ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.05
https://doi.org/10.26493/1855-3974.2764.fe5
(Also available at http://amc-journal.eu)

Regular dessins with moduli fields of the form $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$*

Nicolas Daire

Département de Mathématiques et Applications, École Normale Supérieure, 45 rue d'Ulm, 75005 Paris, France

Fumiharu Kato, Yoshiaki Uchino

Department of Mathematics, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro, Tokyo 152-8551, Japan

Received 10 December 2021, accepted 29 March 2023, published online 27 September 2023

Abstract

Gareth Jones asked during the 2014 SIGMAP conference for examples of regular dessins with nonabelian fields of moduli. In this paper, we first construct dessins whose moduli fields are nonabelian Galois extensions of the form $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$, where p is an odd prime and ζ_p is a pth root of unity and $q \in \mathbb{Q}$ is not a pth power, and we then show that their regular closures have the same moduli fields. Finally, in the special case $p = q = 3$ we give another example of a regular dessin of degree $2^{19} \cdot 3^4$ and genus 14155777 with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$.

Keywords: Dessins d'enfants, coverings.

Math. Subj. Class. (2020): 14H57, 14H30

1 Introduction

Grothendieck first coined the term *Dessin d'enfant* in *Esquisse d'un Programme* [4] to denote a connected bicolored graph embedded on a compact connected oriented topological surface. The study was motivated by the one to one correspondance between dessins d'enfant, the combinatorial data of the associated cartographical group, and the geometric concept of coverings of $\mathbb{P}^1$ by compact Riemann surfaces ramified at most over three

*The authors are grateful to Professor Jürgen Wolfart for valuable comments.

E-mail addresses: nicolas.daire@ens.psl.eu (Nicolas Daire), bungen@math.titech.ac.jp (Fumiharu Kato), uchino.y.ab@m.titech.ac.jp (Yoshiaki Uchino)

points. Moreover, by Belyi's theorem any such covering is given the structure of an algebraic curve defined over a number field, therefore we obtain a natural action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the set of isomorphism classes of dessins. A lot of the interest for dessins stems from the fact that this action is faithful, providing a way to study the absolute Galois group through its action on the set of dessins. A particularly interesting family of dessins is that of regular dessins, characterized by the fact that their automorphism groups act transitively on their sets of edges, and the Galois action was proved to remain faithful when restricted to the subset of isomorphism classes of regular dessins [3].

To any dessin we associate a number field called its moduli field, which is defined as the subfield of $\bar{\mathbb{Q}}$ fixed by the subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that fixes the dessin up to isomorphism. Conder, Jones, Streit and Wolfart noted in [1] that the moduli fields of all the examples of regular dessins known at the time were abelian Galois extensions of $\mathbb{Q}$. Herradón constructed in [6] an explicit equation for a regular dessin whose moduli field $\mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension of $\mathbb{Q}$, and Hidalgo later generalized his construction in [7] to produce regular dessins whose moduli fields are of the form $\mathbb{Q}(\sqrt[p]{2})$ where p is an odd prime number. However there is as of yet no known example of regular dessin whose moduli field is a nonabelian Galois extension of $\mathbb{Q}$. This is the starting point of this paper, in which we will exhibit examples of regular dessins with moduli fields that are nonabelian Galois extensions of $\mathbb{Q}$.

In the present paper, we begin by recalling the main definitions and results on dessins d'enfant. We will then expose constructions of regular dessins whose moduli fields are nonabelian Galois extensions of $\mathbb{Q}$. We first exhibit dessins whose moduli fields are of the form $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$, where ζ_3 is a primitive third root of unity and $q \in \mathbb{Q}$ is not a third power, and show that the regular closures of these dessins possess the same moduli fields. We then generalize this construction to show that there exist regular dessins with moduli fields $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$, where ζ_p is a primitive pth root of unity and $q \in \mathbb{Q}_{>0}$ is not a pth power. Finally, we give an example of a regular dessin of degree $2^{19} \cdot 3^4$ and genus 14155777 with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$.

Notations

- $\mathfrak{S}_E$: the group of self-bijections of the set E, similarly $\mathfrak{S}_n$ is the group of permutations of a set of n elements (we favor a right action, hence we write the product $\sigma\tau \coloneqq \tau \circ \sigma$)
- $\mathrm{Gal}(E/F)$: the Galois group of F-automorphisms of E
- ζ_k: the kth primitive root of unity $\exp(\frac{2i\pi}{k})$
- F_2: the free group of rank 2 with generators (ξ, η)
- Crit: the set of critical values of a function

2 Preliminaries on dessins d'enfant

We refer the reader to existing expositions of the theory such as [5, 8, 9] and [2] for proofs of the presented facts and further details.

A *dessin d'enfant* is a connected bipartite graph embedded on a compact connected orientable topological surface, such that the complement of the graph is a disjoint union of

2-cells. Two such dessins are equivalent if there exists an orientation preserving homeomorphism between the underlying surfaces that induces an isomorphism between the embedded bipartite graphs.

A dessin is determined up to isomorphism by a pair (C, β) where C is a smooth algebraic curve and $\beta\colon C \to \mathbb{P}^1$ is a meromorphic mapping ramified at most over $\{0, 1, \infty\}$, and by Belyi's theorem we can further ask for C and β to both be defined over a number field. We call (C, β) a *Belyi pair* and β a *Belyi function*. The corresponding graph embedding on the underlying surface is recovered by pulling back the segment $[0, 1]$ along β, we define black and white vertices as the preimages of 0 and 1 respectively, and the edges as the preimages of $]0, 1[$.

By covering theory a dessin is also determined up to isomorphism by the *monodromy action* of the fundamental group of the complex projective line $\pi_1(\mathbb{P}^1)$ on the fiber over the point $\frac{1}{2}$ which is identified to the set of edges of the dessin. The fundamental group $\pi_1(\mathbb{P}^1)$ is isomorphic to the free group of rank two $F_2 = \langle \xi, \eta \rangle$ with generators ξ and η which are two loops with base point $\frac{1}{2}$ and circling counter-clockwise around 0 and 1 respectively. The monodromy action of the generators ξ and η then corresponds to the product of the counter-clockwise cyclic permutation of the edges around black and white vertices respectively. We call *monodromy map* $M\colon F_2 \to \mathfrak{S}_E$ the map that associates to each element of F_2 the corresponding permutation of the set of edges, and we call *cartographic group* the image of the monodromy map, which is a transitive subgroup of the group of permutations of the set of edges.

When the *automorphism group* of a dessin $\mathcal{D}$ acts transitively on the set of edges, we say that $\mathcal{D}$ is a *regular dessin*. When that is the case the cartographic group G acts transitively and freely on the set of edges, the monodromy action is thus given by the canonical action of G on itself. There is a natural bijection between regular dessins and finite groups generated by two distinguished elements ξ and η up to isomorphism. Two regular dessins determined by $G_1 = \langle \xi_1, \eta_1 \rangle$ and $G_2 = \langle \xi_2, \eta_2 \rangle$ respectively are isomorphic if and only if there exists an isomorphism between G_1 and G_2 that preserves the distinguished generators. Given a dessin $\mathcal{D}$, there exists a unique regular dessin $\widetilde{\mathcal{D}}$ with a morphism $\phi\colon \widetilde{\mathcal{D}} \to \mathcal{D}$ such that any morphism from a regular dessin to $\mathcal{D}$ factors through ϕ. We call $\widetilde{\mathcal{D}}$ the *regular closure* of $\mathcal{D}$. Moreover, there exists an isomorphism $\mathrm{Cart}(\widetilde{\mathcal{D}}) \cong \mathrm{Cart}(\mathcal{D})$ that preserves the distinguished generators. There exists a natural action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the set of isomorphism classes of dessins, we denote by $\mathcal{D}^\sigma$ the action of an automorphism σ on a dessin $\mathcal{D}$, and this Galois action commutes with regular closure, i.e. we have $(\widetilde{\mathcal{D}})^\sigma \cong \widetilde{(\mathcal{D}^\sigma)}$.

Given a dessin $\mathcal{D}$, we say that a number field k is a *field of definition* of $\mathcal{D}$ if $\mathcal{D}$ is isomorphic to a dessin defined over k. However there does not necessarily exist a smallest field of definition. We thus define the *moduli field* of a dessin $\mathcal{D}$ as the subfield of $\bar{\mathbb{Q}}$ fixed by the subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ constituted of the elements fixing $\mathcal{D}$ up to isomorphism. The moduli field of a dessin is contained in all fields of definition but is not necessarily itself a field of definition, however it is the case in particular for regular dessins.

3 Constructions of regular dessins with nonabelian moduli fields

We are now ready to give examples of regular dessins whose moduli fields are nonabelian Galois extensions of $\mathbb{Q}$. To do so, we will first exhibit dessins with such moduli fields, and then prove that their regular closures admit the same moduli fields.

Before proceeding with the examples, let us first present a classic family of Belyi polynomials that we will use in the following constructions. For positive integers $m, n \in \mathbb{N}$ we define the polynomial

$$B_{m,n} \coloneqq \frac{(m+n)^{m+n}}{m^m n^n} X^m (1-X)^n \in \mathbb{Q}[X].$$

By computing the derivative $B'_{m,n} = \frac{(m+n)^{m+n}}{m^m n^n} X^{m-1}(1-X)^{n-1}(m-(m+n)X)$ we verify that $B_{m,n} : \mathbb{P}^1 \to \mathbb{P}^1$ is a Belyi function that ramifies only at 0, 1, ∞ and $\frac{m}{m+n}$ with ramification indices m, n, $m+n$ and 2 respectively, and $B_{m,n}(0) = 0$, $B_{m,n}(1) = 0$, $B_{m,n}(\infty) = \infty$ and $B_{m,n}(\frac{m}{m+n}) = 1$ (see Figure 1).

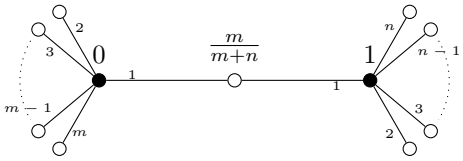


Figure 1: Dessin corresponding to the Belyi pair $(\mathbb{P}^1, B_{m,n})$.

3.1 Regular dessins with moduli fields of the form $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$

Let $q \in \mathbb{Q}_{>0}$ be a positive rational number that is not a third power.

Let $m, n \in \mathbb{N}$ be coprime positive integers such that $\frac{27}{27+q^2} = \frac{m}{m+n}$, and let

$$C\colon y^2 = x(x-(1-\zeta_3))(x-\sqrt[3]{q}),$$
$$\beta\colon C \to \mathbb{P}^1,\ (x,y) \mapsto \frac{1}{27^m q^{2n}}(x^6+27)^m(q^2-x^6)^n.$$

The function β is given by the composition $\beta = \beta_1 \circ \beta_0 \circ \pi$ of the following maps.

1. $\pi\colon C \to \mathbb{P}^1$ is the projection on the coordinate x, which is ramified over $\{0, 1-\zeta_3, \sqrt[3]{q}, \infty\}$.
2. $\beta_0 \coloneqq X^6 \in \mathbb{Q}[X]$, $\mathrm{Crit}(\beta_0) = \{0\}$ so $\beta_1 \circ \pi$ ramifies over $\{0, (1-\zeta_3)^6 = -27, q^2, \infty\}$.
3. $\beta_1 \coloneqq B_{m,n}(\frac{X+27}{q^2+27})$, so $\beta = \beta_1 \circ \beta_0 \circ \pi$ ramifies over $\{0, 1, \infty\}$.

The pair (C, β) is thus a Belyi pair, and we call $\mathcal{D}$ the corresponding dessin. The dessin $\mathcal{D}$ is defined over $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$, so its moduli field is a subfield of $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$. By taking the regular closure we then obtain the inclusion of moduli fields $\mathcal{M}(\widetilde{D}) \subseteq \mathcal{M}(D) \subseteq \mathbb{Q}(\zeta_3, \sqrt[3]{q})$, and moreover $\widetilde{D}$ is regular so it is defined over $\mathcal{M}(\widetilde{D})$. We shall prove that $\mathcal{M}(\widetilde{\mathcal{D}})$ is in fact exactly $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$, which is a nonabelian Galois extension of $\mathbb{Q}$ with Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{q})/\mathbb{Q}) \cong \mathfrak{S}_3.$$

To that end we must show that an automorphism $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ fixes $\widetilde{\mathcal{D}}$ if and only if it fixes ζ_3 and $\sqrt[3]{q}$, or equivalently that $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{q})/\mathbb{Q})$ acts freely on the orbit of $\widetilde{\mathcal{D}}$.

Let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, the Galois conjugate $\mathcal{D}^\sigma$ is given by the Belyi pair (C^σ, β^σ), where

$$C^\sigma : y^2 = x(x - (1 - \sigma(\zeta_3)))(x - \sigma(\sqrt[3]{q})),$$

and β^σ has the same expression as β because all of its coefficients are rational. The orbit of the pair $(\zeta_3, \sqrt[3]{q})$ by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is $\{\zeta_3^i, \zeta_3^j \sqrt[3]{q}\}_{1\leq i\leq 2, 0\leq j\leq 2}$. Elliptic curves given by equations of the form $y^2 = (x-a)(x-b)(x-c)$ are isomorphic if and only if the cross-ratios of the tuples (a, b, c, ∞) coincide. We verify that the cross-ratios are all distinct, so the orbit of $\mathcal{D}$ is given by the six dessins $\mathcal{D}^\sigma$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{q})/\mathbb{Q})$. As a consequence $\mathcal{M}(\mathcal{D}) = \mathbb{Q}(\zeta_3, \sqrt[3]{q})$. To prove that the regular closures $\widetilde{\mathcal{D}^\sigma}$ constituting the orbit of $\widetilde{\mathcal{D}}$ are also non isomorphic, we must first draw the dessins $\mathcal{D}^\sigma$ to compute their cartographic groups.

Let us first draw the dessin $\mathcal{D}_0$ corresponding to the Belyi pair $(\mathbb{P}^1, \beta_1 \circ \beta_0)$ (see Figure 3). The dessin $\mathcal{D}_0$ is defined over $\mathbb{Q}$, so the dessins $\mathcal{D}^\sigma$ in the orbit are then obtained by lifting $\mathcal{D}_0$ to the curves C^σ. To simplify the graphical representations of the dessins, we will use the notation in Figure 2 for consectutive edges incident to a vertex.

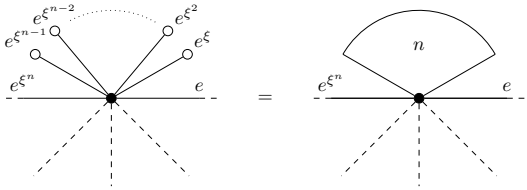


Figure 2: Notation for consecutive edges.

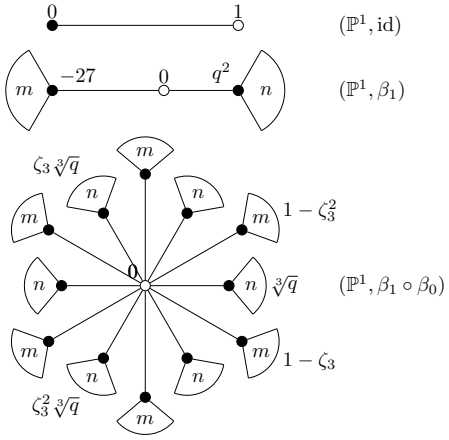
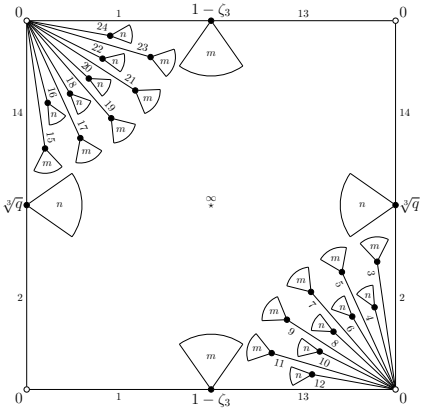
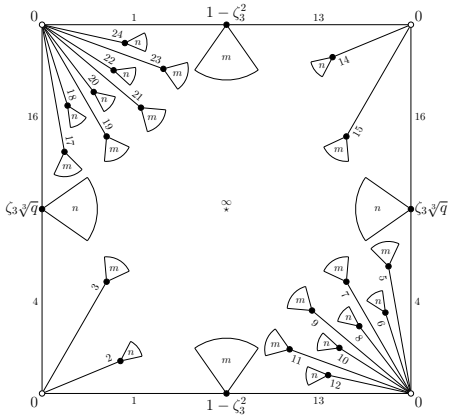


Figure 3: Construction of $\mathcal{D}_0$.

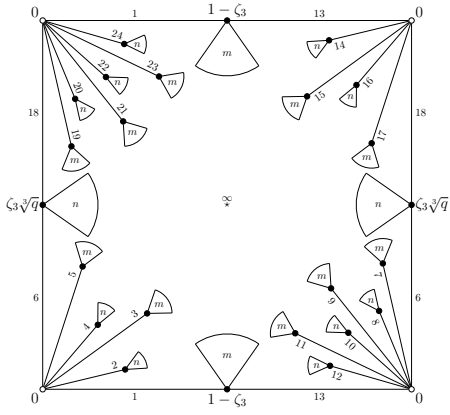
The dessins $\mathcal{D}_1, \ldots, \mathcal{D}_6$ conjugate to $\mathcal{D}$ are embedded on a torus, so in the representations in Figure 4 we will identify the outermost edges on opposite sides.



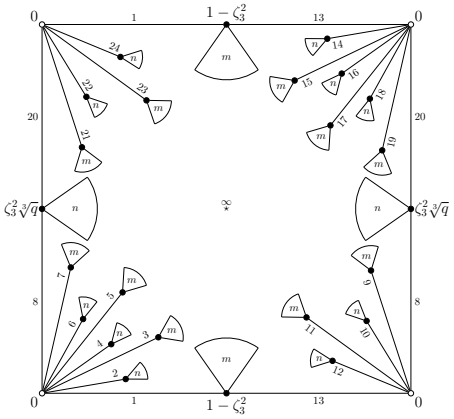
(a) $\mathcal{D}_1 \coloneqq \mathcal{D}$



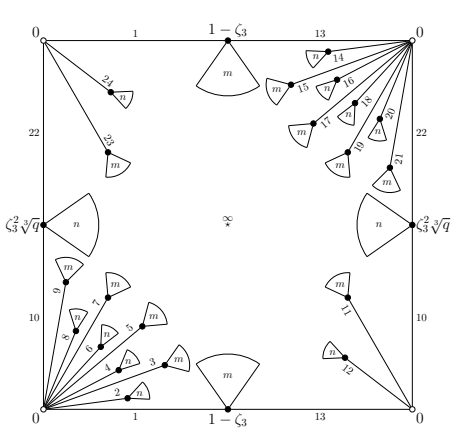
(b) $\mathcal{D}_2 \coloneqq \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \zeta_3\sqrt[3]{q})$



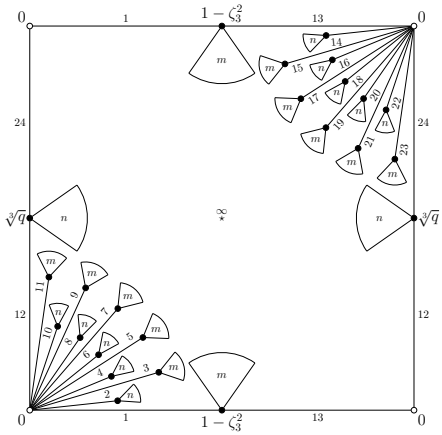
(c) $\mathcal{D}_3 \coloneqq \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3, \zeta_3\sqrt[3]{q})$



(d) $\mathcal{D}_4 \coloneqq \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \zeta_3^2\sqrt[3]{q})$



(e) $\mathcal{D}_5 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3, \zeta_3^2\sqrt[3]{q})$



(f) $\mathcal{D}_6 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \sqrt[3]{q})$

Figure 4: Dessins $\mathcal{D}_1, \ldots, \mathcal{D}_6$ in the Galois orbit of $\mathcal{D}$.

We will now establish that $\widetilde{\mathcal{D}_1}$ is not isomorphic to $\widetilde{\mathcal{D}_2}, \ldots, \widetilde{\mathcal{D}_6}$. To that end it suffices to show that there is no isomorphism between the cartographic groups fixing the canonical generators. We shall therefore exhibit an element $\omega \in F_2 = \langle \xi, \eta \rangle$ such that $M_k(\omega)$ commutes with $M_k(\eta^2)$ only when $k = 1$, where M_k is the monodromy map of $\mathcal{D}_k$.

We have defined m and n to be positive coprime integers such that $\frac{27}{27+q^2} = \frac{m}{m+n}$, so we cannot have $m = n = 1$. We will treat the case where $m \neq 1$ does not divide n, the other case being treated similarly. Let

$$\omega := \xi^n \eta^{-1} \xi^{m-n} \eta \xi^n.$$

We shall show that $M_k(\omega)$ commutes with $M_k(\eta^2)$ only when $k = 1$.

Let $E_k := \{1, 2, \ldots, 24\}$ be the set of edges of $\mathcal{D}_k$ incident to 0. The action of η fixes the set E_k on which it induces the cyclic permutation $(1, 2, \ldots, 24)$, and every white vertex except 0 has degree one so the action of η is trivial on the complement of E_k.

We can write $E_k = E_k^{\text{odd}} \sqcup E_k^{\text{even}}$ as the disjoint union of the sets of respectively odd and even numbered edges incident to 0, such that η sends one to the other. The black vertices of E_k^{odd} are of degree m except for the two black vertices of the edges 1 and 13 that are of degree $2m$. Therefore if m does not divide some integer l then ξ^l sends every edge of E_k^{odd} to the complement of E_k, and otherwise the action of ξ^m on E_k^{odd} corresponds to the sole transposition $(1, 13)$. Similarly if n does not divide l then ξ^l sends every edge of E_k^{even} to the complement of E_k, and the action of ξ^n on E_k^{even} is the transposition $(2k, 2k + 12)$.

In particular, by hypothesis n is not a multiple of m, so $m - n$ is not a multiple of m either, hence both ξ^n and ξ^{m-n} send the edges of E_k^{odd} to the complement of E_k. However η acts trivially on the latter, so $\xi^n \eta^{-1} \xi^{m-n}$ and $\xi^{m-n} \eta \xi^n$ both fix the set E_k^{odd} on which they induce the same action as ξ^m, i.e. the transposition $(1, 13)$. Therefore the action of $\omega = \xi^n \eta^{-1} \xi^{m-n} \eta \xi^n$ is the same as that of $\xi^m \eta \xi^n$ on E_k^{odd} and the same as that of $\xi^n \eta^{-1} \xi^m$ on E_k^{even}. See Figure 5.

The action of ω fixes the set E_k on which it induces the permutation

$$M_k(\omega)|_{E_k} = (1, 13)(2k, 2k + 12) \cdot (1, 2)(3, 4) \cdots (23, 24) \cdot (1, 13)(2k, 2k + 12)$$

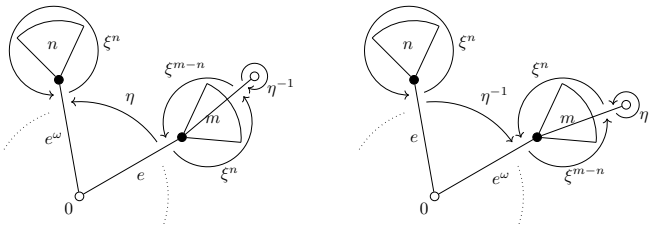


Figure 5: Action of ω on $E_k^{\text{odd}} \setminus \{1, 2k-1\}$ and on $E_k^{\text{even}} \setminus \{2, 2k\}$.

Therefore for $k = 1$,

$$\begin{aligned} M_1(\omega)|_{E_1} &= (1,13)(2,14) \cdot (1,2)(3,4)\cdots(23,24) \cdot (1,13)(2,14) \\ &= (1,2)(3,4)\cdots(23,24) \end{aligned}$$

so ω and η^2 commute on E_1. Moreover η acts trivially on the complement of E_1 so $M_1(\omega)|_{\mathcal{D}_1 \setminus E_1}$ and $M_1(\eta^2)|_{\mathcal{D}_1 \setminus E_1}$ automatically commute. Finally, we obtain that $M_1(\omega)$ and $M_1(\eta^2)$ commute.

For $k = 2$, we observe that $4^{\omega\eta^2} = 15^{\eta^2} = 17$ but $4^{\eta^2\omega} = 6^\omega = 5$. Similarly, for $3 \leq k \leq 6$, we observe that $1^{\omega\eta^2} = 14^{\eta^2} = 16$ but $1^{\eta^2\omega} = 3^\omega = 4$. We have thus shown that $M_k(\omega)$ and $M_k(\eta^2)$ commute only for $k = 1$.

This concludes the proof that $\widetilde{\mathcal{D}}$ is a regular dessin with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$.

3.2 Regular dessins with moduli fields of the form $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$

Let p be an odd prime, and $q \in \mathbb{Q}_{>0}$ a positive rational number that is not a pth power. In this example we will need an additional parameter $\gamma \in \mathbb{Q} \setminus \{0\}$. Let

$$C\colon y^2 = x(x - (1 - \zeta_p))(x - \gamma\sqrt[p]{q}).$$

We construct the Belyi function $\beta\colon C \to \mathbb{P}^1$ as the composition $\beta = \beta_2 \circ \beta_1 \circ \beta_0 \circ \pi$ of the following maps.

1. $\pi\colon C \to \mathbb{P}^1$ is the projection on the coordinate x, which ramifies over $\{0, 1 - \zeta_p, \gamma\sqrt[p]{q}, \infty\}$.
2. $\beta_0 := X^{2p} \in \mathbb{Q}[X]$, and $\mathrm{Crit}(\beta_0) = \{0, \infty\}$ so $\beta_0 \circ \pi$ ramifies over $\{0, (1 - \zeta_p)^{2p}, \gamma^{2p}q^2, \infty\}$.
3. $\beta_1 \in \mathbb{Q}[X]$ is chosen independently of γ such that $\mathrm{Crit}(\beta_1) \cup \{\beta_1((1 - \zeta_p)^{2p})\} = \{0, 1, \infty\}$, $\beta_1((1-\zeta_p)^{2p}) = 0 < \beta_1(0) < 1$ and $\beta_1'(0) > 0$. The existence of β_1 verifying those conditions is assured by Proposition 3.2 below. Under those assumptions $\beta_1 \circ \beta_0 \circ \pi$ ramifies over $\{0, 1, \beta_1(0), \beta_1(\gamma^{2p}q^2), \infty\}$.
4. $\gamma \in \mathbb{Q}_{>0}$ is then chosen small enough so that $\beta_1' > 0$ on $[0, \gamma^{2p}q^2]$. This guarantees us that we have $0 < \beta_1(0) < \beta_1(\gamma^{2p}q^2) < 1$.
5. $\beta_2 := B_{r,s} \circ B_{m,n}$, where (m, n) and (r, s) are pairs of coprime positive integers such that $\beta_1(\gamma^{2p}q^2) = \frac{m}{m+n}$ and $B_{m,n}(\beta_1(0)) = \frac{r}{r+s}$. Finally, $\beta = \beta_2 \circ \beta_1 \circ \beta_0 \circ \pi$ ramifies over $\{0, 1, \infty\}$.

The pair (C, β) is thus a Belyi pair, and we call $\mathcal{D}$ the corresponding dessin. With the same arguments as before, the moduli field of $\mathcal{D}$ is $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$, which is a nonabelian Galois extension of $\mathbb{Q}$ with Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p, \sqrt[p]{q})/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$$

generated by $\sigma\colon \zeta_p^i \sqrt[p]{q} \mapsto \zeta_p^{i+1} \sqrt[p]{q}$ and $\tau\colon \zeta_p^i \sqrt[p]{q} \mapsto \zeta_p^{gi} \sqrt[p]{q}$ where g generates $(\mathbb{Z}/p\mathbb{Z})^\times$. We shall show that there exists $\gamma \in \mathbb{Q} \setminus \{0\}$ such that the regular closure of the dessin $\mathcal{D}$ thus obtained also has moduli field $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$.

Remark 3.1. In the previous subsection we treated the case $p = 3$. In that specific case we gave a simpler expression for β, mainly due to the fact that $\beta_0 \circ \pi$ already had all of its critical values in $\mathbb{Q} \cup \{\infty\}$. However in the general case we must use the intermediate map β_1 as well as the parameter γ to conclude the proof.

Let us first prove the existence of β_1.

Proposition 3.2. *Let $E \subset \bar{\mathbb{Q}} \cap \mathbb{R} \setminus \{0\}$ be a finite set. Then there exists $P \in \mathbb{Q}[X]$ such that $P(E) \subseteq \{0\}$, $\mathrm{Crit}(P) \subseteq \{0, 1\}$, $0 < P(0) < 1$ and $P'(0) > 0$.*

Remark 3.3. In the context of this proposition we only deal with polynomials so for $P \in \mathbb{Q}[X]$ we define $\mathrm{Crit}(P) \coloneqq \{P(z) |\ z \in \mathbb{C}, P'(z) = 0\}$, which does not include the point at infinity to simplify notations.

Proof. To show this we will proceed similarly as in the proof of the *only if* part of Belyi's theorem, by applying additional transformations to ensure that $0 < P(0) < 1$. Let us first prove that we can reduce to the case where E is a subset of rational numbers.

Lemma 3.4. *Let $E \subset \bar{\mathbb{Q}} \cap \mathbb{R} \setminus \{0\}$ be a finite set fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then there exists $P \in \mathbb{Q}[X]$ such that $P(0) = 0$ and $\mathrm{Crit}(P) \cup P(E) \subset \mathbb{Q} \setminus \{0\}$.*

Proof. Let $\{a_1, \dots, a_m\} = E \cap \mathbb{Q}$ and $\{b_1, \dots, b_n\} = E \setminus \mathbb{Q}$. We construct P by induction on the number n of non rational elements of E.

For $\alpha \in \mathbb{Q}$, define $F_\alpha, G_\alpha \in \mathbb{Q}[X]$ by

$$F_\alpha \coloneqq \prod_{j=1}^{n} (X - (b_j - \alpha)^2) \quad \text{and} \quad G_\alpha \coloneqq F_\alpha((X-\alpha)^2) = \prod_{j=1}^{n} (X - b_j)(X + b_j - 2\alpha).$$

Let us first assume that there exists $\alpha \in \mathbb{Q}$ such that $G_\alpha(0) \notin \mathrm{Crit}(G_\alpha) \cup G_\alpha(E)$. Define $P_1(X) \coloneqq G_\alpha(X) - G_\alpha(0) \in \mathbb{Q}[X]$, then $P_1(0) = 0 \notin E' \coloneqq \mathrm{Crit}(P_1) \cup P_1(E) \subset \bar{\mathbb{Q}} \cap \mathbb{R} \setminus \{0\}$. Note that E' is stable under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and $|E' \setminus \mathbb{Q}| = |\mathrm{Crit}(F_\alpha) \cup F_\alpha(0) \setminus \mathbb{Q}| = |\mathrm{Crit}(F_\alpha) \setminus \mathbb{Q}| < \deg F_\alpha = n$. By induction, there exists $P_2 \in \mathbb{Q}[X]$ such that $P_2(0) = 0$ and $\mathrm{Crit}(P_2) \cup P_2(E') \subset \mathbb{Q} \setminus \{0\}$. Now $P \coloneqq P_2 \circ P_1$ has the desired properties, since $P(0) = 0$ and $\mathrm{Crit}(P) \cup P(E) = \mathrm{Crit}(P_2) \cup P_2(\mathrm{Crit}(P_1)) \cup P_2(P_1(E)) = \mathrm{Crit}(P_2) \cup P_2(E') \subset \mathbb{Q} \setminus \{0\}$.

Let us now prove that there exists $\alpha \in \mathbb{Q}$ such that $G_\alpha(0) \notin \mathrm{Crit}(G_\alpha) \cup G_\alpha(E)$. Let us first treat the case where $0 < b_1 < b_2, \dots, b_n$. When α approaches $\frac{1}{2}$, $G_\alpha(0) = \prod_{j=1}^{n} -b_j(b_j - 2\alpha)$ approaches 0 but the critical values of G_α do not. Indeed, $\mathrm{Crit}(G_\alpha) = \mathrm{Crit}\, F_\alpha \cup F_\alpha(\mathrm{Crit}((X-\alpha)^2)) = \mathrm{Crit}(F_\alpha) \cup \{F_\alpha(0)\}$; $F_\alpha(0)$ approaches $F_{\frac{b_1}{2}}(0) \neq 0$, and since $F_{\frac{b_1}{2}}$ does not have multiple roots, the critical values of F_α approach the critical values

of $F_{\frac{b_1}{2}}$ which are all non zero. Therefore for $\alpha \neq \frac{b_1}{2}$ in the neighborhood of $\frac{b_1}{2}$ we have $G_\alpha(0) \notin \mathrm{Crit}(G_\alpha)$. Moreover $G_\alpha(0), G_\alpha(a_1), \dots, G_\alpha(a_m)$ are all distinct polynomials in the indeterminate α, so they coincide at only finitely many points. In particular for $\alpha \neq \frac{b_1}{2}$ in the neighborhood of $\frac{b_1}{2}$ we have $G_\alpha(0) \notin \{G_\alpha(a_1), \dots, G_\alpha(a_m)\}$. Since $\alpha \in \mathbb{Q}$ we also have $G_\alpha(0) \neq 0 = G_\alpha(b_1) = \cdots = G_\alpha(b_n)$ hence $G_\alpha(0) \notin G_\alpha(E)$, proving the existence of α as desired.

Let us now treat the general case where $b_1, \dots, b_n$ are not assumed to be positive by reducing it to the previous case. For $\alpha' \in \mathbb{Q}$, define $H_{\alpha'} \in \mathbb{Q}[X]$ by

$$H_{\alpha'} \coloneqq (X - \alpha')^2 - \alpha'^2 \in \mathbb{Q}[X].$$

Note that $\mathrm{Crit}(H_{\alpha'}) = \{-\alpha'\}$. For $\alpha' > 0$ sufficiently small we have $-\alpha'^2 < H_{\alpha'}(0) = 0 < H_{\alpha'}(a_1), \dots, H_{\alpha'}(a_m), H_{\alpha'}(b_1), \dots, H_{\alpha'}(b_n)$. Let $E'' \coloneqq \mathrm{Crit}(H_{\alpha'}) \cup H_{\alpha'}(E)$. The set E'' is a finite subset of $\bar{\mathbb{Q}} \cap \mathbb{R} \setminus \{0\}$ fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and E'' has at most n non rational elements, which are all positive. By the above, there exists $P_3 \in \mathbb{Q}[X]$ such that $\mathrm{Crit}(P_3) \cup P_3(E'') \subset \mathbb{Q} \setminus \{0\}$ and $P_3(0) = 0$. Then $P \coloneqq P_3 \circ H_{\alpha'}$ has the desired properties, since $P(0) = 0$ and $\mathrm{Crit}(P) \cup P(E) = \mathrm{Crit}(P_3) \cup P_3(\mathrm{Crit}(H_{\alpha'})) \cup P_3(H_{\alpha'}(E)) = \mathrm{Crit}(P_3) \cup P_3(E'') \subset \mathbb{Q} \setminus \{0\}$. □

Let us denote by P_1 the polynomial obtained using this lemma, which verifies $P_1(0) = 0$ and $E' \coloneqq \mathrm{Crit}(P_1) \cup P_1(E) \subset \mathbb{Q} \setminus \{0\}$. We can further assume that $P_1'(0) > 0$ by taking $(-P_1)$ if necessary. We now send the points E' to $\{0, 1\}$.

Lemma 3.5. *Let $E \subset \mathbb{Q} \setminus \{0\}$ a finite set. Then there exists $P \in \mathbb{Q}[X]$ such that $P(E) \subseteq \{0\}$, $\mathrm{Crit}(P) \subseteq \{0, 1\}$, $0 < P(0) < 1$ and $P'(0) > 0$.*

Proof. For $\alpha \in \mathbb{Q}$, let $F_\alpha \coloneqq (X - \alpha)^2 \in \mathbb{Q}[X]$, and note that $\mathrm{Crit}(F_\alpha) = \{0\}$. There exists $\alpha < 0$ sufficiently small such that $0 < F_\alpha(0) < F_\alpha(a)$ for all $a \in E$. We take

$$F \coloneqq \frac{F_\alpha}{\max_{a \in E} F_\alpha(a)}.$$

Let $\{a_1, \dots, a_l\} = F(E)$ such that $0 < F(0) < a_1 < \cdots < a_l = 1$. We also add a rational point $a_0 \in \mathbb{Q}$ such that $F(0) < a_0 < a_1$.

Let m and n be the coprime positive integers such that $a_{l-1} = \frac{m}{m+n}$. We recall that $B_{m,n}$ verifies $\mathrm{Crit}(B_{m,n}) = \{0, 1\}$, $B_{m,n}(0) = B_{m,n}(1) = 0$, $B_{m,n}(\frac{m}{m+n}) = 1$, and $B_{m,n}$ is strictly increasing between 0 and $\frac{m}{m+n}$. Let $P_1 \coloneqq B_{m,n}$, then $\mathrm{Crit}(P_1) = \{0, 1\}$ and $0 < P_1 \circ F(0) < P_1(a_0) < \cdots < P_1(a_{l-1}) = 1$. There is one point fewer than before, so we can iteratively construct $P_2, \dots, P_l$ in the same way, so that $P \coloneqq P_l \circ \cdots \circ P_1$ verifies $\mathrm{Crit}(P) \subseteq \{0, 1\}$, $P(a_1) = \cdots = P(a_l) = 0 < P(F(0)) < 1 = P(a_0)$ and $P'(F(0)) > 0$. Therefore $P \circ F$ has the desired properties. □

Let us denote by P_2 the polynomial obtained using this lemma with the finite set E' obtained previously. Then the polynomial $P \coloneqq P_2 \circ P_1$ verifies $P(E) \subseteq \{0\}$, $\mathrm{Crit}(P) \subseteq \{0, 1\}$, $0 < P(0) < 1$ and $P'(0) > 0$, thus concluding the proof of Proposition 3.2. □

We can now use Proposition 3.2 with the finite set

$$E \coloneqq \{(1 - \zeta_p^k)^{2p}\}_{1 \leq k \leq \frac{p-1}{2}}$$

to obtain the map β_1 as desired. For $1 \leq k \leq \frac{p-1}{2}$ we have $(1-\zeta_p^k)^{2p} = (|1-\zeta_p^k|\zeta_{2p}^{2k-1})^{2p} = |1-\zeta_p^k|^{2p} \in \mathbb{R}$ so $E \subset \bar{\mathbb{Q}} \cap \mathbb{R}$, and the set E is the Galois orbit of $(1-\zeta_p)^{2p}$ so it is fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, hence E verifies the conditions of Proposition 3.2.

Let us denote by $\mathcal{D}(\beta_1)$ the dessin corresponding to the Belyi pair $(\mathbb{P}^1, \beta_1)$. The Belyi pair $(\mathbb{P}^1, \beta_1)$ is fixed by the action of the complex conjugation, so the embedding of $\mathcal{D}(\beta_1)$ on $\mathbb{P}^1$ admits a symmetry along the real line. Moreover the Belyi function β_1 is a polynomial, so $\mathcal{D}(\beta_1) \cap \mathbb{R}$ is a (graph theoretic) path. Let $v_l < \cdots < v_1$ be the negative vertices on the path, and let e_k denote the edge (v_{k-1}, v_k). By hypothesis $\beta_1'(0) > 0$ so v_1 is a black vertex, and for $k < l$, the vertex v_k is of even degree $2d_k$. We then have $e_k^{\xi^{d_k}} = e_{k+1}$ and $e_{k+1}^{\xi^{d_k}} = e_k$ if k is odd, or $e_k^{\eta^{d_k}} = e_{k+1}$ and $e_{k+1}^{\eta^{d_k}} = e_k$ if k is even. See Figure 6.

As remarked earlier, the Galois orbit of $(1-\zeta_p)^{2p}$ is $\{(1-\zeta_p^k)^{2p}\}_{1\leq k\leq \frac{p-1}{2}} \subset \mathbb{R}_-$, and $(1-\zeta_p^{\frac{p-1}{2}})^{2p} < \cdots < (1-\zeta_p)^{2p} < 0$. By construction $\beta_1((1-\zeta_p)^{2p}) = 0$, so $(1-\zeta_p)^{2p}$ and all its Galois conjugates are black vertices of $\mathcal{D}(\beta_1)$ lying on the path $(v_1, \cdots, v_l)$. Let $t > 0$ be the index such that $v_t = (1-\zeta_p)^{2p}$, and v_t is a black vertex so t is odd. Then

$$\mu_0 \coloneqq \xi^{d_1}\eta^{d_2}\cdots\eta^{d_{t-1}}\xi^{2d_t}\eta^{d_{t-1}}\cdots\eta^{d_2}\xi^{d_1}$$

fixes the edge e_1 (Figure 6).

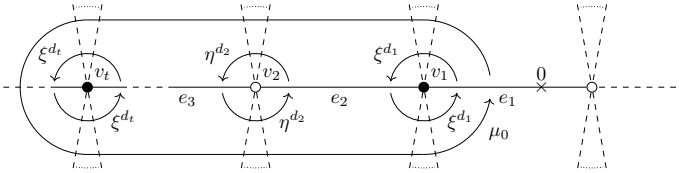


Figure 6: Dessin $\mathcal{D}(\beta_1)$ corresponding to $(\mathbb{P}^1, \beta_1)$.

Let $\gamma > 0$ small enough so that $\beta_1' > 0$ on $[0, \gamma^{2p}q^2]$. Let us next draw the dessin $\mathcal{D}(\beta_2)$ corresponding to the Belyi pair $(\mathbb{P}^1, \beta_2 = B_{r,s} \circ B_{m,n})$. See Figure 7.

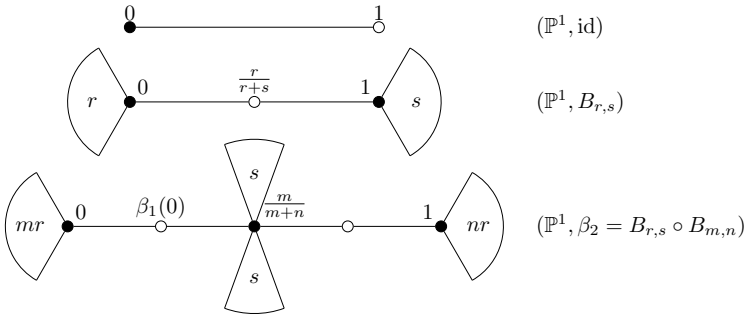


Figure 7: Dessin $\mathcal{D}(\beta_2)$ corresponding to $(\mathbb{P}^1, \beta_2)$.

By lifting the dessin $\mathcal{D}(\beta_2)$ along β_1 we obtain the dessin $\mathcal{D}(\beta_2 \circ \beta_1)$ corresponding to the Belyi pair $(\mathbb{P}^1, \beta_2 \circ \beta_1)$. This amounts to replacing each edge of $\mathcal{D}(\beta_1)$ by a copy of $\mathcal{D}(\beta_2)$. Note that the degrees of the black and white vertices are thus multiplied by mr and

nr, respectively. Analogously to μ_0 we define

$$\begin{aligned}\mu \coloneqq &(\xi^{mrd_1}\eta\xi^s\eta)(\xi^{nrd_2}\eta\xi^s\eta)\cdots(\xi^{mrd_{t-2}}\eta\xi^s\eta)(\xi^{nrd_{t-1}}\eta\xi^s\eta)\\ &\cdot(\xi^{2mrd_t}\eta\xi^s\eta)(\xi^{nrd_{t-1}}\eta\xi^s\eta)(\xi^{mrd_{t-2}}\eta\xi^s\eta)\cdots(\xi^{nrd_2}\eta\xi^s\eta)\xi^{mrd_1}\end{aligned}$$

and we verify again that μ fixes the edge $(0, v_1)$. Note also that ξ^{2s} fixes the edge $(0, \gamma\sqrt[p]{q})$. See Figure 8.

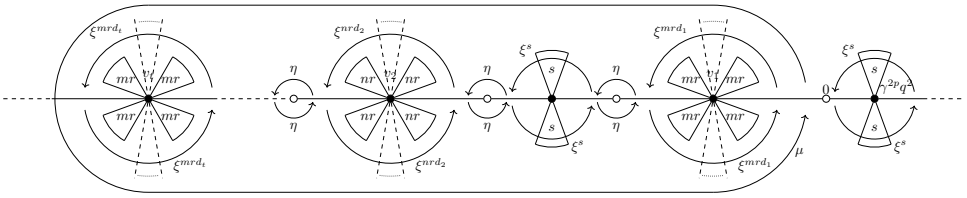


Figure 8: Dessin $\mathcal{D}(\beta_2 \circ \beta_1)$ corresponding to $(\mathbb{P}^1, \beta_2 \circ \beta_1)$.

Let $\mathcal{D}_0$ be the dessin corresponding to the Belyi pair $(\mathbb{P}^1, \beta_2 \circ \beta_1 \circ \beta_0)$. To simplify the representations of the dessins we only show the vertices 0, $\zeta_{2p}^k(1-\zeta_p)$, $1-\zeta_p^k$, and $\zeta_{2p}^k\gamma\sqrt[p]{q}$. We decorate the vertices $\zeta_{2p}^k(1-\zeta_p)$ (which map to $(1-\zeta_p)^{2p} \in \mathbb{R}_-$ by β_0) and $\zeta_{2p}^k\gamma\sqrt[p]{q}$ (which map to $\gamma^{2p}q^2 \in \mathbb{R}_+$ by β_0) respectively with the symbols $\ominus$ and $\oplus$ to distinguish them. See Figure 9.

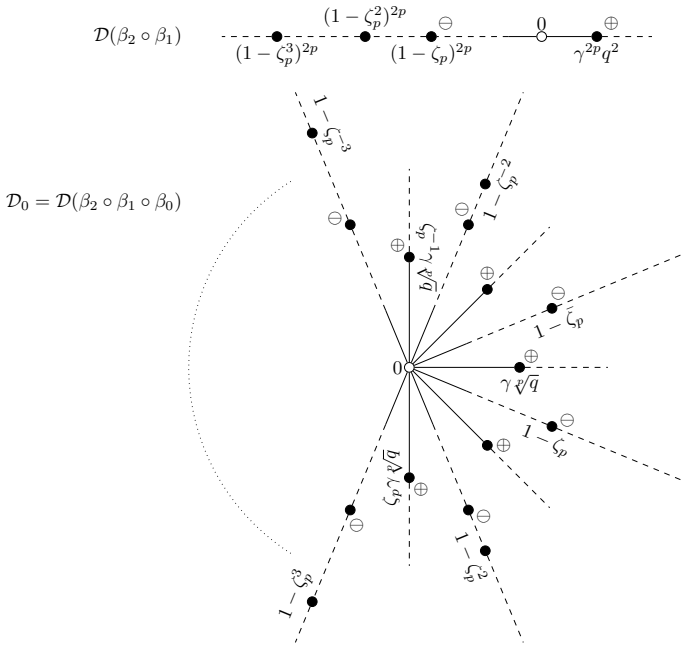
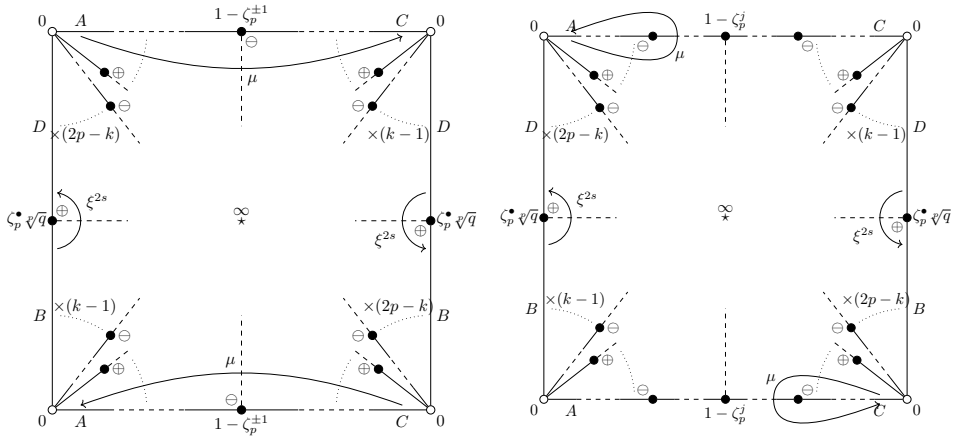


Figure 9: Dessin $\mathcal{D}_0$ corresponding to $(\mathbb{P}^1, \beta_2 \circ \beta_1 \circ \beta_0)$.

We may now draw the Galois conjugates $\mathcal{D}^\sigma$ for $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by lifting the dessin $\mathcal{D}_0$ along the projection π, by treating separately the cases $\sigma(\zeta_p) \in \{\zeta_p, \bar{\zeta_p}\}$ and $\sigma(\zeta_p) \in$

$\{\zeta_p^2, \dots, \zeta_p^{p-2}\}$. We call the dessins respectively $\mathcal{D}_k$ and $\mathcal{D}_k^j$, see Figure 10. We identify the outermost edges on opposite sides in the representations.



(a) $\mathcal{D}_k := \mathcal{D}^\sigma$ with $\sigma(\zeta_p) = \zeta_p^{\pm 1}$.

(b) $\mathcal{D}_k^j := \mathcal{D}^\sigma$ with $\sigma(\zeta_p) = \zeta_p^j$ where $j \in \{2, \dots, p-2\}$.

Figure 10: Dessins (a) $\mathcal{D}_k$ and (b) $\mathcal{D}_k^j$ in the Galois orbit of $\mathcal{D}$.

For all k, we have in fact $\mathcal{D}_{2k-1} = \mathcal{D}^\sigma$ where $\sigma\colon (\zeta_p, \sqrt[p]{q}) \mapsto (\zeta_p, \zeta_p^{k-1}\sqrt[p]{q})$, and $\mathcal{D}_{2k} = \mathcal{D}^\sigma$ where $\sigma\colon (\zeta_p, \sqrt[p]{q}) \mapsto (\bar{\zeta_p}, \zeta_p^k \sqrt[p]{q})$. We have similar expressions for the dessins $\mathcal{D}_k^j$.

Let k be fixed, and let us consider the dessin $\mathcal{D}_k$. Let A denote one of the two edges incident to 0 and on the path to the ramification point $1 - \zeta_p^{\pm 1}$. We also call $B := A^{\eta^{2k-1}}, C := A^{4p}, D := C^{\eta^{2k-1}}$ (See Figure 10a). Let E denote the set of edges incident to 0. The action of η induces the cyclic permutation of the edges of $E = \{A^{\eta^i}\}_{0 \le i < 8p}$. Furthermore by construction every white vertex aside from 0 has degree 1 or 2, so η^2 fixes every edge in the complement of E. We can write $E = E^\ominus \sqcup E^\oplus$ as the disjoint union of $E^\ominus := \{A^{2i}\}_{0 \le i < 4p}$ and $E^\oplus := \{B^{2i}\}_{0 \le i < 4p}$, such that η sends one to the other. The action of μ on $E^\ominus$ is the transposition (A, C), and similarly the action of ξ^{2s} on $E^\oplus$ is the transposition (B, D).

We do the same for the dessins of the form $\mathcal{D}_k^j$, with the only difference that this time the action of μ on $E^\ominus$ is trivial, including on the edges A and C (see Figure 10b).

We are almost in the same configuration as in the first example. We define analogously

$$\omega := \mu\eta\mu^{-1}\xi^{2s}\eta^{-1}\mu,$$

and we shall prove that for some choices of γ, the actions of ω and of η^2 commute only for $\mathcal{D}_1$. To reproduce the proof in the first example we need only show that for some choice of γ the actions of $\mu\eta\mu^{-1}\xi^{2s}$ and $\mu^{-1}\xi^{2s}\eta^{-1}\mu$ on the set $E^\oplus$ is the same as that of ξ^{2s}.

Note that for any edge $e \in E^\oplus$, the edge e^{ξ^i} is fixed by η if i is not a multiple of s. To that end we shall show that for some choice of γ the action of μ on $E^\oplus$ is the same as that of ξ^δ, where δ is the number of occurences of ξ in the word μ, and then that δ is not a multiple of s.

We define the words $\rho_1, \rho_1', \rho_2, \rho_2', \ldots, \rho_{2t-2}, \rho_{2t-2}' \in F_2$ to be the increasing subsequence of the prefixes ending in η of the word μ defined above, such that $\rho_1 \coloneqq \xi^{mrd_1}\eta$, $\rho_1' \coloneqq \rho_1\xi^s\eta$, $\rho_2 \coloneqq \rho_1'\xi^{nrd_2}\eta$, $\rho_2' \coloneqq \rho_2\xi^s\eta$, etc., and $\mu = \rho_{2t-2}'\xi^{mrd_1}$. We shall show by induction that for some choice of γ the action of ρ_i (resp. ρ_i') is the same as the action of ξ^{δ_i} (resp. $\xi^{\delta_i'}$), where δ_i (resp. δ_i') is the number of occurences of ξ in the word ρ_i (resp. ρ_i'). By induction it suffices to show that δ_i, δ_i' are not multiples of s. Modulo s we have $\delta_i \equiv \delta_i'$ equal to the non empty partial sum of

$$mrd_1+nrd_2+\cdots+mrd_{t-2}+nrd_{t-1}+2mrd_t+nrd_{t-1}+mrd_{t-2}+\cdots+nrd_2+mrd_1$$

consisting of the first i terms.

To proceed we shall use the following result, but let us first introduce some notations. Let $P = \sum_{i=0}^{d} c_i X^i \in \mathbb{Z}[X]$ and $c \in \mathbb{Z}_{>0}$ such that $\beta_1 = \frac{P}{c}$. Note that P and c do not depend on the choice of γ, and $0 < \beta_1(0) = \frac{P(0)}{c} < 1$ so $0 < c_0, c - c_0$. We define

$$\alpha \coloneqq v_2(\gamma^{2p}q^2), \quad \nu \coloneqq v_2(c_0) + v_2(c - c_0),$$

where v_2 denotes the 2-valuation.

Lemma 3.6. *If $\alpha > \nu$, then there exists $e \in \mathbb{Z}$ such that $em \equiv c_0 \mod 2^\alpha$ and $en \equiv c - c_0 \mod 2^\alpha$, and $v_2(s) \geq \alpha - \nu$.*

Proof. Let $a, b \in \mathbb{Z}$ coprime such that $\gamma^{2p}q^2 = \frac{a}{b}2^\alpha$.

Firstly,

$$\frac{m}{m+n} = \beta_1(\frac{a}{b}2^\alpha) = \frac{P(\frac{a}{b}2^\alpha)}{c} = \frac{\sum_{i=0}^{d} c_i a^i 2^{\alpha i} b^{d-i}}{b^d c},$$

so there exists $f \in \mathbb{Z}$ such that $fm = \sum_{i=0}^{d} c_i a^i 2^{\alpha i} b^{d-i}$ and $f(m+n) = b^d c$, so

$$em \equiv c_0 \mod 2^\alpha, \quad en \equiv c - c_0 \mod 2^\alpha$$

for $e \in \mathbb{Z}$ such that $eb^d \equiv f \mod 2^\alpha$.

Secondly,

$$\begin{aligned}\frac{r}{r+s} = B_{m,n}(\beta_1(0)) &= \frac{\beta_1(0)^m(1-\beta_1(0))^n}{\beta_1(\frac{a}{b}2^\alpha)^m(1-\beta_1(\frac{a}{b}2^\alpha))^n} \\ &= \frac{b^{d(m+n)}c_0^m(c-c_0)^n}{(b^dP(\frac{a}{b}2^\alpha))^m(b^dc - b^dP(\frac{a}{b}2^\alpha))^n},\end{aligned}$$

so there exists $g \in \mathbb{Z}$ such that $gr = b^{d(m+n)}c_0^m(c-c_0)^n$ and $g(r+s) = (b^dP(\frac{a}{b}2^\alpha))^m(b^dc - b^dP(\frac{a}{b}2^\alpha))^n$. In the expansion of $(b^dP(\frac{a}{b}2^\alpha))^m$, aside from the constant term $b^{dm}c_0^m$, every other term is a multiple of an integer of the form $c_0^i 2^{\alpha j}$ with $i \leq m-1$ and $j \geq m-i$. By hypothesis $\alpha > \nu \geq v_2(c_0)$, so those other terms are all multiples of $2^{\alpha+(m-1)v_2(c_0)}$, hence there exists $A \in \mathbb{Z}$ such that $(b^dP(\frac{a}{b}2^\alpha))^m = b^{dm}c_0^m + A2^{\alpha+(m-1)v_2(c_0)}$. Similarly there exists $B \in \mathbb{Z}$ such that $(b^dc - b^dP(\frac{a}{b}2^\alpha))^n = b^{dn}(c-c_0)^n + B2^{\alpha+(n-1)v_2(c-c_0)}$. Then $g(r+s) = b^{d(m+n)}c_0^m(c-c_0)^n + C2^{\alpha+(m-1)v_2(c_0)+(n-1)v_2(c-c_0)}$ for some $C \in \mathbb{Z}$, so $gr = b^{d(m+n)}c_0^m(c-c_0)^n$ and $gs = C2^{\alpha+(m-1)v_2(c_0)+(n-1)v_2(c-c_0)}$. The integers r and s are coprime, so after dividing gr and gs by their greatest common dividor we obtain that

$$v_2(s) \geq \alpha - \nu > 0. \qquad \square$$

Using this lemma, we know that if $\alpha > \nu$, then there exists $e \in \mathbb{Z}$ such that $em \equiv c_0 \mod 2^\alpha$ and $en \equiv c - c_0 \mod 2^\alpha$, $v_2(s) \geq \alpha - \nu$ where ν does not depend on γ, and r is coprime to s so is not a multiple of 2. Therefore there exists $e' \in \mathbb{Z}$ such that $e'mr \equiv c_0 \mod 2^\alpha$ and $e'nr \equiv c - c_0 \mod 2^\alpha$. Moreover $2^{\alpha-\nu}$ is a common divisor of 2^α and s, so by the above modulo $2^{\alpha-\nu}$ we have $e'\delta_i \equiv e'\delta_i'$ equal to the non empty partial sum $\widetilde{\delta}_i$ consisting of the first i terms of the sum

$$\begin{aligned} &c_0d_1 + (c-c_0)d_2 + \cdots + c_0d_{t-2} + (c-c_0)d_{t-1} + 2c_0d_t \\ &\quad + (c-c_0)d_{t-1} + c_0d_{t-2} + \cdots + (c-c_0)d_2 + c_0d_1. \end{aligned}$$

Similarly $e'\delta$ is equal modulo $2^{\alpha-\nu}$ to the whole sum

$$\widetilde{\delta} \coloneqq 2(c_0d_1 + (c-c_0)d_2 + \cdots + c_0d_{t-2} + (c-c_0)d_{t-1} + c_0d_t).$$

By construction $c_0, c-c_0, d_i$ are positive and do not depend on the choice of γ, so $0 < c_0d_1 \leq \widetilde{\delta}_i \leq \widetilde{\delta}$, thus for any choice of γ such that $\alpha > \nu$ and $\widetilde{\delta} < 2^{\alpha-\nu}$ (for instance $\gamma = \frac{2^u}{2^v+1}$ with $1 \ll u \ll v$), we obtain $\widetilde{\delta}_i, \widetilde{\delta} \not\equiv 0 \mod 2^{\alpha-\nu}$, and in consequence δ_i, δ_i' and δ are not multiples of s. Therefore we can now conclude by induction that the actions of ρ_i and ρ_i' are the same as that of ξ^{δ_i} and $\xi^{\delta_i'}$, respectively. Indeed, δ_1 is not a multiple of s so $\rho_1 = \xi^{\delta_1}\eta$ and ξ^{δ_1} have the same action on $E^\oplus$. If ρ_i has the same action as ξ^{δ_i} on $E^\oplus$, then $\rho_i' = \rho_i\xi^s\eta$ has the same action as $\xi^{\delta_i}\xi^s\eta = \xi^{\delta_i'}\eta$ on $E^\oplus$, and also the same action as $\xi^{\delta_i'}$ because δ_i' is not a multiple of s. Similarly, if ρ_i' has the same action as $\xi^{\delta_i'}$ on $E^\oplus$, then ρ_{i+1} has the same action as $\xi^{\delta_{i+1}}\eta$ on $E^\oplus$, and also the same action as $\xi^{\delta_{i+1}}$ because δ_{i+1} is not a multiple of s.

We have thus proved that μ has the same action as ξ^δ on $E^\oplus$, and by symmetry μ^{-1} has the same action as $\xi^{-\delta}$ on $E^\oplus$. And δ and $2s-\delta$ are not multiples of s, so $\mu\eta\mu^{-1}\xi^{2s}$ and $\mu^{-1}\xi^{2s}\eta^{-1}\mu$ have the same action as ξ^{2s} on $E^\oplus$, as announced. We shall now observe the action of $\omega = \mu\eta\mu^{-1}\xi^{2s}\eta^{-1}\mu$ on E. Let M_k and M_k^j denote the monodromy maps of the dessins $\mathcal{D}_k$ and $\mathcal{D}_k^j$.

For the dessins $\mathcal{D}_k$ for $1 \leq k \leq 2p$, the action of μ on $E^\ominus$ is the transposition (A, C), and the action of ξ^{2s} on $E^\oplus$ is the transposition (B, D), therefore the action of ω fixes the set E on which it induces the permutation

$$M_k(\omega)|_E = (A,C)(B,D) \cdot \prod_{i=0}^{4p-1} (A^{\eta^{2i}}, A^{\eta^{2i+1}}) \cdot (A,C)(B,D).$$

Hence for $k = 1$,

$$\begin{aligned} M_1(\omega)|_E &= (A, A^{\eta^{4p}})(A^\eta, A^{\eta^{4p+1}}) \cdot \prod_{i=0}^{4p-1} (A^{\eta^{2i}}, A^{\eta^{2i+1}}) \cdot (A, A^{\eta^{4p}})(A^\eta, A^{\eta^{4p+1}}) \\ &= \prod_{i=0}^{4p-1} (A^{\eta^{2i}}, A^{\eta^{2i+1}}) \end{aligned}$$

so ω and η^2 commute on E. Moreover η^2 acts trivially on the complement of E, so finally $M_1(\omega)$ and $M_1(\eta^2)$ commute.

For $k = 2$, we observe that $B^{\omega\eta^2} = D^{\eta^{-1}\eta^2} = D^\eta$ but $B^{\eta^2\omega} = B^{\eta^2\eta^{-1}} = B^\eta$. Similarly, for $3 \le k \le 2p$, we observe that $A^{\omega\eta^2} = C^{\eta\eta^2} = C^{\eta^3}$ but $A^{\eta^2\omega} = A^{\eta^2\eta} = A^{\eta^3}$. Therefore $M_k(\omega)$ and $M_k(\eta^2)$ do not commute for $2 \le k \le 2p$.

For the dessins $\mathcal{D}_k^j$ for $1 \le k \le 2p$ and $2 \le j \le \frac{p-1}{2}$, ξ^{2s} on $E^\oplus$ is the transposition (B, D), and μ acts trivially on $E^\ominus$, therefore the action of ω fixes the set E on which it induces the permutation

$$M_k^j(\omega)|_E = (B, D) \cdot \prod_{i=0}^{4p-1} (A^{\eta^{2i}}, A^{\eta^{2i+1}}) \cdot (B, D).$$

Hence we observe that $B^{\omega\eta^2} = D^{\eta^{-1}\eta^2} = D^\eta$ but $B^{\eta^2\omega} = B^{\eta^2\eta^{-1}} = B^\eta$, so $M_k^j(\omega)$ and $M_k^j(\eta^2)$ do not commute.

We have thus shown that the actions of ω and η^2 commute only for $\mathcal{D}_1$, this concludes the proof that $\widetilde{\mathcal{D}}$ is a regular dessin with moduli field $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$.

3.3 Regular dessin with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$

Finally, let us exhibit a regular dessin with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$ of smaller degree by choosing a Belyi map that is a rational function instead of a polynomial as was done in the previous subsections. Let

$$C\colon y^2 = x(x - (1 - \zeta_3))(x - \sqrt[3]{3}),$$
$$\beta\colon C \to \mathbb{P}^1, (x, y) \mapsto \frac{(x + 3^3)^3}{3^5(x - 3^2)^2}.$$

The function β is given by the composition of the following maps $\beta = \beta_1 \circ \beta_0 \circ \pi$.

1. $\pi\colon C \to \mathbb{P}^1$ is the projection on the coordinate x, which ramifies over $\{0, 1 - \zeta_3, \sqrt[3]{3}, \infty\}$.
2. $\beta_0 := X^6 \in \mathbb{Q}[X]$, $\mathrm{Crit}(\beta_0) = \{0\}$ so $\beta_0 \circ \pi$ ramifies over $\{0, (1 - \zeta_3)^6 = -3^3, 3^2, \infty\}$.
3. $\beta_1 := \frac{(X+3^3)^3}{3^5(X-3^2)^2}$, $\mathrm{Crit}(\beta_1) = \{0, 1\}$ so $\beta = \beta_1 \circ \beta_0 \circ \pi$ ramifies over $\{0, 1, \infty\}$.

The pair (C, β) is thus a Belyi pair, and we call $\mathcal{D}$ the dessin corresponding to (C, β). Similarly as in 3.1, $\mathcal{D}$ has moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$. We will proceed analogously to show that the regular closure $\widetilde{\mathcal{D}}$ has the same field of moduli. Let us first draw the dessin $\mathcal{D}_0$ corresponding to the Belyi pair $(\mathbb{P}^1, \beta_1 \circ \beta_0)$ (see Figure 11), and lift it to the conjugate curves C^σ to obtain the conjugate dessins $\mathcal{D}^\sigma$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{3})/\mathbb{Q})$ (see Figure 12).

As usual we identify the outermost edges on opposite sides.

We can now compute the cartographic groups of the dessins. Let M_k denote the monodromy map of $\mathcal{D}_k$. Then

$$M_k(\xi) = \begin{matrix}(1,13,14,7,25,26)(2,15,16)(3,17,18)(4,19,20)(5,21,22)\\(6,23,24)(8,27,28)(9,29,30)(10,31,32)(11,33,34)(12,35,36)\end{matrix}$$

for all $1 \le k \le 6$, and

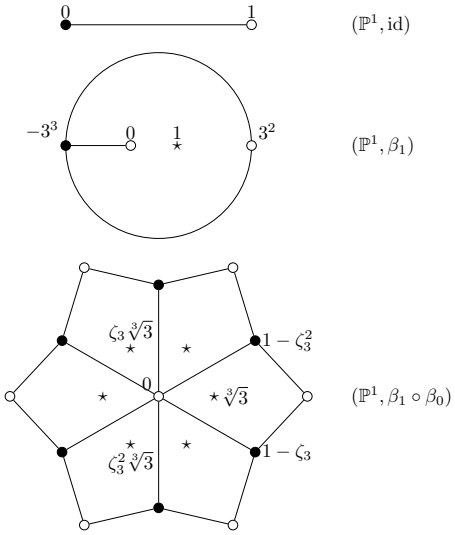
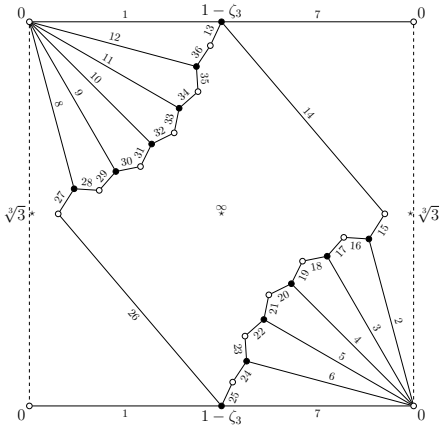
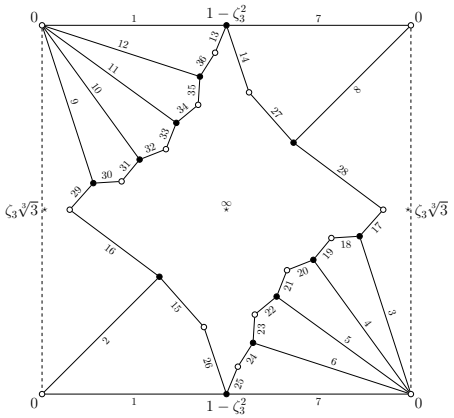


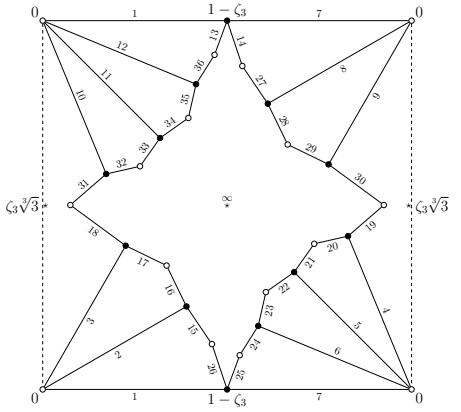
Figure 11: Construction of $\mathcal{D}_0$.



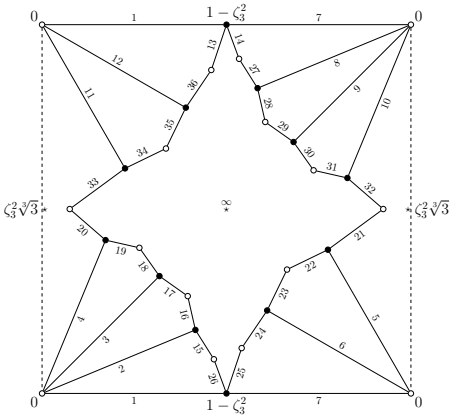
(a) $\mathcal{D}_1 \coloneqq \mathcal{D}$



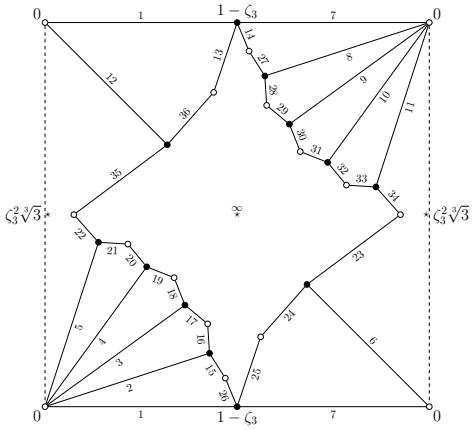
(b) $\mathcal{D}_2 \coloneqq \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \zeta_3 \sqrt[3]{q})$



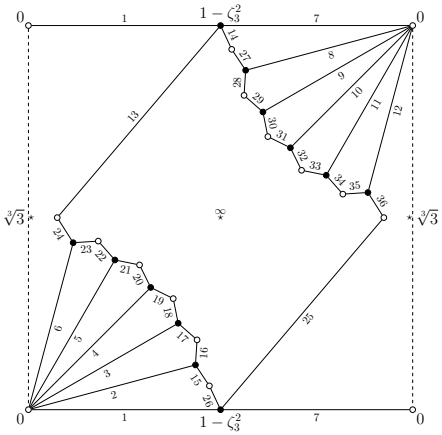
(c) $\mathcal{D}_3 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3, \zeta_3\sqrt[3]{q})$



(d) $\mathcal{D}_4 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \zeta_3^2\sqrt[3]{q})$



(e) $\mathcal{D}_5 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3, \zeta_3^2\sqrt[3]{q})$



(f) $\mathcal{D}_6 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \sqrt[3]{q})$

Figure 12: Dessins $\mathcal{D}_1, \ldots, \mathcal{D}_6$ in the Galois orbit of $\mathcal{D}$.

- $M_1(\eta) =$ (1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,15)(16,17)(18,19)(20,21)(22,23)(24,25)(26,27)(28,29)(30,31)(32,33)(34,35) ,
- $M_2(\eta) =$ (1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,27)(15,26)(16,29)(17,28)(18,19)(20,21)(22,23)(24,25)(30,31)(32,33)(34,35) ,
- $M_3(\eta) =$ (1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,27)(15,26)(16,17)(18,31)(19,30)(20,21)(22,23)(24,25)(28,29)(32,33)(34,35) ,
- $M_4(\eta) =$ (1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,27)(15,26)(16,17)(18,19)(20,33)(21,32)(22,23)(24,25)(28,29)(30,31)(34,35) ,
- $M_5(\eta) =$ (1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,27)(15,26)(16,17)(18,19)(20,21)(22,35)(23,34)(24,25)(28,29)(30,31)(32,33) ,
- $M_6(\eta) =$ (1,2,3,4,5,6,7,8,9,10,11,12)(13,24)(14,27)(15,26)(16,17)(18,19)(20,21)(22,23)(25,36)(28,29)(30,31)(32,33)(34,35) .

Using the computer algebra system SageMath [10], we determined that

$$|\langle M_1(\xi), M_1(\eta)\rangle| = 42467328 = 2^{19} \cdot 3^4.$$

Moreover, $M_1(\xi)$, $M_1(\eta)$ and $M_1(\xi\eta)$ respectively have orders 6, 12 and 12, so the Euler characteristic of the underlying surface of $\widetilde{\mathcal{D}_1}$ is

$$\begin{aligned}\chi &= |\langle M_1(\xi), M_1(\eta)\rangle| \cdot \left(\frac{1}{\operatorname{ord} M_1(\xi)} + \frac{1}{\operatorname{ord} M_1(\eta)} + \frac{1}{\operatorname{ord} M_1(\xi\eta)} - 1\right) \\ &= -28311552 = -2^{20} \cdot 3^3,\end{aligned}$$

and its genus is $g = 1 - \frac{\chi}{2} = 14155777$.

We will now show that $\widetilde{\mathcal{D}_1}$ is not isomorphic to $\widetilde{\mathcal{D}_2}, \ldots, \widetilde{\mathcal{D}_6}$. We claim that $\omega := [\xi^{-1}\eta^2\xi, \xi\eta] \in \ker M_1 \setminus \bigcup_{2\leq k\leq 6} \ker M_k$, thus concluding the proof. Indeed, we obtain:

- $M_1(\omega) = \mathrm{id}$;
- $M_2(\omega) = (13,25)(15,27)(21,33)(23,35)$;
- $M_3(\omega) = (17,29)(21,33)$;
- $M_4(\omega) = (13,25)(15,27)(19,31)(21,33)$;
- $M_5(\omega) = (13,25)(17,29)$;
- $M_6(\omega) = (13,25)(19,31)(21,33)(23,35)$.

We have thus constructed a regular dessin $\widetilde{\mathcal{D}}$ of degree $2^{19} \cdot 3^4$ and genus 14155777 with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$.

ORCID iDs

Fumiharu Kato https://orcid.org/0009-0002-4800-0029

References

[1] M. D. E. Conder, G. A. Jones, M. Streit and J. Wolfart, Galois actions on regular dessins of small genera, *Rev. Mat. Iberoam.* **29** (2013), 163–181, doi:10.4171/rmi/717, https://doi.org/10.4171/rmi/717.

[2] E. Girondo and G. González-Diez, *Introduction to compact Riemann surfaces and dessins d'enfants*, volume 79 of *London Mathematical Society Student Texts*, Cambridge University Press, Cambridge, 2012.

[3] G. González-Diez and A. Jaikin-Zapirain, The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces, *Proc. Lond. Math. Soc. (3)* **111** (2015), 775–796, doi:10.1112/plms/pdv041, https://doi.org/10.1112/plms/pdv041.

[4] A. Grothendieck, Esquisse d'un programme, in: *Geometric Galois actions, 1*, Cambridge Univ. Press, Cambridge, volume 242 of *London Math. Soc. Lecture Note Ser.*, pp. 5–48, 1997, with an English translation on pp. 243–283.

[5] P. Guillot, An elementary approach to dessins d'enfants and the Grothendieck-Teichmüller group, *Enseign. Math.* **60** (2014), 293–375, doi:10.4171/lem/60-3/4-5, https://doi.org/10.4171/lem/60-3/4-5.

[6] M. Herradón Cueto, An explicit quasiplatonic curve with non-abelian moduli field, *Rev. Mat. Complut.* **29** (2016), 725–739, doi:10.1007/s13163-016-0196-z, https://doi.org/10.1007/s13163-016-0196-z.

[7] R. A. Hidalgo and S. Quispe, Regular dessins d'enfants with field of moduli $\mathbb{Q}(\sqrt[p]{2})$, *Ars Math. Contemp.* **13** (2017), 323–330, doi:10.26493/1855-3974.1202.9c1, https://doi.org/10.26493/1855-3974.1202.9c1.

[8] G. A. Jones and J. Wolfart, *Dessins d'enfants on Riemann surfaces*, Springer Monographs in Mathematics, Springer, Cham, 2016, doi:10.1007/978-3-319-24711-3, https://doi.org/10.1007/978-3-319-24711-3.

[9] S. K. Lando and A. K. Zvonkin, *Graphs on surfaces and their applications*, volume 141 of *Encyclopaedia of Mathematical Sciences*, Springer-Verlag, Berlin, 2004, doi:10.1007/978-3-540-38361-1, with an appendix by Don B. Zagier, Low-Dimensional Topology, II, https://doi.org/10.1007/978-3-540-38361-1.

[10] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020-01-01, https://www.sagemath.org.