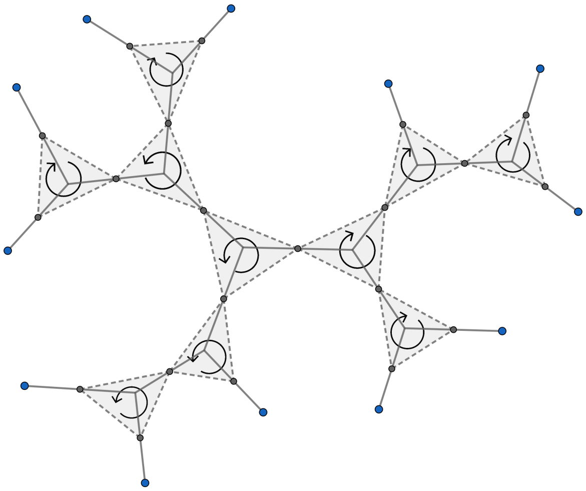


Figure 14: An oriented binary tree

Example 7.1.8. The structure in Figure 14 is an oriented binary tree. In fact, its underlying binary tree is the same as in Figure 12.

Remark 7.1.9. The motivation of Definition 7.1.7 is to keep track of the orientation of a dessin by adding more structure to the graph. More concretely speaking, the φ in the definition allow us to draw the tree on a oriented plane (or sphere to be more precise) in a unique way, namely we flip the faces to the "correct" position according to the orientation. In this manner we see that, in this specific case for binary trees, the notion of isomorphism for such clean dessins is actually coherent with the notion of isomorphism for $\mathfrak{S}_3$-trees, i.e., the topological data is of combinatorial nature.

The combinatorial structure Zannier used in his paper [13] is (essentially) the following more artificial analog of Definition 7.1.7.

Definition 7.1.10 ($\mathfrak{S}_3$-tree)**.** An $\mathfrak{S}_3$*-tree* is a pair $(\mathcal{T}, \sigma)$, where $\mathcal{T}$ is a binary tree, and σ is a map from the set of degree-3 vertices to the set of permutations on the vertices of $\mathcal{T}$, such that $\sigma(v)$ non-trivially permutes its three neighbours cyclically and fixes the rest vertices, for each vertex v of degree 3.

The main result of this section is the following:

Theorem 7.1.11. *Let f, g be two coprime complex coefficient polynomials of degree $2n, 3n$ respectively. Then*

(1) $\deg(f^3 - g^2) \geq n + 1$*;*

(2) The equality can be reached for each positive integer n;

(3) The number μ_n of linearly-equivalent classes of pairs (f, g) obtaining the minimal degree $\deg(f^3 - g^2) = n + 1$ *equals the number ϕ_n of isomorphism classes of oriented binary trees on $2n$ vertices; and*

(4) We have the following estimation for μ_n:

$$c_1 n^{-5/2} 4^n < \mu_n < c_2 n^{-3/2} 4^n$$

for some positive reals c_1, c_2 independent of n.

Remark 7.1.12. The first claim of Theorem 7.1.11 is actually a direct corollary of the *abc* conjecture for polynomials (a.k.a. Mason–Stothers theorem), which has a short and elementary proof. However, our approach here proves both the inequality and the criterion for equality at one strike.

Proof of Theorem 7.1.11. Let

$$r : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$$

be given by the rational function $\frac{f^3}{f^3-g^2}$, then r is of degree $6n$, and $r-1$ is given by the rational function $\frac{g^2}{f^3-g^2}$. Now applying Riemann-Hurwitz formula to r gives

$$\begin{aligned}
-2 = -12n + \sum_{x\in\mathbb{P}^1_{\mathbb{C}}} \nu_r(x) &\geq -12n + \sum_{\substack{x\in\mathbb{P}^1_{\mathbb{C}} \\ r(x)\in\{0,1,\infty\}}} \nu_r(x) \\
&= 6n - (\#r^{-1}(0) + \#r^{-1}(1) + \#r^{-1}(\infty)) \\
&\geq 6n - (2n + 3n + (\deg(f^3-g^2)+1)) \\
&= n - 1 - \deg(f^3-g^2),
\end{aligned}$$

i.e., $\deg(f^3-g^2) \geq n+1$. The first claim is proved.

From the chain of inequalities above we see that, $\deg(f^3-g^2) = n+1$ if and only if the following conditions hold:

(a) r is only ramified above $0, 1, \infty$, i.e., r is a Belyi morphism;

(b) $\#r^{-1}(0) = 2n$, i.e., f has no multiple roots;

(c) $\#r^{-1}(1) = 3n$, i.e., g has no multiple roots;

(d) $\#r^{-1}(\infty) = \deg(f^3-g^2)+1$, i.e., f^3-g^2 has no multiple roots.

Now suppose r satisfy the above conditions, then the graph associated to the clean Belyi morphism r is essentially a tree on $2n$ vertices (discarding the middle-points and the self-loops), all of which are of degree 1 or 3. Recall that Theorem 3.2.3 gives us a bijection between the set of isomorphism classes of clean Belyi morphisms and the set of abstract clean dessins, and that each isomorphism class of clean Belyi morphisms is just a $\mathrm{PSL}_2(\mathbb{C})$-orbit of the natural action of $\mathrm{PSL}_2(\mathbb{C})$ on the set of clean Belyi morphisms, therefore non-linearly-equivalent pairs gives non-isomorphic Belyi morphisms. In conclusion, we have a bijection between the set of linearly-equivalent classes of pairs (f, g) obtaining the minimal degree $\deg(f^3-g^2) = n+1$ and the set of isomorphism classes of oriented binary tree on $2n$ vertices, in view of Remark 7.1.9. This completes the proof of the second and third claim.

As for the fourth claim, note that we've shown in the above paragraph that $\mu_n = \phi_n$, thus by applying the estimation B.0.4 for ϕ_n in Appendix B we obtain the desired estimation. □

7.2 The Mordell conjecture is as easy as the *abc* conjecture[1]

We will prove that the *abc* conjecture implies the Mordell conjecture in this section. The upshot is that validity of the *abc* conjecture gives us bound on ramifications, forcing the number of rational points to be finite, via Belyi's theorem A.0.1.

[1] This amusing equivalent formulation of Elkies' original title "ABC implies Mordell" is noted by Don Zagier, as pointed out by Elkies in [1].

Convention 7.2.1. Whenever we use the capital H for heights, we mean the exponential of the corresponding height h defined in Appendix C. Moreover, recall that we have a homomorphism

$$\mathrm{WCl}(X) \to \mathrm{Pic}(X),\ D \mapsto \mathcal{O}_X(D)$$

for any variety X, which is an isomorphism if X is non-singular. We will use H_D (resp. h_D) to denote the Weil heights $H_{\mathcal{O}(D)}$ (resp. $h_{\mathcal{O}(D)}$). We will also use $D_0(f)$ (resp. $D_\infty(f)$) to denote the divisor of zeros of f (resp. the divisor of poles of f), i.e., we have

$$\mathrm{div}(f) = D_0(f) - D_\infty(f),$$

where $D_0(f)$ and $D_\infty(f)$ are effective.

We first recall the *abc* conjecture and the Mordell conjectures.

Definition 7.2.2 (Conductor on $\mathbb{P}^n$)**.** Let K be a number field. Then the *conductor* $N(x)$ of an algebraic point $x = (x_0, \ldots, x_n) \in \mathbb{P}_K(\overline{K})$ is given by

$$N(x) = N(x_0, \ldots, x_n) = \prod_{\substack{v \in M_{K,f} \text{s.t.} \\ |x_i/x_j|_v > 1 \\ \text{for some } i,j}} N(\wp_v).$$

We will use $N_0(r)$ (resp. $N_1(r), N_\infty(r)$) to denote the products of the absolute norms of the prime ideals at which r (resp. $r-1$, $1/r$) has positive valuation, then

$$N(r, -1, 1-r) = N_0(r) \cdot N_1(r) \cdot N_\infty(r)$$

by direct verification.

Conjecture 7.2.3 (*abc* conjecture over K)**.** *Let K be a number field. Then*

$$N(a, b, c) \gg_\epsilon H(a, b, c)^{1-\epsilon}$$

for all $a, b, c \in K^\times$ with $a + b + c = 0$, for each $\epsilon > 0$.

Theorem 7.2.4 (Mordell conjecture over K, proved by G. Faltings)**.** *Let K be a number field, C a curve of genus $g > 1$ over K. Then the set $C(K)$ of rational points of C is finite.*

Remark 7.2.5. Fatings' proof of the Mordell conjecture makes an essential use of height theory, which is beyond the scope of Appendix C. The idea is that you can define heights of (*not* on) any abelian variety, via two approach: one is directly using the integral of a differential on the abelian variety, obtaining the so-called Faltings height; the other is to view abelian varieties as points of the Siegel modular variety, which is the moduli space of abelian varieties added some extra data to shrink the automorphism group. The upshot is that these two heights are the same up to $O(1)$, giving us Northcott property (see Appendix C for definitions) for the Faltings height, therefore deduce the finiteness of a certain set of abelian varieties associated to each abelian variety, which completes the proof of the Mordell conjecture.

We also have an *effective* version of Mordell conjecture.

Conjecture 7.2.6 (Effective Mordell over K)**.** *Let X be a projective and smooth curve over $\mathbb{Q}$ of genus $g > 1$. Then for any $d \geq 1$, there exist constants $A(X,d)$ and $B(X,d)$ depending only on X and d such that for any finite extension K of $\mathbb{Q}$ of degree d, we have*

$$h(x) < A(X,d) \log |\Delta_K| + B(X,d),$$

for any $x \in X(K)$.

Proposition 7.2.7 (*abc* implies Mordell)**.** *For any number field K, the abc conjecture over K implies the Mordell conjecture over K.*

Remark 7.2.8. In fact, it can be shown that (some version of) the effective Mordell conjecture implies (some version of) the abc conjecture. Thus combining with (some version of) Proposition 7.2.7, these two conjectures are equivalent.

An essential part of the proof is the following observation.

Lemma 7.2.9. *Let C be any curve over K and $f \in K(C)$ be a rational function of degree d. Then for any rational point $x \in C(K) \setminus f^{-1}(0)$ we have*

$$\log N_0(f(x)) < (1 - \frac{b_f(0)}{d}) \log H(1, f(x)) + O(\sqrt{\log H(1, f(x))} + 1).$$

Proof. Write

$$D_0(f) = \sum_k m_k D_k,$$

where the D_k are distinct irreducible divisors of degrees d_k occurring with multiplicities m_k in $D_0(f)$. Then

$$d = \sum_k m_k d_k = \deg D \text{ and } b_f(0) = d - \sum_k d_k = \deg D_0(f) - \deg D_0(f)_{\mathrm{red}},$$

where $D_0(f)_{\mathrm{red}}$ denotes the divisor $\sum_{f(x)=0}(x)$, i.e. $D_0(f)$ with all multiplicities removed. We then have

$$\log H(1, f(x)) = h_{D_0(f)}(x) + O(1) = \sum_k m_k h_{D_k}(x) + O(1).$$

Now note that, a prime occurs in $N_0(f(x))$ if and only if it contributes to $h_{D_k}(x)$ for some k, except for the primes of bad reduction of C and the primes of good reduction at which f reduces to the identically zero function. But the total number of these "bad" primes is finite, giving

$$\log N_0(f(x)) < \sum_k h_{D_k}(x) + O(1) = h_{D_0(f)_{\mathrm{red}}}(x) + O(1).$$

Thus it remains to show

$$h_{D_0(f)_{\mathrm{red}}}(x) = \frac{\deg D_0(f)_{\mathrm{red}}}{\deg D_0(f)} \cdot h_{D_0(f)}(x) + O(\sqrt{\log H(1, f(x))} + 1),$$

which is just

$$h_\Delta(x) = O(\sqrt{\log H(1, f(x))} + 1),$$

where Δ denotes the degree-zero divisor

$$\Delta = (\deg D_0(f))D_0(f)_{\mathrm{red}} - (\deg D_0(f)_{\mathrm{red}})D_0(f).$$

Recall that Theorem C.0.20 tells us this is true for any degree-zero divisor, thus invoking Theorem C.0.20 now completes the proof. □

We can now prove Proposition 7.2.7.

Proof of Proposition 7.2.7. By Belyi's theorem A.0.1, we may choose a rational function $f \in K(C)$ ramified only above $0, 1, \infty$. Then by Riemann-Hurwitz formula, we have

$$m := \#\{x \in C(\overline{\mathbb{Q}}) \mid f(x) \in \{0, 1, \infty\}\} = \deg(f) + 2 - 2g < \deg(f) =: d.$$

Now by summing the three inequalities obtained by applying Lemma 7.2.9 to $f, f - 1, 1/f$ respectively, we see that

$$\log N(f(x), -1, 1 - f(x)) < \frac{m}{d} \log H(1, f(x)) + O(\sqrt{\log H(1, f(x))} + 1),$$

giving a counterexample to the *abc* conjecture over K for $\epsilon > 1 - (m/d)$ once $H(1, f(x)) = H_{D_0(f)}(x)$ is large enough, i.e. for all but finitely many x by Northcott property C.0.16. This completes the proof of *abc* implies Mordell. □

7.3 A characterization for finite image Galois representations

Notation 7.3.1. Let F be any field. For notational convenience, we use G_F to denote the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ over F, and $\mathcal{C}_F$ to denote the class

$$\{V \mid V \text{ appears as a subquotient of } \mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_v)] \text{ for every } v\},$$

if no confusion arises.

The main result in this section the following characterization for finite image Galois representations.

Theorem 7.3.2. *Any continuous finite image representation*

$$\rho : G_F \to \mathrm{GL}_n(\mathbb{Q})$$

can be embedded into the space of locally constant functions

$$\mathrm{Func}^{\text{loc.const.}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_v), \mathbb{Q}),$$

for any tangential base point 0_v.

A key ingredient of the proof of Theorem 7.3.2 is the following telescopic property of the fundamental group of $\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}$.

Proposition 7.3.3. *There exists an open subgroup*

$$\Gamma \subset \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_v)$$

stable under G_F-action and admitting a G_F-equivariant surjection

$$\Gamma \twoheadrightarrow \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_{v_1}) \times \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_{v_2})$$

for some tangential base points $0_{v_1}, 0_{v_2}$ at 0.

Proof. We make use of Belyi's explicit construction of Belyi morphism.

Consider the degree 3 finite morphism

$$f : \mathbb{P}^1_F \to \mathbb{P}^1_F,\ z \mapsto \frac{27}{4} z(z-1)^2,$$

then f is only ramified at $\frac{1}{3}, 1, \infty$. Since $f(1) = 0, f(\frac{1}{3}) = 1, f(\infty) = \infty$ the map f restricts to a finite étale cover

$$\mathbb{P}^1_F \setminus \{0, \frac{1}{3}, 1, \frac{4}{3}, \infty\} \to \mathbb{P}^1_F \setminus \{0, 1, \infty\}.$$

Moreover, since f is unramified at 0, we may choose a tangential base point 0_{v_1} for the truncated projective line $\mathbb{P}^1_F \setminus \{0, \frac{1}{3}, 1, \frac{4}{3}, \infty\}$ such that $f(0_{v_1}) = 0_v$.

Let Γ be defined as

$$\Gamma := f_*(\pi_1^{\text{ét}}(\mathbb{P}^1_F \setminus \{0, \frac{1}{3}, 1, \frac{4}{3}, \infty\}, 0_{v_1})) \subset \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_v).$$

Then the inclusion maps

$$i_1 : \mathbb{P}^1_F \setminus \{0, \frac{1}{3}, 1, \frac{4}{3}, \infty\} \to \mathbb{P}^1_F \setminus \{0, 1, \infty\},\ i_2 : \mathbb{P}^1_F \setminus \{0, \frac{1}{3}, 1, \frac{4}{3}, \infty\} \to \mathbb{P}^1_F \setminus \{0, \frac{1}{3}, \frac{4}{3}\}$$

induce a surjection

$$\Gamma \twoheadrightarrow \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_{v_1}) \times \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, \frac{1}{3}, \frac{4}{3}\}, 0_{v_1})$$

by the Seifert-Van Kampen theorem, this then completes the proof of Lemma 7.3.3 since $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, \frac{1}{3}, \frac{4}{3}\}, 0_{v_1})$ can be identified with $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_{v_2})$ via an automorphism of $\mathbb{P}^1_F$, for some tangential base point 0_{v_2}. □

From Proposition 7.3.3 we deduce the following lemma to be used in the proof of the main theorem 7.3.2.

Lemma 7.3.4. *For a tangential base point 0_v supported at 0 there exist two other tangential base points 0_{v_1} and 0_{v_2} such that, if V_1 and V_2 are representations of G_F appearing as subquotients of $\mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_{v_i})]^{G_F-\text{fin}}$, then $V_1 \otimes V_2$ is a subquotient of $\mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0, 1, \infty\}, 0_v)]^{G_F-\text{fin}}$.*

Proof. Note that the representation $V_1 \otimes V_2$ is a subquotient of

$$\mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_{v_1})]^{G_F-\text{fin}} \otimes \mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_{v_2})]^{G_F-\text{fin}} \subset \mathbb{Q}[\Gamma]^{G_F-\text{fin}},$$

and that $\mathbb{Q}[\Gamma]^{G_F-\text{fin}}$ is a quotient of $\mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v)]^{G_F-\text{fin}}$ by Grothendieck's Galois theory formalism, therefore $V_1 \otimes V_2$ is a subquotient of $\mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v)]^{G_F-\text{fin}}$ as desired. □

We now prove Theorem 7.3.2.

Proof of Theorem 7.3.2. Since the image of

$$\rho : G_F \to \mathrm{GL}_n(\mathbb{Q})$$

is finite, it factor through $\mathrm{Gal}(K/F)$ for a finite Galois extension K/F. Now recall that every faithful representation of a finite group G contains a faithful subrepresentation of dimension $\leq \#G$, thus if we can show that the space $\mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v)]^{G_F-\text{fin}}$ has some faithful representation W_v of $\mathrm{Gal}(K/F)$ as a subquotient for every tangential base point 0_v, then we may choose the representations W_v in a way that they all belong to finitely many isomorphism classes, say $W_1, \ldots, W_N$. Then by repeatedly applying Lemma 7.3.4, we can conclude that $\mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v)]^{G_F-\text{fin}}$ has a subquotient of the form $W_1^{\otimes a_1} \otimes \cdots \otimes W_N^{\otimes a_N}$ with $a_i \geq d$ for at least one i, for any $d \geq 0$. Finally, recall that any representation of a finite group is contained in a large enough tensor power of any faithful representation (†), we see that $\mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v)]^{G_F-\text{fin}}$ has a subquotient of the form $W_1^{\otimes b_1} \otimes \cdots \otimes W_N^{\otimes b_N}$ with $b_i \geq d$ for *all* i, applying (†) again then completes the proof of Theorem 7.3.2. Thus it remains to show the existence of W_v for any v.

For this, we first choose a smooth proper geometrically connected curve C over K that does not descend to any proper subfield $K' \subset K$. By Belyi's theorem A.0.1 there exists a finite map $f : C \to \mathbb{P}^1_K$ that is étale over $\mathbb{P}^1_K \setminus \{0,1,\infty\}$. Denote by $U \subset C$ the preimage $f^{-1}(\mathbb{P}^1_K \setminus \{0,1,\infty\})$ of $\mathbb{P}^1_K \setminus \{0,1,\infty\}$. Choosing a tangential $\overline{F}$-base point x_w for $C \setminus U$ that lies above 0_v, we get an open subgroup $f_*(\pi_1^{\text{ét}}(U_{\overline{K}}, x_w)) \subset \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{K}} \setminus \{0,1,\infty\}, 0_v)$. If an element $\sigma \in G_F$ stabilizes this subgroup, then the scheme $U_{\overline{K}}$ can be descended to the field $(\overline{F})^{\sigma=1}$. Our choice of C then forces the stabilizer of this subgroup to be contained inside $G_K \subset G_F$. In particular, there is a finite G_F-equivariant quotient $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v) \twoheadrightarrow S$ such that the kernel of the action of G_F on S is contained in G_K. In conclusion, there exists a G_F-equivariant finite quotient $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0) \to X$ such that the action of G_F on X factors through a faithful action of $\mathrm{Gal}(K/F)$. □

Remark 7.3.5. In the same manner we could prove a generalization of Theorem 7.3.2, in which the étale fundamental group is replaced with its pro-algebraic completion, and $\mathrm{Func}^{\text{loc.const.}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v), \mathbb{Q})$ (or equivalently $\mathbb{Q}[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v)]^{G_F-\text{fin}}$) is replaced by $\mathbb{Q}_p[\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v)]^{G_F-\text{fin}}$. In fact, it can be shown that *every* semi-simple representation coming from geometry appears as a subquotient of the space of functions on the pro-algebraic completion of $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{0,1,\infty\}, 0_v)$. This then gives an astounding reduction of the Fontaine-Mazur conjecture. For details, see [7].

A Appendix A: The “easy” part of Belyi’s theorem[2]

We first recall Belyi’s theorem:

Theorem A.0.1 (Belyi)**.** *A complex smooth projective curve X is defined over a number field, if and only if there exists a non-constant morphism $f : X \to \mathbb{P}^1_{\mathbb{C}}$ with at most 3 critical values.*

The “only if” part is proved in Section 3.1, the “if” part follows directly from a theorem of Weil (Theorem A.0.2), we will give a proof of this theorem in this section, for the sake of integrity.

Theorem A.0.2 (Weil)**.** *Let $X/\mathbb{C}$ be a projective smooth algebraic curve. If there is a morphism*

$$f : X \to \mathbb{P}^1_{\mathbb{C}}$$

such that all branch values lie in $\overline{\mathbb{Q}}$, then X is defined over $\overline{\mathbb{Q}}$.

Definition A.0.3 (Closed subgroup)**.** Let K be a field. A subgroup G of $\mathrm{Aut}(K)$ is *closed*, if there is a subfield k of K with $G = \mathrm{Aut}(K/k)$.

We will use the following elementary field-theoretic lemma:

Lemma A.0.4. *Let K/k be a field extension. Then,*

1. *Any automorphism of k can be extended to an automorphism of K. Furthermore, we have:*
$$K^{\mathrm{Aut}(K/k)} = k.$$
2. *Let G be a subgroup of $\mathrm{Aut}(K)$, and H be a subgroup of G of finite index. Then the field extension K^H/K^G is finite. If H is a normal subgroup of G or G is closed, then we have $[K^H : K^G] \leq [G : H]$. Moreover, the equality holds if H is closed.*

We also recall a fundamental result in ramification theory:

Proposition A.0.5. *Let S be a finite set of (closed) points of $\mathbb{P}^1_{\mathbb{C}}$, and $d \geq 1$ be a natural number. Then there are at most finitely many isomorphism classes of pairs (X, f) where $X/\mathbb{C}$ is a curve and $f : X \to \mathbb{P}^1_{\mathbb{C}}$ is a finite morphism of varieties over $\mathbb{C}$ of degree d whose branch values lie in S.*

Proof. By translating to the setting of Riemann surfaces, this reduces to the fact that there are at most finitely subgroups of index d of the fundamental group $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus S)$, which is true since $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus S)$ is finitely generated. □

[2] It should be noted that this part is neither easy nor direct. This reason this part is called easy is historical: It follows directly from a (hard) theorem of Weil (Theorem A.0.2), which is proved a lot earlier than the other part of Belyi’s theorem.

Definition A.0.6 (Moduli field)**.** The *moduli field of* (X, f) is the field $M(X, f) := K^{U(X,f)}$ fixed by the group $U(X, f)$ consisting of all $\sigma \in \mathrm{Aut}(K)$ such that there exists an isomorphism $\sigma_X : X^\sigma \to X$ of varieties over K such that the following diagram commutes:

$$\begin{tikzcd}
X^\sigma \arrow[r, "\sigma_X"] \arrow[d, "f^\sigma"] & X \arrow[d, "f"] \\
(\mathbb{P}^1_K)^\sigma \arrow[r, "\mathrm{Proj}(\sigma)"] & \mathbb{P}^1_K .
\end{tikzcd}$$

When $f = 0$, we simply call the field $M(X) := M(X, 0)$ the *moduli field of* X.

Theorem A.0.2 is then the conjunction of the following two lemmas:

Lemma A.0.7. *Let $X/\mathbb{C}$ be a curve, let $f : X \to \mathbb{P}^1_{\mathbb{C}}$ be a finite morphism and let k be a subfield of $\mathbb{C}$ such that the branch values of f are k-rational. Then the moduli field of f is contained in a finite extension of k.*

Proof. For any $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$, the branch values of $f(\sigma) : X^\sigma \overset{t^\sigma}{\longrightarrow} (\mathbb{P}^1_{\mathbb{C}})^\sigma \overset{\mathrm{Proj}(\sigma)}{\longrightarrow} \mathbb{P}^1_{\mathbb{C}}$ also lie in S, and $\deg f(\sigma) = \deg f$. So the $\mathrm{Aut}(\mathbb{C}/K)$-orbit of (the isomorphism class of) the pair (X, f) is finite, by Proposition A.0.5, therefore the stabilizer is of finite index in $\mathrm{Aut}(\mathbb{C}/K)$. Now note that the stabilizer is contained in $U(X, f)$, thus the moduli field $M(X, f) = \mathbb{C}^{U(X,f)}$ is contained in a finite extension of $\mathbb{C}^{\mathrm{Aut}(\mathbb{C}/K)} = K$, by Lemma A.0.4. □

Lemma A.0.8. *X and f are defined over a finite extension of $M(X, f)$.*

Proof. Choose a $\mathbb{Q}$-rational point $y_0 \in \mathbb{P}^1_K(\mathbb{Q}) \setminus S$, and a point x_0 in the fibre $f^{-1}(y_0)$. By Riemann-Roch, there is a meromorphic function $g \in K(X) \setminus K$ such that x_0 is the only pole of g. Then we have $K(X) = K(f, g)$ (as the field extension $K(X)/K(f, g)$ is a subextension of $K(X)/K(f)$ and of $K(X)/K(g)$, hence the corresponding morphism of curves is both unramified and totally ramified at x_0). We assume that we have chosen g in such a way that the order m of the pole is minimal. Then we have

$$T := \{f \in K(X) \mid \mathrm{ord}_{x_0}(f) \geq -m \text{ and } \mathrm{ord}_x(f) \geq 0 \text{ for all } x \in X \setminus \{x_0\}\} = K \oplus Kg;$$

since for any $f_1, f_2 \in T$ with $\mathrm{ord}_{x_0}(f_i) = -m$, $i = 1, 2$, there is a constant $\alpha \in K$ with $-\mathrm{ord}_{x_0}(f_1 - \alpha f_2) < m$, and then $f_1 - \alpha f_2$ is a constant function, as m is minimal. By the choice of y_0, the meromorphic function $f - y_0$ on X is a local parameter on X in x_0; if $K = \mathbb{C}$, this means, in the language of Riemann surfaces, that $f - y_0$ yields a chart of $X(\mathbb{C})$ in a neighborhood of x_0 which maps x_0 to 0. There is a unique function $g' \in T$ such that the leading coefficient and the constant coefficient in the Laurent expansion of g' with respect to the local parameter $f - y_0$ are equal to 1 and 0, respectively. We then assume that $g = g'$. We now claim that the minimal polynomial of g over $K(f)$ has coefficients in $k(f)$ where k is a finite extension of $M(X, t)$. Then, the field extension $K(X)/K(f)$ is defined over k. By the dictionary between curves and function fields, this means Lemma A.0.8 is proved.

As for the proof of the above claim, we denote by $U(X, f, x_0)$ the subgroup of $U(X, f)$ consisting of all $\sigma \in \mathrm{Aut}(K)$ such that there is an isomorphism $\sigma_X : X^\sigma \to X$ of curves over K such that the diagram

$$\begin{tikzcd}
X^\sigma \arrow[r, "\sigma_X"] \arrow[d, "f^\sigma"] & X \arrow[d, "f"] \\
(\mathbb{P}^1_K)^\sigma \arrow[r, "\mathrm{Proj}(\sigma)"] & \mathbb{P}^1_K
\end{tikzcd}$$

commutes and such that $\sigma_X(x_0^\sigma) = x_0$, where x_0^σ denotes the point on X^σ/K corresponding to x_0. Note that σ_X is unique since $\mathrm{Aut}(f)$ acts freely on the fibre $f^{-1}(y_0)$. Thus, mapping σ to the automorphism of the function field $K(X)$ induced by σ_X yields an action of $U(X, f, x_0)$ on $K(X)$ by K-semilinear field automorphisms which fix $f \in K(X)$. Being the stabilizer of $[x_0]$ under the action $(\sigma, [x_0]) \mapsto [\sigma_X(x_0^\sigma)]$ of $U(X, f)$ on $f^{-1}(x_0)/\mathrm{Aut}(f)$, the subgroup $U(X, f, x_0)$ has finite index in $U(X, f)$. The meromorphic function $g \in K(X)$ and hence the minimal polynomial of g over $K(f)$ are invariant under the action of $U(X, f, x_0)$ defined above since the image of g under $\sigma \in U(X, f, x_0)$ has the same three defining properties as g. Now applying Lemma A.0.4 completes the proof of the claim (thus also the proof of Lemma A.0.8). □

Remark A.0.9. From the proof we actually see that X and f are defined over $M(X, f)$ itself provided that f is Galois.

We can now prove Theorem A.0.2.

Proof of Theorem A.0.2. The theorem follows directly from Lemma A.0.7 and Lemma A.0.8. □

B Appendix B: Estimation of oriented binary trees

We establish some combinatorial estimations for getting the claimed estimation 7.1.11 in Section 7.1.

First we recall the definition of oriented binary trees for the sake of integrity.

Definition B.0.1 (Oriented binary tree)**.** An *oriented binary tree* is a pair $(\mathcal{T}, \varphi)$, where $\mathcal{T}$ is a binary tree, and φ is an orientation of the dual graph of $\mathcal{T}$, in the sense of Definition 7.1.6.

We also have a notion of rooted oriented binary trees:

Definition B.0.2 (Rooted oriented binary tree)**.** An *rooted oriented binary tree* is a triple $(\mathcal{T}, \varphi, v)$, where $(\mathcal{T}, \varphi)$ form an oriented binary tree, and v is a degree-1 vertex.

Note that we have natural notions of isomorphism for both oriented binary trees and rooted oriented binary trees.

Now recall that we want to estimate the number of isomorphism classes of oriented binary trees on $2n$ vertices, as Theorem 7.1.11 states that this number is exactly the number of linearly-equivalent classes of pairs (f, g) obtaining the minimal degree $\deg(f^3 - g^2) = n+1$. For this, we first count the number F_n of isomorphism classes of *rooted* oriented binary trees on $2n$ vertices. It turns out that this number is easier to count directly.

Proposition B.0.3. *The number F_n of isomorphism classes of rooted oriented binary trees on $2n$ vertices satisfy the following asymptotic formula*

$$F_n \sim c n^{-3/2} 4^n.$$

Proof. Note that we may split such a rooted oriented oriented binary tree into a pair of new (co-)rooted oriented binary trees by taking out the old root, ordered according to the orientation attached to the face associated to the unique neighbour of the old root, giving rise to the following recurrence formula

$$F_n = \sum_{i+j=n} F_i F_j.$$

Clearly we have $F_0 = 0$, $F_1 = 1$ by definition. Therefore we have the following identity for the generating function $F(x) = \sum_{n=0}^{\infty} F_n x^n$:

$$F(x) = x + F^2(x),$$

thus

$$F(x) = \frac{1}{2}(1 - \sqrt{1-4x}),$$

this tells us

$$F_n = (-1)^{n-1} \frac{1}{2} 4^n \binom{1/2}{n} = \frac{\binom{2n}{n}}{2(2n-1)} \sim c n^{-3/2} 4^n,$$

for a constant $c > 0$ independent of n. □

We can now estimate the number ϕ_n of isomorphism classes of oriented binary trees on $2n$ vertices.

Theorem B.0.4. *The number ϕ_n of isomorphism classes of $\mathfrak{S}_3$-trees on $2n$ vertices satisfy the following inequality*

$$c_1 n^{-5/2} 4^n < \phi_n < c_2 n^{-3/2} 4^n$$

for some positive reals c_1, c_2 independent of n.

Proof. Consider the surjective forgetful map from the set of isomorphic classes of *rooted* oriented binary trees on $2n$ to the set of isomorphism classes of oriented binary trees on $2n$ vertices, then the number of elements of each fiber is between 1 and $2n$ by definition, therefore

$$\frac{1}{2n} F_n \leq \phi_n \leq F_n,$$

applying Proposition B.0.3 then gives the desired inequality

$$c_1 n^{-5/2} 4^n < \phi_n < c_2 n^{-3/2} 4^n$$

for some positive reals c_1, c_2 independent of n. □

C Appendix C: Basic height theory revisited

We recite some basics of the height theory from Diophantine geometry in this section.

Generally speaking, heights are functions from the set of algebraic points on a variety to $\mathbb{R}$, that allow us to "count" algebraic points on varieties. It possesses a certain finiteness property which claims that a set of points with bounded height and degree is necessarily finite.

We first define heights on projective spaces $\mathbb{P}^n$.

Assumption C.0.1. We assume K is one of the following:

- Number field: i.e. a finite extension $K/\mathbb{Q}$;
- Function field: i.e. $K = k(B)$, where k is an arbitrary field, and B is a geometrically integral smooth projective curve over k.

Remark C.0.2. In some applications (e.g. Mordell-Weil theorem), we also require k is finite. Then Assumption C.0.1 is just saying K is a global field.

Notation C.0.3 (Valuations and places)**.**

- Number field: Let $K/\mathbb{Q}$ be a finite extension. We use $M_K, M_{K,f}, M_{K,\infty}$ to denote the set of places of K, the set of finite places of K, the set of infinite places of K, respectively. Then a finite place $v \in M_{K,f}$ corresponds to a prime ideal $\wp_v \subset \mathcal{O}_K$, and the *$v$-adic norm* is given by
$$|x|_v = N(\wp_v)^{-\operatorname{ord}_v(x)},$$
where
$$N(\wp_v) = \#(\mathcal{O}_K/\wp_v)$$
denotes the norm of $\wp_v$; and an infinite place v corresponds to an embedding $\sigma_v : K \to \mathbb{C}$, and the *$v$-adic norm* is given by the restriction of the complex absolute value.
- Function field: Let $K = k(B)$ be a function field over k. We use M_K to denote the set of places of K. Then a place $v \in M_K$ corresponds to a closed point of B, and the *v-adic norm* is given by
$$|x|_v = e^{-\deg(v)\cdot\operatorname{ord}_v(x)}$$
where
$$\deg(v) = [k(v) : k]$$
denotes the degree of the residue field at v.

Theorem C.0.4 (Product formula)**.** *Let K be a field satisfying Assumption C.0.1, then we have*
$$\prod_{v\in M_K} |x|_v = 1,$$
for any $x \in K^\times$.

Proof. We omit the proof and refer the interested reader to [6]. □

Remark C.0.5. The product formula C.0.4 plays a fundamental role in Diophantine Geometry, e.g., in the well-definedness of the naive height on projective space, the development of intersection theory on arithmetic varieties...

Definition C.0.6 (Naive height on $\mathbb{P}^n$)**.** Let K be a field satisfying Assumption C.0.1, define the naive height

$$h = h_K : \mathbb{P}^n(\overline{K}) \to \mathbb{R}$$

by

$$h_K(x_0, \ldots, x_n) = \frac{1}{[K' : K]} \sum_{v \in M_{K'}} \log \max\{|x_0|_v, \ldots, |x_n|_v\},$$

where K' is a finite extension of K containing all the coordinates $x_0, \ldots, x_n \in \overline{K}$.

Remark C.0.7. By a direct computation we may verify that Definition C.0.6 is independent of the choice of K'. Independence of coordinates is guaranteed by the product formula C.0.4.

Proposition C.0.8.

(1) $h(x) \geq 0$*;*

(2) $h(x) = 0$ *if and only if* $x = 0$ *or* x *is a root of unity;*

(3) $h(x_0^m, \ldots, x_n^m) = |m| \cdot h(x_0, \ldots, x_n)$*.*

Proof. The first claim follows from product formula C.0.4. Number field case of the second claim is a well-known result, whereas the function field case is by direct verification, so is the third claim. □

The following result ensured that we could use height to "count" algebraic points.

Theorem C.0.9 (Northcott property)**.** *Let* K *be a global field. Then the set*

$$\{x \in \mathbb{P}^n(\overline{K}) \mid \deg(x) < c_1, h(x) < c_2\}$$

is finite, for any $c_1, c_2 \in \mathbb{R}$*.*

Proof. We omit the proof and refer the interested readers to [9]. □

We can now define heights on general projective varieties.

Convention C.0.10. In our context, a variety is an integral scheme which is separated and of finite type over the base field; a curve is a 1-dimensional variety; a surface is a 2-dimensional variety.

The upshot is that we embed projective varieties into $\mathbb{P}^n$, and use the heights induced by the heights C.0.6 on $\mathbb{P}^n$.

Definition C.0.11 (Naive height on projective varieties)**.** Let X/K be a projective variety, L an ample line bundle on X, and

$$i : X \to \mathbb{P}^N_K$$

a close immersion, with

$$i^*\mathcal{O}_{\mathbb{P}^N_K}(1) \cong mL$$

for some integer $m \geq 1$. Then *the height*

$$h_{(L,m,i)} : X(\overline{K}) \to \mathbb{R}$$

associated to the triple (L, m, i) is the composition of

$$X(\overline{K}) \xrightarrow{i} \mathbb{P}^N_K(\overline{K}) \xrightarrow{\frac{1}{m}h} \mathbb{R},$$

where h is the naive height on $\mathbb{P}^n$ defined in Definition C.0.6.

The following theorem shows that, the height $h_{(L,m,i)}$ in Definition C.0.11 only depends on L, up to $O(1)$. Moreover, non-ample line bundles can also induce heights in a somewhat natural way, giving lots of heights on a variety. For this reason, Theorem C.0.12 is called the height machine.

Theorem C.0.12 (Height machine)**.** *Let K be a field satisfying Assumption C.0.1, and X/K a projective variety. Then there exists a unique homomorphism*

$$\mathcal{H} : \mathrm{Pic}(X) \to \{\text{maps } X(\overline{K}) \to \mathbb{R}\}/\{\text{bounded maps}\}, L \mapsto \mathcal{H}_L,$$

such that

$$\mathcal{H}_L = h_{(L,m,i)} + O(1),$$

for any ample line bundle L on X, and close immersion

$$i : X \to \mathbb{P}^n$$

with

$$i^*\mathcal{O}_{\mathbb{P}^n}(1) \cong mL.$$

Remark C.0.13. The uniqueness of $\mathcal{H}$ is already contained in the statement of Theorem C.0.12, as any line bundle can be written as a difference of two very ample ones. The hard part is actually the existence of such an $\mathcal{H}$. As for a complete proof, we refer the interested readers to [9].

We call the heights given by the height machine C.0.12 *Weil heights.*

Definition C.0.14 (Weil height)**.** Let K and X/K be as above. For any line bundle L on X, any function

$$h_L : X(\overline{K}) \to \mathbb{R}$$

in the class $\mathcal{H}_L$ is called a *Weil height* associated to L.

We have a projection formula for Weil heights.

Corollary C.0.15 (Projection formula). *Let K be a field satisfying Assumption C.0.1, and $f : X' \to X$ a morphism of varieties over K. Let $L \in \operatorname{Pic}(X)$ be a line bundle on X. Then*

$$h_{f^*L} = f^* h_L + O(1).$$

i.e., the following diagram

$$\begin{tikzcd} X'(\overline{K}) \arrow[rr, "f"] \arrow[dr, "h_{f^*L}"'] & & X(\overline{K}) \arrow[dl, "h_L"] \\ & \mathbb{R} & \end{tikzcd}$$

commutes up to $O(1)$.

We also have Northcott property for Weil heights.

Theorem C.0.16 (Northcott property). *Let K be a global field, X/K a projective variety, L an ample line bundle on X, and $h_L : X(\overline{K}) \to \mathbb{R}$ the associated Weil height. Then the set*

$$\{x \in X(\overline{K}) \mid \deg(x) < c_1, h(x) < c_2\}$$

is finite, for any $c_1, c_2 \in \mathbb{R}$.

Proof. This follows directly from the Northcott property C.0.9 for the naive height on $\mathbb{P}^n$. □

The following interpretation of Weil heights as an intersection number justifies our definition.

Theorem C.0.17 (Height = intersection number). *Let $K = k(B)$ be a function field, where B is a regular and geometrically integral projective curve. Let*

$$h : \mathbb{P}^n(\overline{K}) \to \mathbb{R}$$

be the naive height on $\mathbb{P}^n_{\overline{K}}$. Then

$$h(x) = \frac{1}{\deg(x)} \deg(\mathcal{O}_{\mathbb{P}^n_B}(1)|_{\tilde{x}}),$$

for any $x \in \mathbb{P}^n(\overline{K})$, where $\tilde{x} \subset \mathbb{P}^n_B$ is the zariski closure of the image of the composition of

$$\operatorname{Spec} \overline{K} \to \mathbb{P}^n_K \to \mathbb{P}^n_B.$$

Proof. By base change, we may assume $\deg(x) = 1, x \in \mathbb{P}^n(K)$, and $\tilde{x}$ is the section corresponding to x. Then the equation becomes

$$h(x) = \deg(\mathcal{O}_{\mathbb{P}^n_B}(1)|_{\tilde{x}}).$$

Note that $\deg(\mathcal{O}_{\mathbb{P}^n_B}(1)|_{\tilde{x}})$ is just the intersection number $H \cdot \tilde{x}$ for any hyperplane section H of $\mathbb{P}^n_B$, for which we have

$$H \cdot \tilde{x} = \sum_{\substack{v \in B \\ \text{closed point}}} m_v \deg(v),$$

where the $m_v \geq 0$ are the intersection multiplicities. Now write $x = (x_0, \ldots, x_n)$ with $x_i \in K$ and $x_0 \neq 0$. Then take $H = \mathrm{V}(x_0)$ in $\mathbb{P}^n_B$. By a direct computation we see that

$$m_v = \mathrm{ord}_v(x_v) - \min_{0 \leq i \leq n} \{\mathrm{ord}_v(x_i)\},$$

for any closed point $v \in B$. This then completes the proof of Theorem C.0.17. □

Corollary C.0.18 (General version of Theorem C.0.17)**.** *Let $K = k(B)$ be as in Theorem C.0.17, X/K a projective variety, and L a line bundle on X. Let $(\mathcal{X}, \mathcal{L})$ be an integral model of (X, L) over B. Then the function*

$$h_{\mathcal{L}} : X(\overline{K}) \to \mathbb{R}, \; x \mapsto \frac{1}{\deg(x)} \deg(\mathcal{L}|_{\tilde{x}})$$

is a Weil height associated to L, where $\tilde{x}$ is the zariski closure of the image of the composition

$$\operatorname{Spec} \overline{K} \xrightarrow{x} X \to \mathcal{X}.$$

Remark C.0.19. In the number field (i.e. "arithmetic") case, by adding Hermitian metrics as part of the data "at ∞", and developing intersection theory in parallel, we may obtain a function (analogous to the one defined above)

$$h_{\overline{\mathcal{L}}} : X(\overline{K}) \to \mathbb{R}, \; x \to \frac{1}{\deg(x)} \overline{\mathcal{L}} \cdot \tilde{x},$$

where $(\mathcal{X}, \overline{\mathcal{L}})$ is an "arithmetic model" of (X, L), and $\tilde{x}$ is the zariski closure of the image of the composition

$$\operatorname{Spec} \overline{K} \xrightarrow{x} X \to \mathcal{X}.$$

The upshot is that we can use this "height" function to develop height machine in the number field case in parallel to our original approach. In fact, this is exactly the fundamental idea of Arakelov theory.

We include the following result used in Section 7.2 for the sake of integrity.

Theorem C.0.20 (Néron)**.** *Let X be a non-singular projective variety, L and L_1 be two elements of* $\mathrm{Pic}(X)$*, with* $\deg L = 0$ *and L_1 ample. Then we have*

$$|h_L(x)| \leq O(\sqrt{h_{L_1}(x)} + 1).$$

Proof. See Serre's book [9]. □

D Appendix D: Étale fundamental group revisited

In the setting of algebraic geometry, the topological fundamental group of the underlying (Zariski) topological space contains very little information about the scheme, as Zariski topology is very "coarse" in some sense. The key is to encapsulate the essence of covering theory in a more categorical way, i.e. the so-called Grothendieck's Galois theory; and to realize that, (finite) étale morphisms in algebraic geometry are the analog of (finite) coverings in classical topology. However, many technical details arise. For example, there are no analog of universal covering in the setting of schemes, one would have to either choose to interpret the "algebraic fundamental group" of a scheme as an automorphism group of the category of finite étale morphisms over the scheme, or enlarge the category of schemes so that an "universal covering" may exist. Our approach here is the former.

We work under the framework of Grothendieck's Galois theory formalism. For details, see [11]. We first recall some notions from this framework, for the sake of integrity.

Definition D.0.1 (Galois category)**.** A *Galois category* is a pair $(\mathcal{C}, F)$, where $\mathcal{C}$ is a category and $F : \mathcal{C} \to Fin$ is a functor from $\mathcal{C}$ to the category of finite sets, such that

(1) $\mathcal{C}$ has finite limits and finite colimits;

(2) Every object in $\mathcal{C}$ is a finite coproduct of connected objects in $\mathcal{C}$;

(3) F detects isomorphisms and is exact.

Here an object X in $\mathcal{C}$ is called *connected* if $\operatorname{Aut}(X)$ acts freely on X. The functor F is usually addressed as the *fiber functor* of the Galois category $(\mathcal{C}, F)$.

Example D.0.2. Take $\mathcal{C}$ to be the category of finite coverings of a fixed pointed (locally simply connected) space, and F to be the literal "fiber" functor. Then $(\mathcal{C}, F)$ form a Galois category. This is one of the most import examples to keep in mind.

The "universal Galois group" $\operatorname{Aut}(F) := \varprojlim_X \operatorname{Aut}(F(X))$ in fact determines completely the structure of $\mathcal{C}$:

Theorem D.0.3. *Let $\mathcal{C}$ be a Galois category with fiber functor F, and $G = \operatorname{Aut}(F)$ be the profinite automorphism group of F. Then there is an equivalence of categories between $\mathcal{C}$ and the category $GFin$ of finite G-sets.*

After some easy checking, we may obtain:

Proposition D.0.4. *Let X be a connected scheme with a geometric point $\overline{x} : \operatorname{Spec} \overline{k} \to X$. Then the category $\mathbf{F\acute{E}t}_X$ of finite étale morphisms to X, together with the induced fiber functor*

$$F_{\overline{x}} : \mathbf{F\acute{E}t}_X \to \mathbf{Fin},\ (f : Y \to X) \mapsto |Y_{\overline{x}}|,$$

form a Galois category.

We can now define the étale fundamental group.

Definition D.0.5 (Étale fundamental group)**.** Let X be a connected scheme with a geometric point $\overline{x} : \operatorname{Spec} \overline{k} \to X$, and $F_{\overline{x}}$ be as above. Then the *étale fundamental group* $\pi_1^{\text{ét}}(X, \overline{x})$ *of* X *at* $\overline{x}$ is the automorphism group $\operatorname{Aut}(F_{\overline{x}})$ of $F_{\overline{x}}$.

By a routine reduction to curve case, in which we apply Grothendieck's comparison theorem along with a result of Shafarevich (see [11]), we see that:

Theorem D.0.6 (Grothendieck)**.** *Let X be a smooth projective scheme over an algebraically closed field k, and $\overline{x} : \operatorname{Spec} \overline{k} \to X$ be a geometric point. Then $\pi_1^{\text{ét}}(X, \overline{x})$ is topologically finitely generated as a profinite group.*

Remark D.0.7. The curve case can also be proved by deforming the curve to a curve of characteristic zero, for which the result follows from Lefschetz principle and the structure of the topological fundamental group of Riemann surfaces of finite type. Moreover, by applying de Jong's theory of alterations, we may only assume X is connected in Theorem D.0.6. Note that even properness of X is not necessary to deduce topologically finitely generatedness.

It is sometimes of great benefit to also have a notion of étale fundamental groups at certain "missed" points of a scheme, e.g., the "point" 0 of the truncated projective line $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}$. This is the so-called "étale fundamental group with tangential basepoints", which we will now discuss.

Definition D.0.8 (Tangential basepoint)**.** Let X be an integral proper normal curve over a field k. A *k-rational tangential basepoint of X* is just a $k((t))$-point $x_v : \operatorname{Spec} k((t)) \to X$ of X.

Remark D.0.9. Let $\overline{X}$ be the compactification of X, then such a x_v in Definition D.0.8 gives a k-rational point $x : \operatorname{Spec} k \to \overline{X}$ along with a tangent vector $v \in T_x\overline{X}$ given by the parameter t, hence the name. These data allow us to recover more information from the fiber over x_v compared to x, such as the ramification indices over x.

The following theorem of Deligne allow us to apply Grothendieck's Galois theory formalism as in Definition D.0.5.

Theorem D.0.10 (Deligne)**.** *Let X be an integral normal curve over a field k of characteristic 0, and $x_v : \operatorname{Spec} k((t)) \to X$ be a k-rational tangential basepoint. Then the category FÉt$_X$ of finite étale morphisms to X, together with the induced fiber functor*

$$F_{x_v} : \mathbf{F\acute{E}t}_X \to \mathbf{Fin},\ (f : Y \to X) \mapsto \{(y, e) \mid y \in \overline{f}^{-1}(x), e \in \overline{f}^{-1}(v) \cap T_y\overline{Y}\},$$

form a Galois category.

We can now make the following definition.

Definition D.0.11. Let X be an integral normal curve over a field k of characteristic 0, and $x_v : \operatorname{Spec} k((t)) \to X$ be a k-rational tangential basepoint. Then the *étale fundamental group* $\pi_1^{\text{ét}}(X, x_v)$ *of* X *at* x_v is the automorphism group $\operatorname{Aut}(F_{x_v})$ of F_{x_v}.

References

[1] N. D. Elkies, ABC implies Mordell. *International Mathematics Research Notices*, **1991**, no. 7, 99–109.

[2] E. Girondo and G. González-Diez, *Introduction to compact Riemann surfaces and dessins d'enfants*. London Math. Soc. Stu. Texts 79, Cambridge Univ. Press, 2012.

[3] A. Grothendieck, *Esquisse d'un Programme*, Preprint, 1985.

[4] B. Köck, Belyi's theorem revisited. *Beiträge Algebra Geom.*, **45** (2004), no.1, 253–265.

[5] W. Melanie, Belyi-extending maps and the Galois action on dessins d'enfants, *Publications of the Research Institute for Mathematical Sciences*, **42** (2006), 721–737.

[6] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.

[7] A. Petrov, *Universality of the Galois action on the fundamental group of* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, arXiv: 2109.09301 (2021).

[8] L. Schneps, Dessins d'enfants on the Riemann sphere, in *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lect. Note Ser. 200, Cambridge Univ. Press, 1994.

[9] J-P. Serre, *Lectures on the Mordell-Weil Theorem*, Springer, 1997.

[10] G. Shabat and V. Voevodsky, Drawing curves over number fields, in *The Grothendieck Festschrift, Volume III*, Springer, 2007.

[11] A. Shmakov, *Galois Representations in Étale Fundamental Groups and the Profinite Grothendieck-Teichmüller Group*, Preprint.

[12] X. Yuan, *Lectures on Arakelov geometry*, lecture notes, 2022.

[13] U. Zannier, On Davenport's bound for the degree of $f^2 - g^3$ and Riemann's Existence Theorem, *Acta Arithmetica*, **71** (1995), no. 2, 107–137.

[14] Y. Zhao, *Géométrie Algébrique et Géométrie Analytique*, unpublished notes, 2013.

[15] A. Zvonkine, Belyi functions: examples, properties, and applications. *Application of Group Theory to Combinatorics*, Jul 2007, Pohang, South Korea. pp. 161–180.