Regular dessins uniquely determined by a nilpotent automorphism group

Na-Er Wang∗1,2, Roman Nedela†3,4, and Kan Hu‡1,2

1School of Mathematics, Physics and Information Science, Zhejiang Ocean University, Zhoushan, Zhejiang 316022, People’s Republic of China
2Key Laboratory of Oceanographic Big Data Mining & Application of Zhejiang Province, Zhoushan, Zhejiang 316022, People’s Republic of China
3University of West Bohemia, NTIS FAV, Pilsen, Czech Republic
4Mathematical Institute, Slovak Academy of Sciences, Banská Bystrica, Slovak Republic

Abstract

It is well known that the automorphism group of a regular dessin is a two-generator finite group, and the isomorphism classes of regular dessins with automorphism groups isomorphic to a given finite group \( G \) are in one-to-one correspondence with the orbits of the action of \( \text{Aut}(G) \) on the ordered generating pairs of \( G \). If there is only one orbit, then up to isomorphism the regular dessin is uniquely determined by the group \( G \) and it is called uniquely regular. In the paper we investigate the classification of uniquely regular dessins with a nilpotent automorphism group. The problem is reduced to the classification of finite maximally automorphic \( p \)-groups \( G \), i.e., the order of the automorphism group of \( G \) attains Hall’s upper bound. Maximally automorphic \( p \)-groups of nilpotency class three are classified.

Keywords: group automorphism, Hall’s upper bound, regular dessin

MSC(2010) 20D15, 20B35, 58D19,
1 Introduction

A dessin is a 2-cell embedding of a connected 2-coloured bipartite graph into a compact Riemann surface. An automorphism of a dessin is a colour-preserving automorphism of the underlying graph, regarded as permutations of the edges, which extends to a conformal self-homeomorphism of the supporting surface. It is well known that the group of automorphisms of a dessin acts semi-regularly on the edges. In the case where this action is transitive, and hence regular, the dessin will be called regular as well.

Belyi’s theorem [1] establishes a correspondence between dessins and Riemann surfaces definable over the field of algebraic numbers, and thus, as observed by Grothendieck [5], develops a combinatorial approach to the absolute Galois group through its action on dessins. It is recently proved by González-Diez and Jaikin-Zapirain that this action remains faithful when restricted to regular dessins [4]. Therefore it is important to investigate regular dessins and the associated quasiplatonic Riemann surfaces, see [14, 16, 18, 19] and references therein for more details on this subject.

Our ambition is to investigate regular dessins with a maximal group of external symmetries. In order to explain our motivation we need to introduce a group-theoretical approach to regular dessins. It is well known that the automorphism group of a regular dessin is a two-generator finite group, and for a given two-generator finite group $G$, the isomorphism classes of regular dessins with automorphism group isomorphic to $G$ are in one-to-one correspondence with the orbits of the action of $\text{Aut}(G)$ on the generating pairs of $G$ [14]. In the case where $\text{Aut}(G)$ has just one orbit the corresponding dessin will be called uniquely regular.

The simplest example of a uniquely regular dessin is determined by the group $C_n \times C_n$, the direct product of two cyclic groups of order $n$. Note that the associated algebraic curve is the well known Fermat curve defined by the equation $x^n + y^n = z^n$, see [13] for details. It follows from the uniqueness that uniquely regular dessins are invariant under the action of the group of dessin operations, and hence possess the highest level of external symmetry. The uniqueness also implies that all uniquely regular dessins are invariant under the action of the absolute Galois group, and hence the associated algebraic curves can be defined over the field of rational numbers.

The classification problem of uniquely regular dessins translates to the language of group theory as follows:

**Problem 1:** Classify finite two-generator groups $G$ such that $\text{Aut}(G)$ is transitive on the set of ordered generating pairs of $G$.

Though every finite non-abelian simple group $G$ is two-generated [21], it
cannot determine a uniquely regular dessin, since the generating pair of G can be chosen as an involution and a non-involution, and G does not admit an automorphism transposing them. In this paper we restrict our investigation on Problem 1 to finite nilpotent groups. More precisely, we consider

**Problem 2A:** Classify finite two-generator nilpotent groups G such that Aut(G) is transitive on the set of ordered generating pairs of G.

Since every finite nilpotent group is a direct product of its Sylow subgroups, Problem 2A reduces to

**Problem 2B:** Classify finite two-generator p-groups G such that Aut(G) is transitive on the set of ordered generating pairs of G.

A solution to Problem 2B (and hence to Problem 2A) is surprisingly nice. Let G be a d-generator p-group of order $p^n$, P. Hall showed in [6] that

$$|\text{Aut}(G)| \leq p^{d(n-d)}(p^d - 1)(p^d - p) \cdots (p^d - p^{d-1}).$$

The group G will be called **maximally automorphic** if the equality holds. In Theorem 3 we prove that a two-generator p-group determines a uniquely regular dessin if and only if it is maximally automorphic. Although this gives a general answer to Problems 2A and 2B a complete description of maximally automorphic p-groups is not at hand.

Two-generator abelian maximally automorphic p-groups are exactly the homocyclic p-groups isomorphic to $C_{p^n} \times C_{p^n}$ for some integer $n \geq 1$. Two-generator maximally automorphic p-groups of nilpotency class two have been classified in [11, Theorem 5]. The main result of this paper is the following theorem classifying two-generator maximally automorphic p-groups of nilpotency class three:

**Theorem 1.** Let $G = \langle x, y \rangle$ be a maximally automorphic p-group of nilpotency class three, then G is isomorphic to one of the groups listed below:

(i) $p = 3$ and $1 \leq c < b = a$ or $1 \leq c \leq b \leq a - 1,$

$$G = \langle x, y | x^{3a} = y^{3b} = z^{3c} = u^{3c} = v^{3c} = [x, u] = [y, u] = [y, v] = 1, \quad z = [x, y], u = [z, x], v = [z, y] \rangle.$$ 

(ii) $p > 3$ and $1 \leq c \leq b \leq a,$

$$G = \langle x, y | x^{pa} = y^{p^b} = z^{p^c} = u^{p^c} = v^{p^c} = [x, u] = [y, u] = [y, v] = 1, \quad z = [x, y], u = [z, x], v = [z, y] \rangle.$$
(iii) $p = 2$ and $1 \leq c \leq b \leq a - 1$,

$$G = \langle x, y | x^{2^a} = y^{2^b} = z^{2^c} = u^{2^c} = v^{2^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, z = [x, y], u = [z, x], v = [z, y] \rangle.$$  

(iv) $p = 2$ and $1 \leq c \leq b \leq a - 1$,

$$G = \langle x, y | z^{2^a} = u^{2^c} = v^{2^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, x^{2^a} = u^{2^c-1}, y^{2^a} = v^{2^c-1}, z = [x, y], u = [z, x], v = [z, y] \rangle.$$  

(v) $p = 2$ and $1 \leq c \leq a - 2$,

$$G = \langle x, y | z^{2^{a-1}} = u^{2^c} = v^{2^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, x^{2^{a-1}} = z^{2^{2-2}}, y^{2^{a-1}} = z^{2^{2-2}}, z = [x, y], u = [z, x], v = [z, y] \rangle.$$  

(vi) $p = 2$ and $1 \leq c \leq a - 2$,

$$G = \langle x, y | z^{2^{a-1}} = u^{2^c} = v^{2^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, x^{2^{a-1}} = z^{2^{2-2}} u^{2^{c-1}}, y^{2^{a-1}} = z^{2^{2-2}} v^{2^{c-1}}, z = [x, y], u = [z, x], v = [z, y] \rangle.$$

Moreover, the above groups are pairwise non-isomorphic.

In proving the result we employ the theory of group extensions together with some results on metabelian groups.

## 2 Maximaly automorphic $p$-groups

Let $G$ be a $d$-generator finite $p$-group of order $p^n$, Hall [6] has shown that $|\text{Aut}(G)|$ divides $U(p; n, d)$ where

$$U(p; n, d) = p^{d(n-d)}(p^d - 1)(p^d - p) \cdots (p^d - p^{d-1}).$$

The group $G$ is called maximally automorphic if $|\text{Aut}(G)| = U(p; n, d)$. Berkovich and Janko posed the problem of studying maximally automorphic $p$-groups in [2, Research problems and themes I 35(a)]. Clearly finite homocyclic $p$-groups $C_d^p$ are examples of maximally automorphic $p$-groups.

**Example 1.** The quaternion group $Q_8$ is a non-abelian two-generator 2-group of order $2^3$. Since $|\text{Aut}(Q_8)| = 24 = U(2; 3, 2)$, $Q_8$ is maximally automorphic. It determines a unique regular dessin, which is the embedding of the doubled 4-cycle $C_4^{(2)}$, the cycle of length 4 with multiplicity 2, into the double torus of genus 2. This is depicted in Fig. [1] where the opposite sides of the outer octagon are identified to form the double torus.
Lemma 2. A $d$-generator finite $p$-group $G$ of order $p^n$ is maximally automorphic if and only if $\text{Aut}(G)$ is transitive (or equivalently, regular) on the generating $d$-tuples of $G$.

Proof. For brevity we denote a $d$-tuple $(x_1, \ldots, x_d)$ by $(x_i)$. Let $T$ be the set of generating $d$-tuples of $G$, that is,

$$T = \{(x_1, x_2, \ldots, x_d) \mid G = \langle x_1, x_2, \ldots, x_d \rangle\}.$$

By Burnside’s Basis Theorem $\overline{G} = G/\Phi(G)$ is elementary abelian of rank $d$ where $\Phi(G)$ is the Frattini subgroup of $G$. Regarding $\overline{G}$ as a linear space of dimension $d$ over the Galois field $\mathbb{F}_p$, a generating $d$-tuple of $\overline{G}$ is a base of the linear space. Thus the number of generating $d$-tuples of $\overline{G}$ is equal to $|GL(d, p)| = (p^d - 1)(p^d - p) \cdots (p^d - p^{d-1})$.

Moreover, each generating $d$-tuple $(\overline{x}_i)$ of $\overline{G}$ lifts to precisely $|\Phi(G)|^d = p^{d(n-d)}$ generating $d$-tuples $\{(x_i, g_i) \mid g_i \in \Phi(G)\}$, and each generating $d$-tuple of $G$ arises in this way. Hence $|T| = p^{d(n-d)}|GL(d, p)| = U(p; n, d)$. Since the action of $\text{Aut}(G)$ on $T$ is semiregular, $G$ is maximally automorphic if and only if $\text{Aut}(G)$ acts transitively (or equivalently, regularly) on $T$. \hfill \Box

The following result is an immediate consequence of Lemma 2.

Theorem 3. Let $G$ be a finite two-generator $p$-group, then $G$ determines a uniquely regular dessin if and only if it is maximally automorphic.

Proof. $G$ determines a unique regular dessin if and only if $\text{Aut}(G)$ acts transitively on the generating pairs of $G$, or equivalently, $G$ is maximally automorphic by Lemma 2. \hfill \Box

Figure 1: $C_{4}^{(2)}$ embedded into double torus
Lemma 4. Let $G$ be a $d$-generator finite maximally automorphic $p$-group. If $N \text{ char } G$ and $N \leq \Phi(G)$, then the following statements hold true:

(i) the quotient group $G/N$ is maximally automorphic,

(ii) for each $\sigma \in \text{Aut}(G)$, the mapping $\varphi: \sigma \mapsto \bar{\sigma}$ is a group epimorphism from $\text{Aut}(G)$ onto $\text{Aut}(G/N)$ where $\bar{\sigma}(gN) = \sigma(g)N$,

(iii) $\ker \varphi = C_{\text{Aut}(G)}(G/N)$ is a finite $p$-group of order $|N|^d$, where

$$C_{\text{Aut}(G)}(G/N) = \{ \sigma \in \text{Aut}(G) \mid g^{-1}\sigma(g) \in N \text{ for all } g \in G \},$$

(iv) $\text{Aut}(G)$ is a semidirect product of $C_{\text{Aut}(G)}(G/N)$ by a subgroup $Q \cong \text{Aut}(G/N)$,

(v) $\text{Aut}(G)$ is transitive on the maximal subgroups of $G$.

Proof. Assume $|G| = p^n$, then $|\Phi(G)| = p^{n-d}$. Since $N \leq \Phi(G)$ we may assume $|N| = p^m$ where $m \leq n - d$. By hypothesis $N \text{ char } G$, so each automorphism $\sigma \in \text{Aut}(G)$ of $G$ induces an automorphism $\bar{\sigma}$ of $G/N$ of the form $\bar{\sigma}: gN \mapsto \sigma(g)N$, and the mapping $\varphi: \text{Aut}(G) \to \text{Aut}(G/N)$, $\sigma \mapsto \bar{\sigma}$ is a group homomorphism.

Moreover, for any generating $d$-tuple $(x_i)$ of $G$, define a set of $d$-tuples as

$$\Delta = \{(x_1g_1, x_2g_2, \ldots, x_dg_d) \mid \text{ each } g_i \in N \}.$$ 

Since $N \leq \Phi(G)$, each $d$-tuple in $\Delta$ generates $G$, and the group $K := \ker \varphi$ acts semiregularly on $\Delta$. Thus $|K|$ divides $|\Delta| = |N|^d = p^{md}$, and hence

$$|\text{Aut}(G/N)| \geq |\text{Aut}(G)|/|K| \geq U(p; n, d)/|\Delta| = U(p; n - m, d).$$

By Hall’s theorem $|\text{Aut}(G/N)|$ divides $U(p; n - m, d)$. Thus $|\text{Aut}(G/N)| = U(p; n - m, d)$ and $G/N$ is maximally automorphic.

The above proof also implies that $|\text{Aut}(G/N)| = |\text{Aut}(G)|/|K|$ and $|K| = |\Delta|$, so the mapping $\varphi$ is indeed an epimorphism and $K$ is indeed regular on $\Delta$. It follows that the set $T$ consisting of generating $d$-tuples of $G$ splits into $q := |\text{Aut}(G/N)|$ disjoint blocks of equal size $|K|$. It is easily seen that $K$ fixes every block, and $\text{Aut}(G)$ has a subgroup $Q \cong \text{Aut}(G/N)$ transitive on the blocks, so $K \cap Q = 1$ and $\text{Aut}(G) = K \rtimes Q$.

Finally, since $G/\Phi(G)$ is elementary abelian, $\text{Aut}(G/\Phi(G))$ is transitive on the maximal subgroups of $G/\Phi(G)$. Note that for each maximal subgroup $M$ of $G$ we have $\Phi(G) \leq M$, thus by (ii) $\text{Aut}(G)$ is transitive on the maximal subgroups of $G$, as required. \hfill \Box
Remark 1. A finite group $G$ is called an **MI-group** if all maximal subgroups of $G$ are isomorphic. MI-groups were investigated by Hermann [7, 8, 9] and Mann [22]. By Lemma 4(v) every maximally automorphic $p$-group is an MI-group.

Example 2. Let $p > 2$ be a prime, let $G$ be the non-abelian $p$-group of order $p^3$ and of exponent $p$ defined by the presentation

$$G = \langle x, y \mid x^p = y^p = z^p = [z, x] = [z, y] = 1, z := [x, y] \rangle.$$ 

Since $G' \leq Z(G)$ and $\exp(G) = p$, every generating pair $(x', y')$ of $G$ fulfills the above defining relations, so the mapping $x \mapsto x'$, $y \mapsto y'$ extends to an automorphism of $G$. By Lemma 2 the group $G$ is maximally automorphic. The associated uniquely regular dessin is of type $(p, p, p)$, embedded into an oriented surface of genus $p^2(p - 3)/2 + 1$ (The reader is referred to [11] for the formulae of calculating type and genus of a regular dessin). For $p = 3$ the dessin is given by a regular embedding of the Pappus graph into the torus, as depicted in Fig. 2, where the opposite sides of the outer hexagon are identified to form the torus.

Example 3. Let $F_d$ denote the free group of rank $d$, $H = \langle g^{p^e} \mid g \in F_d \rangle$, then $H \text{ char } F_d$. Define $B(d, p^e) = F_d/H$. The group $B(d, p^e)$, called the **Burnside group** of exponent $p^e$ with $d$ generators, is not necessarily a finite group. Let $K$ be the intersection of all finite-index subgroups of $B(d, p^e)$, then $K \triangleleft B(d, p^e)$ and the quotient $R(d, p^e) = B(d, p^e)/K$ is finite by the positive
answer to the restricted Burnside problem. By the construction every finite
d-generator $p$-group of exponent no more than $p^e$ is a homomorphic image
of $R(d, p^e)$. In particular, any mapping between two generating $d$-tuples of
$R(d, p^e)$ extends to an automorphism of $R(d, p^e)$. Therefore by Lemma 2
$R(d, p^e)$ is maximally automorphic. For example the restricted Burnside
group $R(2, 4) = B(2, 4)$ has been investigated by Janko in [2, §60]. This is
a group of order $2^{12}$ and class 5. It determines a uniquely regular dessin of
type $(4, 4, 4)$, embedded into a surface of genus $2^9 + 1$.

Finite two-generator maximally automorphic $p$-groups of class two have
been classified in [11, Theorem 5]. The result reads as follows:

**Theorem 5.** [11] Let $G$ be a finite two-generator $p$-group of nilpotency class
two. If $G$ is maximally automorphic then $G$ is isomorphic to one of the
groups listed below:

(i) $p$ is odd and $1 \leq b \leq a$:

$$G = \langle x, y \mid x^{p^a} = y^{p^a} = z^{p^b} = [z, x] = [z, y] = 1, z = [x, y] \rangle.$$  

(ii) $p = 2$ and $1 \leq b \leq a - 1$:

$$G = \langle x, y \mid x^{2^a} = y^{2^a} = z^{2^b} = [z, x] = [z, y] = 1, z = [x, y] \rangle.$$  

(iii) $p = 2$ and $a \geq 2$:

$$G = \langle x, y \mid z^{2^{a-1}} = [z, x] = [z, y] = 1, x^{2^{a-1}} = y^{2^{a-1}} = z^{2^{a-2}}, z = [x, y] \rangle.$$  

Moreover, the above groups are pairwise non-isomorphic.

## 3 Classification

In this section we present a classification of two-generator maximally auto-
morphic $p$-groups of class three. We shall use the standard notation from
group theory. In particular, recall that $G^{(1)} = G' = [G, G]$ is the derived
subgroup of $G$, and for $i \geq 1$ the $(i + 1)$-th derived subgroup of $G$ is
defined by induction as $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. Moreover, we denote $G_1 = G$, and
$G_{i+1} = [G_i, G]$ for $i \geq 1$.

In what follows familiarity with the basic commutator formulae is assu-
med, see [12, Chapter III]. In particular the following well known proper-
ties on metabelian groups will be frequently referred to. For the proof see
[3, 10] or [24, Proposition 2.1.5]
Lemma 6. [3, 10, 24] Let $G$ be a metabelian group, $x, y, z \in G$. Then the following hold true:

(i) if $z \in G'$ then $[z, x]^{-1} = [z^{-1}, x]$;
(ii) if $y \in G'$ then $[xy, z] = [x, z][y, z]$ and $[z, xy] = [z, x][z, y]$;
(iii) for any $x, y, z \in G$, $[x, y^{-1}, z]^y = [y, x, z]$;
(iv) for any $x, y, z \in G$, $[x, y][y, z][z, x, y] = 1$;
(v) if $z \in G'$ then $[z, x, y] = [z, y, x]$.

By induction it is easy to extend the formula of Lemma 6(v) as follows. Let $x_1, \ldots, x_n$ be arbitrary elements of a metabelian group $G$, then for any $z \in G'$ and for any permutation $\alpha$ of $\{1, 2, \ldots, n\}$, we have $[z, x_1, x_2, \ldots, x_n] = [z, x_{\alpha(1)}, x_{\alpha(2)}, \ldots, x_{\alpha(n)}]$. Therefore for brevity we may denote

$$[i, j] = [x, y, x, \ldots, x, y, \ldots, y],$$

where $i$ and $j$ are positive integers.

To proceed we need more sophisticated formulae on metabelian groups. For the proof see [3, 10] or [24, Chapter 2].

Lemma 7. [3, 10, 24] Let $G = \langle x, y \rangle$ be a metabelian group. Then for any integer $s \geq 2$,

$$G_s = \langle [ix, (s - i)y], G_{s+1} \mid i = 1, 2, \ldots, s - 1 \rangle.$$

Lemma 8. [3, 10, 24] Let $G$ be a metabelian group, $x, y \in G$. Then for any positive integers $m$ and $n$

$$[x^m, y^n] = \prod_{i=1}^{m} \prod_{j=1}^{n} [i, j]^{m_i(n_j)}.$$

Lemma 9. [3, 10, 24] Let $G$ be a metabelian group, $x, y \in G$. Then for any integer $m \geq 2$

$$ (xy^{-1})^m = x^m \left( \prod_{i+j \leq m} [i, j]^{m_{i,j}} \right) y^{-m}. $$

The following theorem on cyclic extensions of groups is well known.
Theorem 10. [13, Theorem 3.36] Let $N$ be a group and $m$ a positive integer, and let $a \in N$ and $\sigma \in \text{Aut}(N)$. If

$$a^\sigma = a \quad \text{and} \quad x^{\sigma^m} = x^a$$

for all $x \in N$, then there exists a group $G$, unique up to isomorphism, and having $N$ as a normal subgroup with the following properties:

(i) $G/N = \langle gN \rangle$ is cyclic of order $m$,

(ii) $g^m = a$,

(iii) $x^\sigma = x^a$.

Now we turn to the classification of two-generator maximally automorphic $p$-groups of class three. The following technical result will be useful.

Lemma 11. Let $G = \langle x, y \rangle$ be a maximally automorphic $p$-group of class three, denote $z = [x, y]$, $u = [z, x]$ and $v = [z, y]$. Then $G$ is metabelian and each of the assignments $\tau : x \mapsto y, y \mapsto x$, $\pi : x \mapsto x^{-1}, y \mapsto y$ and $\eta : x \mapsto x, y \mapsto xy$ extends to an automorphism of $G$, with the images of $z, u$ and $v$ under the corresponding automorphisms summarized in Table 1

| Automorphisms $\sigma$ | $z^\sigma$ | $u^\sigma$ | $v^\sigma$ |
|------------------------|-----------|-----------|-----------|
| $\tau : x \mapsto y, y \mapsto x$ | $z^{-1}$ | $v^{-1}$ | $u^{-1}$ |
| $\pi : x \mapsto x^{-1}, y \mapsto y$ | $z^{-1}u$ | $u$ | $v^{-1}$ |
| $\eta : x \mapsto x, y \mapsto xy$ | $zu$ | $u$ | $uv$ |

Proof. By hypothesis $G$ is a $p$-group of class three, so $G_4 = 1$. Since $G^{(2)} \leq G_4$ [12, Theorem 2.12, Chapter III], we have $G^{(2)} = 1$, that is, $G$ is metabelian. Note that $G = \langle x, y \rangle = \langle x^{-1}, y \rangle = \langle x, yx \rangle$. Since $G$ is maximally automorphic, by Lemma 2, each of the above assignments $\tau, \pi$ and $\eta$ extends to an automorphism of $G$.

To calculate the images of $z, u$ and $v$ we employ the basic commutator formulae from Lemma 6. Then

$$z^\tau = [x, y]^\tau = [x^\tau, y^\tau] = [y, x] = z^{-1},$$

$$u^\tau = [z, x]^\tau = [z^\tau, x^\tau] = [z^{-1}, y] = [z, y]^{-1} = v^{-1},$$

$$v^\tau = [z, y]^\tau = [z^\tau, y^\tau] = [z^{-1}, x] = [z, x]^{-1} = u^{-1}.$$
Similarly, for \( \pi \) we have
\[
\begin{align*}
  z^{\pi} &= [x^{-1}, y] = [x^{-1}, y]^x = [y, x]^y = [y, x][y, x, x^{-1}] \\
  &= [x, y][y, x, x^{-1}] = [x, y][x, x, y] = z^{-1}u,
\end{align*}
\]
\[
\begin{align*}
  u^{\pi} &= [z^{\pi}, x^{\pi}] = [z^{-1}u, x^{-1}] = [z^{-1}, x^{-1}] = [z, x] = u,
\end{align*}
\]
\[
\begin{align*}
  v^{\pi} &= [z^{\pi}, y^{\pi}] = [z^{-1}u, y] = [z^{-1}, y] = v^{-1}.
\end{align*}
\]

Finally, for \( \eta \) we have
\[
\begin{align*}
  z^{\eta} &= [x, y]^{\eta} = [x, yx] = [x, y]^{x} = z^{x} = zu,
\end{align*}
\]
\[
\begin{align*}
  u^{\eta} &= [zu, x] = [z, x]^{u}[u, x] = [z, x] = u,
\end{align*}
\]
\[
\begin{align*}
  v^{\eta} &= [zu, yx] = [z, yx] = [z, x][z, y]^{x} = uv^{x} = uv.
\end{align*}
\]

We remark that in the proof we have used the fact that \( G_{4} = 1 \) and \( G_{3} = \langle u, v \rangle \leq Z(G) \).

**Remark 2.** With the notation as in Lemma 11, the formulae in Lemma 8 and 9 are reduced to the following form:
\[
\begin{align*}
  [x^{m}, y^{n}] &= [x, y]^{mn}[x, y, x]^{n} = [x, y]^{m} = z^{m}u^{n}y^{m},
\end{align*}
\]
\[
\begin{align*}
  (xy^{-1})^{m} &= x^{m}[x, y]^{\left(\frac{m}{2}\right)}[x, y, x]^{n} = [x, y]^{m}y^{-m}.
\end{align*}
\]

Replacing \( y^{-1} \) by \( y \) in the second identity we obtain
\[
\begin{align*}
  (xy)^{m} &= x^{m}[x, y^{-1}]^{\left(\frac{m}{2}\right)}[x, y, x]^{n} = [x, y]^{m}y^{m}.
\end{align*}
\]
Since \( [x, y^{-1}] = z^{-1}v, [x, y^{-1}, x] = u^{-1} \) and \( [x, y^{-1}, y^{-1}] = v \) we get
\[
\begin{align*}
  (xy)^{m} &= x^{m}z^{-\left(\frac{m}{2}\right)}u^{-\left(\frac{m}{2}\right)}v^{\left(\frac{m}{2}\right)}y^{m}, \quad (3)
\end{align*}
\]
Applying \( \tau \) to Eq. (3) we obtain
\[
\begin{align*}
  (yx)^{m} &= y^{m}z^{\left(\frac{m}{2}\right)}u^{-\left(\frac{m}{2}\right)}v^{\left(\frac{m}{2}\right)}x^{m}. \quad (4)
\end{align*}
\]

**Remark 3.** The automorphisms \( \tau, \pi \) and \( \eta \) correspond to three types of dessin operations studied in [17]: the first swaps the black and the white vertices, the second is the Petrie duality operation, and the last interchanges the black vertices and faces. It was shown that the three operations generate the entire group \( \Omega \) of dessin operations which is isomorphic to \( GL(2, \mathbb{Z}) \).

**Lemma 12.** With the same hypothesis and notation as Lemma 11, \( G_{3} \) is a homocyclic \( p \)-group of rank two with a presentation
\[
G_{3} = \langle u, v \mid u^{p^{c}} = v^{p^{c}} = [u, v] = 1 \rangle \cong C_{p^{c}}^{2} \text{ for some } c \geq 1.
\]
Proof. By Lemma 8 we have \( G_3 = \langle u, v \rangle \). Assume that \( \langle u \rangle \cap \langle v \rangle = \langle u^i \rangle \), then \( u^i = v^j \) for some integer \( j \). Applying \( \eta \) to the relation we have \( u^i = (uv)^j \), so \( v^j = u^i = (uv)^j = u^jv^j \), and hence \( u^j = 1 \); since \( \tau(u) = v^{-1} \), we have \( o(u) = o(v) = p^c \) for some integer \( c \geq 0 \). Consequently \( v^j = 1 \), whence \( \langle u \rangle \cap \langle v \rangle = 1 \). Since \( G_3 > 1 \), we have \( c \geq 1 \). Therefore \( G_3 \) has the claimed presentation. \( \square \)

Proof of Theorem 1: By hypothesis \( G \) is maximally automorphic of class three. Since \( G_3 \leq \Phi(G) \) and \( G_3 \) char \( G \), by Lemma 4 the quotient \( \tilde{G} = G/G_3 \) is maximally automorphic of class two. It follows that \( \tilde{G} \) is one of the groups listed in Theorem 5. Denote \( u = [x, y, x] \) and \( v = [x, y, y] \). Then by Lemma 12 \( o(u) = o(v) = p^c \), \( c \geq 1 \), and \( G_3 = \langle u, v \mid u^{p^c} = v^{p^c} = [u, v] = 1 \rangle \cong C_{p^c}^2 \). Therefore \( G \) is a central extension of a homocyclic \( p \)-group \( G_3 \cong C_{p^c}^2 \) by a maximally automorphic \( p \)-group of class two. In what follows, we prove the result in three steps.

Step (1). Determination of the presentation of \( \tilde{G} \).

We distinguish two cases according to the presentation of \( \tilde{G} \) listed in Theorem 5.

Case (A). \( \tilde{G} \) has a presentation of the form

\[
\tilde{G} = \langle \bar{x}, \bar{y} \mid \bar{x}^{p^c} = \bar{y}^{p^c} = \bar{z}^{p^c} = [\bar{z}, \bar{x}] = [\bar{z}, \bar{y}] = 1, \bar{z} = [\bar{x}, \bar{y}] \rangle,
\]

where \( p \) is a prime, \( p \geq 2 \). We assume that

\[
z^{p^c} = u^iv^j, \tag{5}
\]

\[
x^{p^c} = u^r v^s, \tag{6}
\]

where \( i, j, r, s \in \mathbb{Z}_{p^c} \). Then \( u^{p^c} = [z, x]^{p^c} = [z^{p^c}, x] = [u^iv^j, x] = 1 \), so \( c \leq b \). Applying the automorphisms \( \tau \) and \( \eta \) to Eq. (5) we obtain \( z^{p^c} = u^iv^j \) and \( (zu)^{p^c} = u^{i+j}v^j \). Since \( c \leq b \), the latter is reduced to \( z^{p^c} = u^{i+j}v^j \). Combining these relations with Eq. (5) yields \( u^{i-j} = u^{i-j} \) and \( u^j = 1 \), so \( i \equiv j \equiv 0 \) (mod \( p^c \)), which implies that \( o(z) = p^b \) and \( \langle z \rangle \cap G_3 = 1 \). Moreover, by Lemma 8 and using substitution for \( x^{p^c} \) in Eq. (6) we have

\[
1 = [u^rv^s, y] \quad [x^{p^c}, y] \quad z^{p^c} u^{(p^c)}
\]

so \( z^{p^c} = u^{-(p^c)} \). Since \( \langle z \rangle \cap G_3 = 1 \), we have \( z^{p^c} = u^{-(p^c)} = 1 \), whence \( b \leq a \) and

\[
\left( \frac{p^a}{2} \right) \equiv 0 \pmod{p^c}. \tag{7}
\]
Moreover, applying $\pi$ and $\eta$ to Eq. (6) we have $x^{p^s} = u^{-r}v^s$ and $x^{p^s} = u^{r+s}v^s$. Combining these relations with Eq. (11) yields $u^{2r} = 1$ and $u^s = 1$, so $s \equiv 0 \pmod{p^c}$ and

$$2r \equiv 0 \pmod{p^c}. \quad (8)$$

Therefore Eq. (6) is reduced to $x^{p^s} = u^{-r}$. Applying $\tau$ to this relation we get $y^{p^s} = v^{-r}$, and applying $\eta$ to the latter equation yields $(yx)^{p^s} = u^{-r}v^{-r}$. So by Lemma 5 we have

$$u^{-r}v^{-r} = (yx)^{p^s} \equiv y^{p^s}z_{\alpha}^{(r^s)}u^{-\alpha}v^{-\alpha}x^{p^s} = z_{\alpha}^{(r^s)}u^{-\alpha}v^{-\alpha}r \equiv z_{\alpha}^{(r^s)}u^{-\alpha}v^{-\alpha}r \equiv z_{\alpha}^{(r^s)}u^{-\alpha}v^{-\alpha}r.$$

This is reduced to $z_{\alpha}^{(r^s)} = u^{2r}v^{-\alpha} \equiv u^{(s)}v^{-\alpha}$. Since $(z) \cap G_3 = \langle u \rangle \cap \langle v \rangle = 1$, we get

$$\begin{align*}
\left(\frac{p^a}{2}\right) & \equiv 0 \pmod{p^b}, \\
\left(\frac{p^a}{3}\right) & \equiv 0 \pmod{p^b}.
\end{align*} \quad (9)$$

If $p > 2$, then by Eq. (8) we get $r \equiv 0 \pmod{p^c}$; in particular, if $p = 3$, then by Eq. (10) we have $c \leq a - 1$. Consequently we obtain the groups in (i) and (ii). On the other hand, if $p = 2$, then by Eq. (9) we get $b \leq a - 1$, and by Eq. (8) either $r \equiv 0 \pmod{2^c}$ or $r \equiv 2^{-1} \pmod{2^c}$, corresponding to the groups in (iii) and (iv) respectively.

**Case (B).** $\tilde{G}$ has a presentation of the form

$$\tilde{G} = \langle \bar{x}, \bar{y} \mid \bar{z}^{2a-1} = [\bar{z}, \bar{x}] = [\bar{z}, \bar{y}] = 1, \bar{x}^{2a-1} = \bar{y}^{2a-1} = \bar{z}^{2a-2}, \bar{z} = [\bar{x}, \bar{y}] \rangle.$$

As before we assume that

$$\begin{align*}
z^{2a-1} & = u^iv^j, \\
x^{2a-1} & = z^{2a-2}u^iv^s,
\end{align*} \quad (11)$$

where $i, j, r, s \in \mathbb{Z}_{2^c}$. Since $u^{2a-1} = [z^{2a-1}, x] = [u^iv^j, x] = 1$, we have $c \leq a - 1$. Applying $\tau$ and $\eta$ to Eq. (11) we get $z^{2a-1} = u^iv^j$ and $z^{2a-1} = u^{i+j}v^j$. Combining these with Eq. (11) we obtain $u^{-i+j} = v^{i+j}$ and $v^j = 1$, so $i \equiv j \equiv 0 \pmod{2^c}$, and hence $o(z) = 2^{a-1}$ and $(z) \cap G_3 = 1$.

Moreover, by Lemma 8 we have $[x^{2a-1}, y] = z^{2a-1}u(z^{a-1}) = u(z^{a-1})$, and by Eq. (12) we have $[x^{2a-1}, y] = [z^{2a-2}u^iv^j, y] = [z^{2a-2}, y] = v^{2a-2}$, so $u^{(2a-1)} =
v^{2a-2}. Since \langle u \rangle \cap \langle v \rangle = 1, we get \( u^{(z^a+v)} = v^{2a-2} = 1 \), so \( c \leq a - 2 \). Applying \( \eta \) to Eq. (12) yields \( x^{2a-1} = z^{2a-2} - u^r v^s \). Combining this with Eq. (12) we get \( v^s = 1 \), so \( s \equiv 0 \) (mod \( 2^c \)). Hence Eq. (12) is reduced to \( x^{2a-1} = z^{2a-2} - u^r \). By applying \( \pi_1 = \tau \pi \tau : x \mapsto x, y \mapsto y^{-1} \) this relation is transformed to \( x^{2a-1} = z^{2a-2} - u^r \). Combining these two relations we get \( z^{2a-2} - u^r x^r = z^{2a-2} - u^r \), so \( u^r x^r = 1 \), and hence \( 2r \equiv 0 \) (mod \( 2^c \)). It follows that either \( r \equiv 0 \) (mod \( 2^c \)) or \( r \equiv 2^{a-1} \) (mod \( 2^c \)), corresponding to the groups in (v) and (vi) of Theorem 1.

It remains to show that in each case the group \( G \) given by the presentation is the desired extension, provided that the numerical conditions are satisfied. We will demonstrate the proof for Case (i) of Theorem 1 and leave other cases to the reader. We start with an abelian group \( N \) defined by the presentation

\[
N = \langle u, v, z \mid u^{3v} = v^{3y} = z^{3b} = [u, v] = [u, z] = [v, z] = 1 \rangle,
\]

where \( 1 \leq c \leq b \). Add an element \( x \) to \( N \) by

\[
x^{3v} = 1, u^x = u, v^x = v, z^x = zu,
\]

where \( c \leq a \). Then by Theorem 10 it is easily verified that \( H = \langle N, x \rangle \) is an extension of \( N \) by \( \langle x \rangle \cong C_{3^a} \). Moreover, add an element \( y \) to \( H \) by

\[
y^{3a} = 1, u^y = u, v^y = v, z^y = zv, x^y = xz,
\]

where \( b \leq a \). By Theorem 10 again \( K = \langle H, y \rangle \) is an extension of \( H \) by \( \langle y \rangle \cong C_{3^a} \). Thus \( K \) is a finite group with the presentation

\[
K = \langle u, v, z, x, y \mid u^{3v} \rangle = v^{3y} = z^{3b} = [u, v] = [u, z] = [v, z] = 1, \\
x^{3v} = 1, u^x = u, v^x = v, z^x = zu, \\
y^{3a} = 1, u^y = u, v^y = v, z^y = zv, x^y = xz, \rangle,
\]

where the numerical condition is \( 1 \leq c \leq b \leq a \). Observe that in the presentation of \( K \) the relations \( [u, v] = [u, z] = [u, z] = 1 \) can be derived from the others, so can be deleted, and the relations \( z^x = zu, u^x = u, v^x = v, u^y = v, v^y = xz, z^y = zu \) and \( z^y = zv \) can be rewritten as \( [x, u] = 1, [x, v] = 1, [y, u] = 1, [y, v] = 1, z = [x, y], u = [z, x] \) and \( v = [z, y] \), respectively. In particular if \( 1 \leq c < b = a \) or \( 1 \leq c \leq b \leq a - 1 \) then we have \( K = G \) (the reason why we have more restrictive numerical conditions is that \( G \) is maximally automorphic, as one can see from the preceding proof). In particular, the defining relations give true orders of the generating elements. We remark that one may employ an alternative approach to verify the existence of such an extension, see [23, Chapter 9].
Theorem 1, and leave the verification for other cases to the reader. By von Dyck’s Theorem \[20\] the assignment $x \mapsto x$, $y \mapsto y_1$ extends to an epimorphism from $G$ onto itself, which therefore must be an automorphism of $G$. We will demonstrate this for Case (i) of Theorem 1 and leave the verification for other cases to the reader.

Denote $z_1 = [x_1, y_1]$, $u_1 = [z_1, x_1]$ and $v_1 = [z_1, y_1]$. Bearing formulae in Remark 2 in mind we do the following calculation:

$$z_1 = [x^i y^j z^k u^m v^n, x^r y^s z^t u^h v^f] = [x^i y^j z^k, x^r y^s z^t]$$

$$= [x^i, y^j]^{z^k} [x^r, y^s]^{z^t} [x^i, y^j]$$

$$= [x^i, y^j]^{z^k} [y^j, x^r y^s] [x^i y^j, z^t] [z, x^r y^s]^k$$

$$= [x^i, y^j]^{z^k} [y^j, x^r]^{z^t} [x, z]^t [y, z]^{jr} [z, x]^k [z, y]^s k$$

$$= (z^{is} u^i v^j z^k y^j (z^{jr} u^j v^s) v^f u^{kr} u(v^{ks} v^f)$$

$$u = [z^{is} u^i v^j z^k y^j u^{kr} u(v^{ks} v^f)$$

$$v = [z^{is} u^i v^j z^k y^j u^{kr} u(v^{ks} v^f)$$

It is clear that $z_1^3 = u_1^9 = v_1^3 = [x_1, u_1] = [x_1, v_1] = [y_1, u_1] = [y_1, v_1] = 1$. It remains to show $x_1^3 = y_1^3 = 1$. Note that $\exp(G_2) = 3^b$ and $\exp(G_3) = 3^c$ where either $c < b = a$ or $c \leq b < a - 1$. By formula (3) we have

$$x_1^{3a} = (x^i y^j z^k u^m v^n)^{3a} = (x^i y^j z^k)^{3a} = (x^i y^j)^{3a} [x^i, y^j, z^k]^{3a} z^{k^3a}$$

$$= x^{3a} [x^i, y^j]^{3a} [x^i, y^j, z^k]^{3a} [x^i, y^j, z^k]^{3a} y^{3a} u^{3a} v^{3a} u^{3a} v^{3a} = 1.$$
Table 2: Invariant Types of $G_3$, $G'$ and $G^{ab}$

| Case | $G_3$ | $G'$ | $G^{ab}$ | Condition |
|------|-------|------|----------|-----------|
| (i)  | $C_2^{3c}$ | $C_2^{3c} \times C_3^{3y}$ | $C_2^{3a}$ | $1 \leq c < b = a$ or $1 \leq c < b \leq a - 1$ |
| (ii) | $C_2^{p^c}$ | $C_2^{p^c} \times C_3^{p^y}$ | $C_2^{p^a}$ | $1 \leq c \leq b \leq a$ |
| (iii) | $C_2^{p^c}$ | $C_2^{p^c} \times C_3^{p^y}$ | $C_2^{p^a}$ | $1 \leq c < b \leq a - 1$ |
| (iv) | $C_2^{2c}$ | $C_2^{2c} \times C_3^{2y}$ | $C_2^{2a}$ | $1 \leq c \leq b \leq a - 1$ |
| (v)  | $C_2^{2c}$ | $C_2^{2c} \times C_2^{a-1}$ | $C_2^{2a-1}$ | $1 \leq c \leq a - 2$ |
| (vi) | $C_2^{2c}$ | $C_2^{2c} \times C_2^{a-1}$ | $C_2^{2a-1}$ | $1 \leq c \leq a - 2$ |

From the table it is easily seen that the groups are pairwise non-isomorphic, except possibly groups $A$ and $B$ from (v) and (vi), respectively, with $A' \cong B'$ and $A^{ab} \cong B^{ab}$. Let $A = \langle x, y \rangle$ and $B = \langle x', y' \rangle$, where the generating pairs satisfy the defining relations in (v) and (vi), respectively. If $A \cong B$ then there is a generating pair $(x_1, y_1)$ of $A$ such that the mapping $\alpha : x' \mapsto x_1, y' \mapsto y_1$ is an isomorphism from $B$ to $A$. Since $A$ is maximally automorphic, the mapping $\beta : x_1 \mapsto x, y_1 \mapsto y$ is an automorphism of $A$, so the composition $\gamma = \alpha \beta : x' \mapsto x, y' \mapsto y$ is an isomorphism from $B$ to $A$. We have $z^{2^a-2} = x^{2^a-1} = \gamma(x^{2^a-1}) = \gamma(z^{2^a-2} u^{2^a-1}) = z^{2^a-2} u^{2^a-1}$, so $u^{2^a-1} = 1$. This is a contradiction since $o(u) = 2^c$. Therefore $A \not\cong B$.

By Corollary 3 each of the maximally automorphic $p$-groups of class three given by Theorem 1 determines a unique regular dessin. Their types and genera are summarized in Table 3.

Table 3: Uniquely Regular Dessins of Class Three

| Case | $|G|$ | Type | Genus |
|------|------|------|-------|
| (i)  | $2^{2(a+c)+b}$ | $(2^a, 3^a, 3^a)$ | $2^{a+b+2c+1}(2^a-1) + 1$ |
| (ii) | $p^{2(a+c)+b}$ | $(p^a, p^a, p^a)$ | $p^{a+b+2c+1}(p^a-1)/2 + 1$ |
| (iii) | $2^{2(a+c)+b}$ | $(2^a, 2^a, 2^a)$ | $2^{a+b+2c-1}(2^a-1) + 1$ |
| (iv) | $2^{2(a+c)+b}$ | $(2^a+2, 2^a+1, 2^a+1)$ | $2^{a+b+2c-2}(2^a+1-1) + 1$ |
| (v)  | $2^{2a+2c-3}$ | $(2^a, 2^a, 2^a)$ | $2^{a+b+2c-4}(2^a-3) + 1$ |
| (vi) | $2^{2a+2c-3}$ | $(2^a, 2^a, 2^a)$ | $2^{a+b+2c-4}(2^a-3) + 1$ |

Acknowledgement

The authors would like to thank the anonymous referees for helpful comments and suggestions which have improved the content and the presentation of the
paper. The first author is supported by Natural Science Foundation of Zhejiang Province (No. LQ17A010003). The second author is supported by the grants APVV-15-0220, VEGA 1/0150/14, Project LO1506 of the Czech Ministry of Education, Youth and Sports and Project P202/12/G061 of Czech Science Foundation. The third author is supported by Natural Science Foundation of Zhejiang Province (No. LY16A010010).

References

[1] G.V. Belyi, Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), 267-276.

[2] Y. Berkovich and Z. Janko, Groups of Prime Power Order (Vol II), Walter de Gruyter & Co., 2008.

[3] D. Garrison and L.-C. David, On some subnormality conditions in metabelian groups, In: Computational group theory and the theory of groups, 89–103, Contemp. Math., 470, Amer. Math. Soc., Providence, RI, 2008.

[4] G. González-Diez and A. Jaikin-Zapirain, The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces, Proc. London Math. Soc. 111(4) (2015), 775–796.

[5] A. Grothendieck, Esquisse d’un programme, in: L. Schneps and P. Lochak (eds.), Geometric Galois Actions 1. The inverse Galois problem, Moduli Spaces and Mapping Class Groups, London Math. Soc. Lecture Notes Ser. 242, Cambridge Univ. Press, Cambridge, 1997.

[6] P. Hall, A contribution to the theory of groups of prime power orders, Proc. London Math. Soc. 36 (1933), 29–95.

[7] P. Herman, On a class of finite groups having isomorphic maximal subgroups, Ann. Univ. Sci. Budapest, Eötvös Sect. Math. 24 (1981), 87–92.

[8] P. Herman, On finite $p$-groups with isomorphic maximal subgroups, J. Austral. Math. Soc. Ser. A 48(2) (1990), 199–213.

[9] P. Herman, MI-groups acting uniserially on a normal subgroup, Group ’93 Galway/St. Andrews, Vol. 1(Galway, 1993), 264–268, London Math. Soc. Lecture Note Ser. 211, Cambridge Univ. Press, Cambridge, 1995.
[10] G.T. Hogan and W.P. Kappe, On the $H_p$-problem for finite $p$-groups, Proc. Amer. Math. Soc. 20 (1969), 450–454.

[11] K. Hu, R. Nedela and N.-E. Wang, Nilpotent groups of class two which underly a unique regular dessin, Geom. Dedicata 179 (2015), 177–186.

[12] B. Huppert, Endliche Gruppen (Vol. I), Springer-Verlag, Berlin, 1967.

[13] I.M. Isaacs, Finite Group Theory, Amer. Math. Soc., Providence RI, 2008.

[14] G.A. Jones, Regular dessins with a given automorphism group, In: M. Izquierdo, S.A. Broughton, A.F. Costa, R.E. Rodríguez (eds), Riemann and Klein surfaces, Automorphisms, Symmetries and Moluli Spaces. American Math. Soc., Providence, Rhode Island, 2014.

[15] G.A. Jones, Bipartite graph embeddings, Riemann surfaces and Galois groups, Discrete Math. 338 (2015), 1801–1913.

[16] G.A. Jones, Hypermaps and multiply quasiplatonic Riemann surfaces, European J. Combin. 33(7) (2012), 1588–1605.

[17] G.A. Jones and D. Pinto, Hypermap operations of finite order, Discrete Math. 310 (2010), 1820–1827.

[18] G.A. Jones and D. Singerman, Belyi functions, hypermaps and Galois groups, Bull. London Math. Soc. 28 (1996), 561–590.

[19] G.A. Jones and J. Wolfart, Dessins d’Enfants on Riemann surfaces, Springer Monographs in Mathematics, Springer, Heidelberg, 2016.

[20] R.C. Lyndon and P.E. Schupp, Combinatorial Group Theory, Springer-Verlage, Berlin - Heidelberg - New York, 1977.

[21] G. Malle, J. Saxl and T. Weigel, Generators of classical groups, Geom. Dedicata 49 (1994), 85–116.

[22] A. Mann, On $p$-groups whose maximal subgroups are isomorphic, J. Austral. Math. Soc. Ser. A 59 (2) (1995), 143–147.

[23] C.C. Sims, Computation with finitely presented groups, Encyclopedia of Mathematics and its Applications, 48, Cambridge University Press, Cambridge, 1994.

[24] M. Xu and H. Qu, Finite $p$-Groups (in Chinese), Peking University Press, Beijing, 2010.