Geometry of integers revisited

Igor V. Nikolaev

Abstract. We study geometry of the ring of integers $O_K$ of a number field $K$. Namely, it is proved that the inclusion $\mathbb{Z} \subset O_K$ defines a covering of the Riemann sphere $\mathbb{C}P^1$ ramified over the points $\{0, 1, \infty\}$. Our approach is based on the notion of a Serre $C^*$-algebra. As an application, a new proof of the Belyi Theorem is given.

Mathematics Subject Classification. Primary 11R04, 14H55; Secondary 46L85.

Keywords. Arithmetic geometry, Serre $C^*$-algebra.

1. Introduction

An interplay between arithmetic and geometry is well known [11]. The Weil’s Conjectures were a motivation for the notion of a scheme [3]. Recall that the spectrum $\text{Spec } R$ of a commutative ring $R$ is the set of all prime ideals of $R$ endowed with the Zariski topology. Such a topology is non-Hausdorff but admits a cohomology theory and an analog of the Lefschetz Fixed-Point Theorem. The latter is enough to prove Weil’s Conjectures.

Let $\mathbb{Z}$ be the ring of integers. It was noticed long ago that the space $\text{Spec } \mathbb{Z}$ is “similar” to the Riemann sphere $\mathbb{C}P^1$ [2, p. 83]. Moreover, if $O_K$ is the ring of integers of a number field $K$, then the inclusion $\mathbb{Z} \subset O_K$ corresponds to a Riemann surface $\mathcal{R}$, such that there exists a ramified covering map $\mathcal{R} \to \mathbb{C}P^1$. The Grothendieck’s theory of schemes cannot explain this analogy [6, Section 2.2].

In this note we clarify the relation between the ring $\mathbb{Z}$ and the sphere $\mathbb{C}P^1$. Namely, it is proved that the inclusion $\mathbb{Z} \subset O_K$ defines a covering $\mathcal{R} \to \mathbb{C}P^1$ ramified over three points $\{0, 1, \infty\}$ (Theorem 1.3). Our approach is based on the notion of a Serre $C^*$-algebra [7, Section 5.3.1]. To formalize our results, we need the following definitions.

Let $V$ be a complex projective variety. Denote by $B(V, \mathcal{L}, \sigma)$ the twisted homogeneous coordinate ring of $V$, where $\mathcal{L}$ is an invertible sheaf and $\sigma$ is an automorphism of $V$ [10, p. 173]. Recall that the Serre $C^*$-algebra, $\mathcal{A}_V$, is the norm closure of a self-adjoint representation of the ring $B(V, \mathcal{L}, \sigma)$ by the
bounded linear operators on a Hilbert space $\mathcal{H}$; such an algebra depends on
$V$ alone, since the values of $L$ and $\sigma$ are fixed by the $\ast$-involution of algebra
$B(V, L, \sigma)$ [7, Section 5.3.1]. The map $V \mapsto \mathcal{A}_V$ is a functor. Namely, if $V$
and $V'$ are defined over a number field $K \subset \mathbb{C}$, then $V$ is $K$-isomorphic to $V'$
if and only if the algebra $\mathcal{A}_V$ is isomorphic to $\mathcal{A}_{V'}$. In contrast, the variety
$V$ is $\mathbb{C}$-isomorphic to $V'$ if and only if the algebra $\mathcal{A}_V$ is Morita equivalent to
$\mathcal{A}_{V'}$, i.e. $\mathcal{A}_V \otimes \mathcal{H} \cong \mathcal{A}_{V'} \otimes \mathcal{H}$, where $\mathcal{H}$ is the $C^*$-algebra of compact operators [9, Corollary 1.2]. In other words, the tensor product $\mathcal{A}_V \otimes \mathcal{H}$ is an analog of
the change of base from $K$ to $\mathbb{C}$.

The latter remark can be used to “geometrize” the ring $O_K$ as follows. Recall that there exists an isomorphism $B(V, L, \sigma) \cong M_2(R)$, where $R$ is the
homogeneous coordinate ring of a variety $V$ [10, Section 8]. If $R \cong O_K$, then
the norm closure of a self-adjoint representation of the ring $M_2(O_K)$ is a
$C^*$-algebra which we denote by $\mathcal{A}_{O_K}$. Notice that in general the $\mathcal{A}_{O_K}$ is no
longer the Serre $C^*$-algebra. However, changing the base from $K$ to $\mathbb{C}$, we
conclude that the tensor product $\mathcal{A}_{O_K} \otimes \mathcal{H}$ must be isomorphic to a Serre
$C^*$-algebra. Thus, one gets the following definition.

**Definition 1.1.** The complex projective variety $V$ will be called an *avatar* of
the ring $O_K$, if there exists a $C^*$-algebra homomorphism

$$h : \mathcal{A}_V \to \mathcal{A}_{O_K} \otimes \mathcal{H}.$$  \hfill (1.1)

**Example 1.2.** If $R$ is the homogeneous coordinate ring of a complex projective
variety $V$, then $V$ is the avatar of $R$. In this case, $\mathcal{A}_R \otimes \mathcal{H} \cong \mathcal{A}_V$, i.e. the
map $h$ is a $C^*$-algebra isomorphism.

Our main result can be formulated as follows.

**Theorem 1.3.** Let $\mathbb{Z}$ be the ring of rational integers and let $O_K$ be the ring of
algebraic integers of a number field $K$. Then:

(i) the Riemann sphere $\mathbb{C}P^1$ is an avatar of the ring $\mathbb{Z}$;
(ii) there exists a Riemann surface $\mathcal{R} = \mathcal{R}(K)$, such that $\mathcal{R}$ is an avatar of
the ring $O_K$;
(iii) the inclusion $\mathbb{Z} \subset O_K$ defines a covering $\mathcal{R} \to \mathbb{C}P^1$ ramified over the
points $\{0, 1, \infty\}$.

The article is organized as follows. In Sect. 2 we briefly review noncommutative
algebraic geometry and arithmetic groups. Theorem 1.3 is proved
in Sect. 3. As an application of theorem 1.3, we give a new proof of the Belyi
Theorem [Belyi 1979] [1, Theorem 4].

## 2. Preliminaries

We review some facts of noncommutative algebraic geometry and arithmetic
groups. The reader is referred to [4,10] for a detailed account.

---

1For the lack of a better word meaning the “image”.
2.1. Noncommutative algebraic geometry

Let $V$ be a projective variety over the field $k$. Denote by $\mathcal{L}$ an invertible sheaf of the linear forms on $V$. If $\sigma$ is an automorphism of $V$, then the pullback of $\mathcal{L}$ along $\sigma$ will be denoted by $\mathcal{L}^\sigma$, i.e. $\mathcal{L}^\sigma(U) := \mathcal{L}(\sigma U)$ for every $U \subset V$. The graded $k$-algebra

$$B(V, \mathcal{L}, \sigma) = \bigoplus_{i \geq 0} H^0 \left( V, \mathcal{L} \otimes \mathcal{L}^\sigma \otimes \cdots \otimes \mathcal{L}^{i-1} \right)$$

is called a twisted homogeneous coordinate ring of $V$. Such a ring is always non-commutative, unless the automorphism $\sigma$ is trivial. A multiplication of sections of $B(V, \mathcal{L}, \sigma) = \bigoplus_{i=1}^{\infty} B_i$ is defined by the rule $ab = a \otimes b$, where $a \in B_m$ and $b \in B_n$. An invertible sheaf $\mathcal{L}$ on $V$ is called $\sigma$-ample, if for every coherent sheaf $\mathcal{F}$ on $V$, the cohomology group $H^k(V, \mathcal{L} \otimes \mathcal{L}^\sigma \otimes \cdots \otimes \mathcal{L}^{n-1} \otimes \mathcal{F})$ vanishes for $k > 0$ and $n >> 0$. If $\mathcal{L}$ is a $\sigma$-ample invertible sheaf on $V$, then

$$\text{Mod} \left( B(V, \mathcal{L}, \sigma) \right) / \text{Tors} \cong \text{Coh} (V),$$

where Mod is the category of graded left modules over the ring $B(V, \mathcal{L}, \sigma)$, Tors is the full subcategory of Mod of the torsion modules and Coh is the category of quasi-coherent sheaves on a scheme $V$. In other words, the $B(V, \mathcal{L}, \sigma)$ is a coordinate ring of the variety $V$.

Example 2.1. ([10, p.173]) Denote by $P^1(k)$ a projective line over the field $k$. Consider an automorphism $\sigma$ of the $P^1(k)$ given by the formula $\sigma(u) = qu$, where $u \in P^1(k)$ and $q \in k^\times$. Then $B(P^1(k), \mathcal{L}, \sigma) \cong U_q$, where $U_q$ is the $k$-algebra of polynomials in variables $x_1$ and $x_2$ satisfying a commutation relation:

$$x_2 x_1 = qx_1 x_2.$$  \hfill (2.3)

Example 2.2. ([10, p.197]) Denote by $E(k) = \{ (u, v, w, z) \in P^3(k) \mid u^2 + v^2 + w^2 + z^2 = \frac{1 - \alpha}{1 + \beta} u^2 + \frac{1 - \gamma}{1 + \gamma} w^2 + z^2 = 0 \}$ an elliptic curve over the field $k$, where $\alpha, \beta, \gamma \in k$ are constants, such that $\beta \neq -1$ and $\gamma \neq 1$. Let $\sigma$ be a shift automorphism of the $E(k)$. Then $B(E(k), \mathcal{L}, \sigma) \cong S(\alpha, \beta, \gamma)$, where $S(\alpha, \beta, \gamma)$ is the Sklyanin algebra on four generators $x_i$ satisfying the commutation relations:

$$\begin{align*}
    x_1 x_2 - x_2 x_1 &= \alpha (x_3 x_4 + x_4 x_3), \\
    x_1 x_2 + x_2 x_1 &= x_3 x_4 - x_4 x_3, \\
    x_1 x_3 - x_3 x_1 &= \beta (x_4 x_2 + x_2 x_4), \\
    x_1 x_3 + x_3 x_1 &= x_4 x_2 - x_2 x_4, \\
    x_1 x_4 - x_4 x_1 &= \gamma (x_2 x_3 + x_3 x_2), \\
    x_1 x_4 + x_4 x_1 &= x_2 x_3 - x_3 x_2,
\end{align*}$$

where $\alpha + \beta + \gamma + \alpha \beta \gamma = 0$. \hfill (2.4)

Example 2.3. ([8, Lemma 3.1]) Let $\mathcal{R}$ be an arithmetic Riemann surface, i.e. given by the AF-algebra of stationary type [7, Section 5.2]. (Such Riemann surfaces can be identified with the complex algebraic curves defined over a number field.) Then

$$B(\mathcal{R}, \mathcal{L}, \sigma) \cong R[\pi_1(S^3 \setminus \mathcal{L})],$$

(2.5)
where $\mathcal{L}$ is a link embedded in the three-sphere $S^3$ and $R[\pi_1(S^3 \setminus \mathcal{L})]$ is the group ring of the fundamental group $\pi_1(S^3 \setminus \mathcal{L})$.

### 2.2. Arithmetic groups

Let $G$ be a linear algebraic group defined over the field $\mathbb{Q}$. Denote by $G_\mathbb{Z}$ the group of integer points of $G$. A subgroup $\Gamma \subset G$ is called arithmetic if $\Gamma$ is commensurable with the $G_\mathbb{Z}$, i.e. $\Gamma \cap G_\mathbb{Z}$ has a finite index both in $\Gamma$ and $G_\mathbb{Z}$. Informally, the arithmetic group is a discrete subgroup of the group $GL_n(\mathbb{C})$ defined by some arithmetic properties. For instance, $\mathbb{Z} \subset \mathbb{R}$, $GL_n(\mathbb{Z}) \subset GL_n(\mathbb{R})$ and $SL_n(\mathbb{Z}) \subset SL_n(\mathbb{R})$ are examples of the arithmetic groups.

Denote by $\mathcal{O}$ the ring of algebraic integers of all finite extensions of the number field $\mathbb{Q}$. Let $H^3$ be the hyperbolic 3-dimensional space. The following remarkable result establishes a deep link between arithmetic groups and topology.

**Theorem 2.4.** ([5, p. 169]) Let $M = H^3 / \Gamma$ be a finite volume hyperbolic 3-manifold. Then $\Gamma$ is conjugate to a subgroup of the group $PSL_2(\mathcal{O})$.

**Example 2.5.** Let $\mathcal{L}$ be a hyperbolic link, i.e. $S^3 \setminus \mathcal{L} \cong H^3 / \Gamma$ for an arithmetic group $\Gamma$. Then

$$\pi_1(S^3 \setminus \mathcal{L}) \cong \Gamma.$$  \hfill (2.6)

### 3. Proof of theorem 1.3

(i) Let us show that the $\mathbb{C}P^1$ is an avatar of $\mathbb{Z}$. Indeed, in this case $R \cong \mathbb{Z}$ and $\mathbb{C}^2_\mathbb{Z}$ is the closure of a self-adjoint representation of the ring $M_2(\mathbb{Z})$. Consider the group $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) / \pm I$, where $SL_2(\mathbb{Z})$ is the group of invertible elements of $M_2(\mathbb{Z})$. Recall that the group $PSL_2(\mathbb{Z})$ is generated by the matrices:

$$u = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad v = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$  \hfill (3.1)

which satisfy the relations modulo $\pm I$:

$$u^2 = v^3 = 1.$$  \hfill (3.2)

On the other hand, consider Example 2.1 with $k \cong \mathbb{Q}$ and assume that $q = -1$ in relation (2.3). In other words, one gets a relation:

$$x_2x_1 = -x_1x_2.$$  \hfill (3.3)

Consider a substitution:

$$\begin{cases} u = x_2x_1x_2^{-1}x_1^{-1} \\ v = x_2. \end{cases}$$  \hfill (3.4)

The reader can verify, that substitution (3.4) and relation (3.3) reduces relations (3.2) to the form:

$$x_2^3 = 1.$$  \hfill (3.5)
Let \( \mathcal{I} \) be a two-sided ideal in the algebra \( B(P^1(\mathbb{Q}), \mathcal{L}, \sigma) \) of Example 2.1 generated by relation (3.5). In view of (3.2)–(3.5), one gets a ring isomorphism:

\[
B(P^1(\mathbb{Q}), \mathcal{L}, \sigma)/\mathcal{I} \cong M_2(\mathbb{Z}). \tag{3.6}
\]

Let \( \rho \) be a self-adjoint representation of the ring \( B(P^1(\mathbb{Q}), \mathcal{L}, \sigma) \) by the linear operators on a Hilbert space \( \mathcal{H} \). Notice that such a representation exists, because relation (3.3) is invariant under the involution \( x_1^* = x_2 \) and \( x_2^* = x_1 \). Since \( \rho(B(P^1(\mathbb{Q}), \mathcal{L}, \sigma)) = \mathcal{A}_{P^1(\mathbb{Q})} \) and \( \rho(M_2(\mathbb{Z})) = \mathcal{A}_Z \), it follows from (3.6) that there exists a \( C^* \)-algebra homomorphism

\[
h : \mathcal{A}_{P^1(\mathbb{Q})} \to \mathcal{A}_Z, \tag{3.7}
\]

where \( \ker h = \rho(\mathcal{I}) \). The homomorphism \( h \) extends to a homomorphism between the products

\[
h : \mathcal{A}_{P^1(\mathbb{Q})} \otimes \mathcal{K} \to \mathcal{A}_Z \otimes \mathcal{K}, \tag{3.8}
\]

where \( \mathcal{K} \) is the \( C^* \)-algebra of compact operators. But \( \mathcal{A}_{P^1(\mathbb{Q})} \otimes \mathcal{K} \cong \mathcal{A}_{CP^1} \) and, therefore, one gets a \( C^* \)-algebra homomorphism

\[
h : \mathcal{A}_{CP^1} \to \mathcal{A}_Z \otimes \mathcal{K}. \tag{3.9}
\]

In other words, the Riemann sphere \( CP^1 \) is an avatar of the ring \( \mathbb{Z} \).

(ii) Let us show that if \( K \) is a number field, then there exists a Riemann surface \( \mathcal{R} \), such that \( \mathcal{R} \) is an avatar of the ring \( O_K \). Indeed, we can always assume that \( K \) has at least one complex embedding and fix one of such embeddings \( K \not\subset \mathbb{R} \). (For otherwise, we replace \( K \) by a CM-field of \( K \), i.e. a totally imaginary quadratic extension of the totally real field \( K \). This case corresponds to the double covering \( \mathcal{R}' \) of the Riemann surface \( \mathcal{R} \).) For simplicity, let \( R \cong O_K \) and \( \Gamma \cong PSL_2(O_K) \). (The case of a non-maximal order \( \Lambda \subseteq O_K \) is treated likewise and corresponds to the covering of the Riemann surface \( \mathcal{R} \).) In view of (2.6), there exists a hyperbolic link \( \mathcal{L} \), such that:

\[
PSL_2(O_K) \cong \pi_1(S^3 \setminus \mathcal{L}). \tag{3.10}
\]

On the other hand, it is known that

\[
R[\pi_1(S^3 \setminus \mathcal{L})] \cong B(\mathcal{R}, \mathcal{L}, \sigma), \tag{3.11}
\]

where \( R[\pi_1(S^3 \setminus \mathcal{L})] \) is the group ring of \( \pi_1(S^3 \setminus \mathcal{L}) \) and \( \mathcal{R} \) is a Riemann surface, see Example 2.3. In particular, it follows from (3.10) that

\[
B(\mathcal{R}, \mathcal{L}, \sigma) \cong R[PSL_2(O_K)]. \tag{3.12}
\]

Let \( \rho \) be a self-adjoint representation of the ring \( B(\mathcal{R}, \mathcal{L}, \sigma) \) by the linear operators on a Hilbert space \( \mathcal{K} \). The norm closure of \( \rho(B(\mathcal{R}, \mathcal{L}, \sigma)) \) is the Serre \( C^* \)-algebra \( \mathcal{A}_{\mathcal{R}} \).

On the other hand, it follows from (3.12) that taking the norm closure of \( \rho(R[PSL_2(O_K)]) \), one gets a \( C^* \)-algebra \( \mathcal{A}_{O_K} \), such that

\[
\mathcal{A}_{O_K} \otimes \mathcal{K} \cong \mathcal{A}_{\mathcal{R}}. \tag{3.13}
\]

In other words, there exists an isomorphism:

\[
h : \mathcal{A}_{\mathcal{R}} \to \mathcal{A}_{O_K} \otimes \mathcal{K}. \tag{3.14}
\]
(iii) Finally, let us show that the inclusion $Z \subset O_K$ defines a covering $R \to \mathbb{C}P^1$ ramified over three points $\{0, 1, \infty\}$. 

In the lemma below we shall prove a stronger result. Namely, let $\mathfrak{A}$ be a category of the Galois extensions of the field $\mathbb{Q}$, such that the morphisms in $\mathfrak{A}$ are inclusions $K \subseteq K'$, where $K, K' \in \mathfrak{A}$. Likewise, let $\mathfrak{R}$ be a category of the Riemann surfaces, such that the morphisms in $\mathfrak{R}$ are holomorphic maps $R \to \mathcal{R}'$, where $R, \mathcal{R}' \in \mathfrak{R}$. Let $F: \mathfrak{A} \to \mathfrak{R}$ be a map acting by the formula $O_K \mapsto R$, where $R$ is the Riemann surface defined by the isomorphism (3.12).

Remark 3.1. The category $\mathfrak{R}$ consists of the Riemann surfaces, which are algebraic curves defined over a number field. In particular, the morphisms in $\mathfrak{R}$ can be defined over the number field. Both facts follow from the property of the AF-algebra $A_R$ being of a stationary type [7, Section 5.2]. We refer the reader to Example 2.3 and [8, Lemma 3.1].

Lemma 3.2. The map $F: \mathfrak{A} \to \mathfrak{R}$ is a covariant functor, i.e. $F$ transforms inclusions in the category $\mathfrak{A}$ to holomorphic maps in the category $\mathfrak{R}$.

Proof. Let $K \in \mathfrak{A}$ be a number field and let $R = F(K)$ be the corresponding Riemann surface $R \in \mathfrak{R}$. Let $K \subseteq K'$ be an inclusion, where $K' \in \mathfrak{R}$.

Using isomorphism (3.13), one gets an inclusion of the corresponding Serre $C^*$-algebras:

$$A_R \subseteq A_{R'}, \quad \text{(3.15)}$$

On the other hand, it is known the algebra $A_R$ is a coordinate ring of the Riemann surface $R$ [7, Theorem 5.2.1]. In particular, if $h: A_{R'} \to A_R$ is a homomorphism, one gets a holomorphic map $w: R' \to R$ defined by a commutative diagram in Fig. 1.

Thus $F$ is a functor, which maps the inclusion $K \subseteq K'$ into a holomorphic map $w: R' \to R$. The reader can verify that $F$ is a covariant functor. Lemma 3.2 is proved. □

Lemma 3.3. The inclusion $Z \subset O_K$ defines a covering $R \to \mathbb{C}P^1$ ramified over three points $\{0, 1, \infty\}$.

Proof. Let $\mathbb{U}$ be the Riemann sphere $\mathbb{C}P^1$ without three points, which we always assume to be $\{0, 1, \infty\}$ after a proper Möbius transformation. It is
easy to see, that the fundamental group $\pi_1(\mathcal{U}) \cong \mathbb{F}_2$, where $\mathbb{F}_2$ is a free group on two generators $u$ and $v$.

Since the Riemann surface $\mathcal{U}$ corresponds to an unlink $\mathcal{L} \cong S^1 \cup S^1$, one gets an isomorphism:

$$B(P^1(\mathcal{U}, \mathcal{L}, \sigma)) \cong R[\mathbb{F}_2].$$  \hspace{1cm} (3.16)

Consider a two-sided ideal $\mathcal{I} \subset B(P^1(\mathcal{U}, \mathcal{L}, \sigma))$ generated by relations (3.2). In view of (3.16), we have:

$$B(P^1(\mathcal{U}, \mathcal{L}, \sigma))/\mathcal{I} \cong R[PSL_2(\mathbb{Z})].$$  \hspace{1cm} (3.17)

In other words, one gets a homomorphism between the $C^*$-algebras:

$$\mathcal{A}_\mathcal{U} \to \mathcal{A}_{CP^1}.$$  \hspace{1cm} (3.18)

Using the commutative diagram in Fig. 1, we get a holomorphic map between the corresponding Riemann surfaces:

$$\mathcal{U} \to CP^1.$$  \hspace{1cm} (3.19)

Let now $\mathcal{Z} \subset O_K$ be an inclusion, where $K$ is a number field. By item (ii) of Theorem 1.3 there exists a Riemann surface $\mathcal{R} \in \mathcal{R}$ corresponding to $O_K$. By Lemma 3.2, there exists a holomorphic map:

$$\mathcal{R} \to CP^1.$$  \hspace{1cm} (3.20)

Using (3.19) and (3.20), one gets a commutative diagram in Fig. 2. We use the diagram in Fig. 2 to define a holomorphic map:

$$\mathcal{R} \to \mathcal{U}.$$  \hspace{1cm} (3.21)

Since $\mathcal{U} = CP^1\setminus\{0, 1, \infty\}$, one gets the conclusion of Lemma 3.3. \hspace{1cm} □

Item (iii) of Theorem 1.3 follows from Lemmas 3.2 and 3.3. Theorem 1.3 is proved.

4. Belyi’s Theorem

Belyi’s Theorem says that the algebraic curve $\mathcal{R}$ can be defined over a number field if and only if there exist a covering $\mathcal{R} \to CP^1$ ramified over three points of the Riemann sphere $CP^1$. This remarkable result was proved by [1, Theorem 4]. In this section we show that Belyi’s Theorem follows from Theorem 1.3 and remark 3.1.
Theorem 4.1. (Belyi’s Theorem) A complete non-singular algebraic curve over $\mathbb{C}$ can be defined over an algebraic number field if and only if such a curve is a covering of the Riemann sphere $\mathbb{CP}^1$ ramified over three points.

Proof. We identify the Riemann surface $\mathcal{R} \in \mathfrak{R}$ with a complete non-singular algebraic curve over the field of characteristic zero (Chow’s Theorem).

In view of the Remark 3.1, we have $\mathcal{R} \in \mathfrak{R}$ is the algebraic curve defined over a finite extension of the field $\mathbb{Q}$. On the other hand, item (iii) of Theorem 1.3 says that each Riemann surface $\mathcal{R} \in \mathfrak{R}$ is a covering of the $\mathbb{CP}^1$ ramified over the points $\{0, 1, \infty\}$. The “only if” part of Belyi’s Theorem follows.

Let $\mathcal{R}$ be a covering of the $\mathbb{CP}^1$ ramified over the points $\{0, 1, \infty\}$. Using Lemma 3.2, one can construct a ring $O_K$ corresponding to the Riemann surface $\mathcal{R}$. By item (ii) of Theorem 1.3 and Remark 3.1 we have $\mathcal{R} \in \mathfrak{R}$. In other words, $\mathcal{R}$ is an algebraic curve defined over an algebraic number field. The “if” part of of Belyi’s Theorem is proved. □

Remark 4.2. It is interesting to calculate the ramification data and equations of the Belyi curves $\mathcal{R}$ in terms of the orders $\Lambda \subseteq O_K$ and number fields $K$ obtained in Theorem 1.3.

Data availability Data sharing is not applicable to this article as no new dataset were generated during the current study.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

References

[1] Belyi, G.V.: Galois extensions of a maximal cyclotomic field. Izv. Akad. Nauk SSSR Ser. Mat. 43, 267–276 (1979)
[2] Eisenbud, D., Harris, J.: The Geometry of Schemes. GTM, vol. 197. Springer, Berlin (1999)
[3] Grothendieck, A.: The cohomology theory of abstract algebraic varieties. In: Proceedings of the ICM, August 14–25, pp. 103–118. Cambridge University Press, Edinburgh 1960 (1958)
[4] Humphreys, J.E.: Arithmetic Groups, Springer Lecture Notes, vol. 789. Springer, Berlin (1980)
[5] Maclachlan, C., Reid, A.W.: The Arithmetic of Hyperbolic 3-Manifolds, GTM, vol. 219. Springer, Berlin (2003)
[6] Manin, Y.I.: The notion of dimension in geometry and algebra. Bull. Am. Math. Soc. 43, 139–161 (2006)
[7] Nikolaev, I.: Noncommutative Geometry. De Gruyter Studies in Math, Second Edition, vol. 66. Berlin (2022)

[8] Nikolaev, I.: Remark on arithmetic topology. arXiv:1706.06398

[9] Nikolaev, I.: Remark on Galois cohomology. arXiv:1712.07516

[10] Stafford, J.T., van den Bergh, M.: Noncommutative curves and noncommutative surfaces. Bull. Am. Math. Soc. 38, 171–216 (2001)

[11] Weil, A.: Numbers of solutions of equations in finite fields. Bull. Am. Math. Soc. 55, 497–508 (1949)

Igor V. Nikolaev
Department of Mathematics and Computer Science
St. John’s University
8000 Utopia Parkway
New York NY11439
USA
e-mail: igor.v.nikolaev@gmail.com

Accepted: February 28, 2022.