Math. J. Okayama Univ. **46** (2004), 105–113

NONCRITICAL BELYI MAPS

Shinichi MOCHIZUKI

Abstract. In the present paper, we present a slightly *strengthened version* of a well-known *theorem of Belyi* on the existence of *"Belyi maps"*. Roughly speaking, this strengthened version asserts that there exist Belyi maps which are *unramified at* [cf. Theorem 2.5] — *or even near* [cf. Corollary 3.2] — *a prescribed finite set of points.*

1. Introduction

Write $\mathbb{C}$ for the *complex number field*; $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ for the subfield of *algebraic numbers.* Let X be a *smooth, proper, connected algebraic curve* over $\overline{\mathbb{Q}}$. If F is a field, then we shall denote by $\mathbb{P}^1_F$ the *projective line* over F.

Definition 1. We shall refer to a dominant morphism [of $\overline{\mathbb{Q}}$-schemes]

$$\phi : X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

as a *Belyi map* if ϕ is unramified over the open subscheme $U_P \subseteq \mathbb{P}^1_{\overline{\mathbb{Q}}}$ given by the complement of the points "0", "1", and "∞" of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$; in this case, we shall refer to $U_X \stackrel{\text{def}}{=} \phi^{-1}(U_P) \subseteq X$ as a *Belyi open* of X.

In [1], it is shown that X always admits *at least one Belyi open.* From this point of view, the *main result* (Theorem 2.5) of the present paper has as an immediate formal consequence (pointed out to the author by A. Tamagawa) the following interesting [and representative] result:

Corollary 1.1 (Belyi Opens as a Zariski Base)**.** *If $V_X \subseteq X$ is any open subscheme of X containing a closed point $x \in X$, then there exists a Belyi open $U_X \subseteq V_X \subseteq X$ such that $x \in U_X$. In particular, the Belyi opens of X form a base for the Zariski topology of X.*

Acknowledgment. The author wishes to thank *A. Tamagawa* for helpful discussions during November 1999 concerning the proof of Theorem 2.5 given here.

2. The Main Result

We begin with some elementary lemmas:

Mathematics Subject Classification. Primary 14H25; Secondary 14H30.
Key words and phrases. Belyi map, Zariski base.

Lemma 2.1 (Separating Properties of Belyi Maps). *Let $C \in \mathbb{R}$ be such that $C \geq 2$; let*

$$S \subseteq \mathbb{P}^1(\mathbb{Q})$$

be a finite set of rational points such that:

(i) $0, 1, \infty \in S$;
(ii) *there exists an* $r \in S$ *such that* $0 < r < 1$;
(iii) *every* $\alpha \in S$ *such that* $\alpha \neq 0, r, 1, \infty$ *satisfies* $\alpha > 1$.

Suppose that $\beta \in \mathbb{Q} \backslash S$ *satisfies the following condition:*

(iv) $\beta/\alpha \geq C$, *for all* $\alpha \in S \backslash \{0, \infty\}$.

Write $r = m/(m+n)$, *where* $m, n \geq 1$ *are integers. Then the function*

$$f(x) \stackrel{\text{def}}{=} x^m \cdot (x-1)^n$$

satisfies the following properties:

(a) $f(\{0, r, 1, \infty\}) \subseteq \{0, f(r), \infty\}$;
(b) $f'(x) = 0$ *(where* $x \in \mathbb{C}$*) implies* $x \in \{0, r, 1, \infty\} \subseteq S$;
(c) $f(\beta) \notin f(S)$;
(d) $(f(\beta)+f_0)/(f(\alpha)+f_0) \geq C$ *for all* $\alpha \in S \backslash \{\infty\}$ *such that* $f(\alpha)+f_0 \neq 0$.

Here, we write $f_0 \stackrel{\text{def}}{=} -\min_\alpha \{f(\alpha)\}$, *where* α *ranges over the elements of* $S \backslash \{\infty\}$.

Proof. Property (a) is immediate from the definitions. Property (b) follows immediately from the fact that:

$$f'(x) = x^{m-1} \cdot (x-1)^{n-1} \cdot \{(m+n)x - m\}$$

This computation also implies that for real $x > 1$, we have $f'(x) > 0$, hence that $f(x)$ is *monotone increasing*, for real $x > 1$. In particular, since, by condition (iv), $\beta \geq C \cdot \alpha \geq 2 \cdot \alpha > \alpha$, for all $\alpha \in S \backslash \{0, \infty\}$, we conclude that $f(\beta) > f(\alpha)$, for all $\alpha \in S \backslash \{\infty\}$ such that $\alpha > 1$.

Next, observe that since $1 \in S \backslash \{0, \infty\}$, condition (iv) implies that $\beta \geq C \geq 2$, so $f(\beta) > 1$. Since $|f(x)| \leq 1$ for $x \in [0, 1]$, we thus conclude that $f(\beta) \notin f(S)$, i.e., that property (c) is satisfied.

Next, let us observe the following property:

(e) If $\alpha \in S \backslash \{\infty\}$ satisfies $\alpha > 1$, then $(\beta - 1)/(\alpha - 1) \geq \beta/\alpha \geq 1$; $f(\beta)/f(\alpha) \geq (\beta/\alpha)^2 \geq \beta/\alpha$.

[Indeed, as observed above, $\beta \geq \alpha$; thus, $f(\beta)/f(\alpha) = (\beta/\alpha)^m \cdot \{(\beta-1)/(\alpha-1)\}^n \geq (\beta/\alpha)^{m+n} \geq (\beta/\alpha)^2 \geq \beta/\alpha$.] Now we proceed to verify property (d) as follows:

Suppose that n is *even*. Then $f(\alpha) \geq 0$, for all $\alpha \in S \backslash \{\infty\}$, so $f(0) = 0$ implies that $f_0 = 0$. Thus, if $(S\backslash\{\infty\}) \ni \alpha > 1$, then, by condition (iv) and property (e), we have: $f(\beta)/f(\alpha) \geq \beta/\alpha \geq C$, as desired. Since $f(0) = f(1) = 0$, to complete the proof of property (d) for n even, it suffices to observe that $0 < f(r) \leq 1$, so $f(\beta)/f(r) \geq f(\beta) = \beta^m \cdot (\beta - 1)^n \geq \beta \geq C$ [since $\beta \geq C \geq 2$, as observed above].

Now suppose that n is *odd*. Then $f(x) \leq 0$ for $x \in [0, 1]$, so [since $f'(x) = 0$ for $x \in (0, 1) \iff x = r$] we conclude that:

$$f_0 = |f(r)| = \{m/(m + n)\}^m \cdot \{n/(m + n)\}^n$$

Note, moreover, that this expression for f_0 implies that $0 < f_0 \leq \frac{1}{4}$. [Indeed, this is immediate in the following three cases: $m, n \geq 2$; $m = n = 1$; one of m, n is $= 1$ and the other is ≥ 3. When one of m, n is $= 1$ and the other is $= 2$, it follows from the fact that $(\frac{1}{3}) \cdot (\frac{2}{3})^2 \leq \frac{1}{4}$.] Then if $\alpha > 1$, then *either* $f(\alpha) \geq f_0$, in which case

$$(f(\beta) + f_0)/(f(\alpha) + f_0) \geq f(\beta)/\{2 \cdot f(\alpha)\} \geq \frac{1}{2} \cdot (\beta/\alpha)^2 \geq (\beta/\alpha) \geq C$$

[by property (e)] *or* $f(\alpha) \leq f_0$, in which case

$$(f(\beta) + f_0)/(f(\alpha) + f_0) \geq f(\beta)/\{2 \cdot f_0\} \geq 2 \cdot f(\beta) = 2\beta^m(\beta - 1)^n \geq \beta \geq C$$

[since $0 < f_0 \leq \frac{1}{4}$, $\beta \geq C \geq 2$]. On the other hand, if $\alpha \in \{0, 1\}$, then

$$(f(\beta) + f_0)/(f(\alpha) + f_0) = (f(\beta) + f_0)/f_0 \geq f(\beta) \geq \beta^m \cdot (\beta - 1)^n \geq \beta \geq C$$

[since $\beta \geq C \geq 2$, as observed above]. This completes the proof of property (d). $\square$

Lemma 2.2 (Belyi Maps Noncritical at Prescribed Rational Points)**.** *Let*

$$S \subseteq \mathbb{P}^1(\mathbb{Q})$$

be a finite set of rational points such that:

(i) $0, \infty \in S$*;*
(ii) $\alpha \in S\backslash\{0, \infty\}$ *implies* $\alpha > 0$*.*

Suppose that $\beta \in \mathbb{Q}\backslash S$ *satisfies the following condition:*

(iii) $\beta/\alpha \geq 2$*, for all* $\alpha \in S\backslash\{0, \infty\}$*.*

Then there exists a nonconstant polynomial $f(x) \in \mathbb{Q}[x]$ *which defines a morphism*

$$\phi : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$$

such that: (a) $\phi(S) \subseteq \{0, 1, \infty\}$*; (b)* $\phi(\beta) \notin \{0, 1, \infty\}$*; (c)* ϕ *is unramified over* $\mathbb{P}^1_{\mathbb{Q}}\backslash\{0, 1, \infty\}$*.*

Proof. Indeed, we induct on the *cardinality* $|S|$ of S and apply Lemma 2.1 [with, say, $C = 2$] to the set $\lambda \cdot S \subseteq \mathbb{P}^1_{\mathbb{Q}}$, for some appropriate *positive rational number* λ. Then, so long as $|S| \geq 4$, the polynomial "$f(x) + f_0$" of Lemma 2.1 determines a morphism $\mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$, unramified away from the image of S, that maps β, S to some β', S' that satisfy conditions (i), (ii), (iii) of the present Lemma 2.2, but for which the cardinalities of S', S satisfy $|S'| < |S|$. Thus, by applying the induction hypothesis and composing the resulting morphisms $\mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$, we conclude the existence of an "f", "ϕ" as in the statement of the present Lemma 2.2. $\square$

Lemma 2.3 (Separation of Collections of Points)**.** *Let*

$$S \subseteq \mathbb{P}^1(\mathbb{C})$$

be a finite set of complex points. Then for any real $C > 0$ and $\beta \in \mathbb{C}\backslash S \subseteq \mathbb{P}^1(\mathbb{C})\backslash S$, there exists a $\lambda \in \mathbb{C}$ such that the rational function

$$f(x) = 1/(x - \lambda)$$

satisfies $f(\beta) \neq 0, \infty$; $f(\alpha) \neq \infty$; and $|f(\beta)| \geq C \cdot |f(\alpha)|$, for all $\alpha \in S$. Moreover, if $\beta \in \mathbb{Q}$, then one may take $\lambda \in \mathbb{Q}$.

Proof. Indeed, it suffices to take λ such $|\lambda - \beta|$ is *sufficiently small.* $\square$

Lemma 2.4 (Reduction to the Rational Case)**.** *Write $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ for the subset of algebraic numbers. Let*

$$S \subseteq \mathbb{P}^1(\overline{\mathbb{Q}}) \subseteq \mathbb{P}^1(\mathbb{C})$$

be a finite set of $\overline{\mathbb{Q}}$-rational points. Suppose that $\beta \in \overline{\mathbb{Q}}\backslash S$. Then there exists a nonconstant rational function $f(x) \in \overline{\mathbb{Q}}(x)$ which defines a morphism

$$\phi : \mathbb{P}^1_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

such that, for some $S_\phi \subseteq \mathbb{P}^1(\mathbb{Q})$, we have: (a) $\phi(S) \subseteq S_\phi$; (b) $\phi(\beta) \in \mathbb{P}^1(\mathbb{Q})\backslash S_\phi$; (c) ϕ is unramified over $\mathbb{P}^1_{\overline{\mathbb{Q}}}\backslash S_\phi$. Moreover, if S, β are defined over a number field F, then ϕ may be taken to be defined over F.

Proof. First of all, we observe that by applying the automorphism $x \mapsto x - \beta$, we may assume that $\beta \in \mathbb{P}^1(\mathbb{Q})$. Moreover, under the hypothesis that $\beta \in \mathbb{P}^1(\mathbb{Q})$, we shall construct a $f(x)$ satisfying the required conditions such that $f(x) \in \mathbb{Q}(x)$. Also, we may replace S by the union of all $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates of S and assume, without loss of generality, that S is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-*stable.*

If F is a *finite extension* of $\mathbb{Q}$, then let us refer to the number $[F : \mathbb{Q}] - 1$ as the *reduced degree* of F. Write

$$m(S)$$

for the *maximum of the reduced degrees* of the fields of definition of the various points contained in S and

$$d(S)$$

for the *sum of those reduced degrees* of the fields of definition of the various points contained in S which are *equal to* $m(S)$. Thus, $d(S) = 0$ if and only if $m(S) = 0$ if and only if $S \subseteq \mathbb{P}^1(\mathbb{Q})$.

Now we perform a *"nested induction"* on $m(S)$, $d(S)$: That is to say, we induct on $m(S)$, and, for each fixed value of $m(S)$, we induct on $d(S)$. If $m(S), d(S) \neq 0$, then let $\alpha_0 \in S \backslash \mathbb{P}^1(\mathbb{Q})$ be such that $d_0 \stackrel{\text{def}}{=} [\mathbb{Q}(\alpha_0) : \mathbb{Q}]$ is equal to $m(S) + 1$. Then by applying an automorphism (with rational coefficients!) as in Lemma 2.3 and then multiplying by some positive rational number, we may assume that $|\alpha| \leq 1$, for all $\alpha \in S \backslash \{\infty\}$, while $|\beta| \geq C$, for some *sufficiently large* C, where "sufficiently large" is relative to d_0. Let $f_0(x) \in \mathbb{Q}[x]$ be the *monic minimal polynomial* for α_0 over $\mathbb{Q}$. Then one verifies immediately that all of the coefficients of $f_0(x)$ have absolute value $\leq d_0^{d_0}$. In particular, it follows that the value of f_0 at every $\alpha \in S \backslash \{\infty\}$, as well as at every element of the set S_0 of roots of the derivative $f_0'(x)$ has absolute value bounded by some *fixed expression in* d_0. Thus, for a suitable choice of C, it follows that $f_0(\beta) \notin S' \stackrel{\text{def}}{=} f_0(S) \bigcup f_0(S_0)$. Moreover, since $f_0(\alpha_0) = 0$; $[\mathbb{Q}(\alpha') : \mathbb{Q}] < d_0$ for every $\alpha' \in f_0(S_0)$ [since $f_0(x), f_0'(x) \in \mathbb{Q}[x]$; $f_0'(x)$ has degree $\leq d_0 - 1$], it follows that S' is $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable and satisfies the property that *either*

$$m(S') < m(S)$$

or

$$m(S') = m(S); \quad d(S') < d(S)$$

— thus *completing the induction step.* In particular, replacing S by S', β by $f_0(\beta)$, applying the induction hypothesis, and composing the resulting morphisms yields a morphism ϕ as in the statement of Lemma 2.4. □

Theorem 2.5 (Belyi Maps Noncritical at Prescribed Points)**.** *Let X be a smooth, proper, connected curve over $\overline{\mathbb{Q}}$ and*

$$S, T \subseteq X(\overline{\mathbb{Q}})$$

finite sets of $\overline{\mathbb{Q}}$-rational points such that $S \bigcap T = \emptyset$. Then there exists a morphism

$$\phi : X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

such that: (a) ϕ is unramified over $\mathbb{P}^1_{\overline{\mathbb{Q}}} \backslash \{0, 1, \infty\}$; (b) $\phi(S) \subseteq \{0, 1, \infty\}$; (c) we have $\phi(T) \bigcap \{0, 1, \infty\} = \emptyset$. Moreover, if X, S, and T are defined over a number field F, then ϕ may be taken to be defined over F.

Proof. Since $X(\overline{\mathbb{Q}})$ is *infinite*, we may always adjoin to T *extra points* of $X(\overline{\mathbb{Q}})$ that do not lie in S; in particular, we may *assume*, without loss of generality, that T has *cardinality* $\geq 2g_X + 1$, where g_X is the genus of X. Write

$$D \stackrel{\text{def}}{=} \sum_{t \in T} [t]$$

for the *effective divisor* on X obtained by taking the formal sum of the points in T, each with *multiplicity one*; denote the associated *line bundle* $\mathcal{O}_X(D)$ by $\mathcal{L}$ and the *canonical bundle* of X by ω_X. Also, we shall write $s_0 \in \Gamma(X, \mathcal{L})$ for the section [uniquely determined up to a $\overline{\mathbb{Q}}^{\times}$-multiple] whose zero divisor is D. Thus, the degree $\deg(\mathcal{L})$ of $\mathcal{L}$ is $\geq 2g_X + 1 \geq 1$. In particular, if $x \in X(\overline{\mathbb{Q}})$, then

$$\deg(\omega_X \otimes \mathcal{L}^{-1}(x)) \leq (2g_X - 2) - (2g_X + 1) + 1 = -2$$

so $\Gamma(X, \omega_X \otimes \mathcal{L}^{-1}(x)) = 0$. Since, by Serre duality, $\Gamma(X, \omega_X \otimes \mathcal{L}^{-1}(x))$ is dual to $H^1(X, \mathcal{L}(-x))$, we thus conclude that $H^1(X, \mathcal{L}(-x)) = 0$. Now if we consider the *long exact cohomology sequence* associated to the exact sequence of coherent sheaves on X

$$0 \to \mathcal{L}(-x) \to \mathcal{L} \to \mathcal{L} \otimes k(x) \to 0$$

[where $k(x)$ is the residue field of X at x] we obtain an exact sequence

$$\ldots \to \Gamma(X, \mathcal{L}) \to \mathcal{L} \otimes k(x) \to H^1(X, \mathcal{L}(-x)) \to \ldots$$

— i.e., we have a *surjection* $\Gamma(X, \mathcal{L}) \twoheadrightarrow \mathcal{L} \otimes k(x)$. Since $\overline{\mathbb{Q}}$ is *infinite*, it thus follows that there exists an $s_1 \in \Gamma(X, \mathcal{L})$ such that $s_1(t) \neq 0$ for all $t \in T$. Thus, the *linear series* determined by the sections s_0, s_1 of $\mathcal{L}$ has *no basepoints*, hence determines a *finite morphism*

$$\psi : X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

such that the pull-back by ψ of the unique [up to isomorphism] line bundle of degree 1 on $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ is isomorphic to $\mathcal{L}$; ψ maps every $t \in T$ to the point "0" of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$. Moreover, since every point of the support of D has *multiplicity one* in D, ψ is *unramified* over the point "0" of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$; since no point of S lies in the support of D, this point "0" of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ does not lie in the set $\psi(S)$.

Thus, in summary, by *replacing* X by $\mathbb{P}^1_{\overline{\mathbb{Q}}}$, T by the point "0" of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$, and S by the union of $\psi(S)$ and the points of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ over which ψ *ramifies*, we conclude that we may reduce to the case $X = \mathbb{P}^1_{\overline{\mathbb{Q}}}$, $T = \{\beta\}$, for some $\beta \in \mathbb{P}^1(\overline{\mathbb{Q}}) \backslash \{\infty\}$. Next, by applying Lemma 2.4, one reduces to the case $X = \mathbb{P}^1_{\overline{\mathbb{Q}}}$, $S \subseteq \mathbb{P}^1(\mathbb{Q})$, $T = \{\beta\}$, for some $\beta \in \mathbb{P}^1(\mathbb{Q}) \backslash \{\infty\}$. Finally, by applying an automorphism as in Lemma 2.3 [for, say, $C = 4$], followed by a suitable automorphism of the form $x \mapsto \nu \cdot x + \mu$, where $\nu \in \{\pm 1\}$ and $\mu \in \mathbb{Q}$, gives rise to a situation in which the hypotheses of Lemma 2.2 are valid. Thus, Theorem 2.5 follows from Lemma 2.2. $\square$

3. Some Generalizations

Corollary 3.1 (Belyi Maps Noncritical at Arbitrary Sets of Prescribed Cardinality)**.** *Let $n \geq 1$ be an integer; X a smooth, proper, connected curve over $\overline{\mathbb{Q}}$ and*

$$S \subseteq X(\overline{\mathbb{Q}})$$

a finite set of $\overline{\mathbb{Q}}$-rational points. Then there exists a finite collection of morphisms

$$\phi_1, \ldots, \phi_N : X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

such that: (a) ϕ_i is unramified over $\mathbb{P}^1_{\overline{\mathbb{Q}}} \backslash \{0, 1, \infty\}$, for all $i = 1, \ldots, N$; (b) $\phi_i(S) \subseteq \{0, 1, \infty\}$, for all $i = 1, \ldots, N$; (c) for any subset $T \subseteq X(\overline{\mathbb{Q}})$ of cardinality n for which $S \bigcap T = \emptyset$, there exists an $i \in \{1, \ldots, N\}$ such that $\phi_i(T) \bigcap \{0, 1, \infty\} = \emptyset$.

Proof. Note that we may think of T as a $\overline{\mathbb{Q}}$-valued point of the n-fold product $Y \stackrel{\text{def}}{=} (X \backslash S)^n$ of $(X \backslash S)$ over $\overline{\mathbb{Q}}$. Then observe that for any $\phi : X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ such that: (a) ϕ is unramified over $\mathbb{P}^1_{\overline{\mathbb{Q}}} \backslash \{0, 1, \infty\}$; (b) $\phi(S) \subseteq \{0, 1, \infty\}$, the subset

$$U_\phi \subseteq Y(\overline{\mathbb{Q}})$$

of $y \in Y(\overline{\mathbb{Q}})$ for which $\phi(y) \bigcap \{0, 1, \infty\} = \emptyset$ [where, by abuse of notation, we write $\phi(y)$ for the subset of $\mathbb{P}^1_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}})$ which is the image under ϕ of the subset of $X(\overline{\mathbb{Q}})$ determined by y] is nonempty and *open* [in the Zariski topology]. Moreover, by Theorem 2.5, the U_ϕ *cover* $Y(\overline{\mathbb{Q}})$ [i.e., as ϕ varies over those morphisms satisfying the conditions (a), (b)]. Since Y is *quasi-compact*, we thus conclude that there exist *finitely many* $\phi_1, \ldots, \phi_N$ such that $Y(\overline{\mathbb{Q}})$ is covered by $U_{\phi_1}, \ldots, U_{\phi_N}$, as desired. $\square$

In the following, we shall refer to as a *locally compact field* any completion of a number field at an archimedean or nonarchimedean place.

Corollary 3.2 (Belyi Maps Noncritical Near Arbitrary Points of Prescribed Degree)**.** *Let $c, d \geq 1$ be integers; X a smooth, proper, connected curve over a number field $F \subseteq \overline{\mathbb{Q}}$; V a finite set of* **valuations** *(archimedean or nonarchimedean) of F. If $v \in V$, then we denote by F_v the completion of F at v. Then there exists a finite collection of* **morphisms**

$$\phi_1, \ldots, \phi_N : X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

and, for each $v \in V$, a **locally compact field** L_v *and a* **compact set**

$$H_v \subseteq (\mathbb{P}^1 \backslash \{0, 1, \infty\})(L_v) \subseteq \mathbb{P}^1(L_v)$$

satisfying the following properties:

(i) $F \subseteq F_v \subseteq L_v$ *[i.e., L_v is a topological field extension of F_v];*
(ii) L_v *contains all $\mathbb{Q}$-conjugates of all extensions of F of degree $\leq d$;*
(iii) *every ϕ_i (where $i \in \{1, \ldots, N\}$) is defined over every L_v (where $v \in V$);*
(iv) ϕ_i *is unramified over $\mathbb{P}^1_{\overline{\mathbb{Q}}} \backslash \{0, 1, \infty\}$, for all $i = 1, \ldots, N$;*
(v) *for any subset $T \subseteq X(\overline{\mathbb{Q}})$ of cardinality $\leq c$ consisting of points $x \in T$ whose field of definition is of degree $\leq d$ over F, there exists an $i \in \{1, \ldots, N\}$ such that $\phi_i(x^\sigma) \in H_v$, for all $x \in T$, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$, $v \in V$.*

Proof. As in the proof of Corollary 3.1, write $Y \stackrel{\mathrm{def}}{=} X^n$ for the n-fold product X over F, where we set $n \stackrel{\mathrm{def}}{=} c \cdot d$. Thus, for any $T \subseteq X(\overline{\mathbb{Q}})$ as in the statement of Corollary 3.2, (v), the *conjugates over* F of the various $x \in T$ [in any order, with possible repetition] form a point $\in Y(\overline{\mathbb{Q}})$. Let L_v be a *locally compact field* containing F_v, as well as all $\mathbb{Q}$-conjugates of all extensions of F of degree $\leq d$. Then observe that for any $\phi : X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ which is defined over all of the L_v [as v ranges over the elements of V] and unramified over $\mathbb{P}^1_{\overline{\mathbb{Q}}} \backslash \{0, 1, \infty\}$, the subset

$$U_\phi \subseteq Y(L_V) \stackrel{\mathrm{def}}{=} \prod_{v \in V} Y(L_v)$$

of $y \in Y(L_V)$ for which $\phi(y) \bigcap \{0, 1, \infty\} = \emptyset$ [by abuse of notation, as in the proof of Corollary 3.1] is nonempty and *open* relative to the product topology of the *Zariski topologies on the* $Y(L_v)$, hence *a fortiori*, relative to the product topology of the topologies on the $Y(L_v)$ determined by the L_v. Moreover, by arguing as in the proof of Corollary 3.1 using Theorem 2.5 and the *Zariski topology*, we may assume that the L_v are *sufficiently large* that [in fact, finitely many] such U_ϕ *cover* $Y(L_V)$. Now since each U_ϕ is *locally compact* and contains a *countable dense subset*, it follows that each U_ϕ admits an *exhaustive chain of open subsets*

$$V_{\phi,1} \subseteq V_{\phi,2} \subseteq \ldots \subseteq U_\phi$$

[i.e., $\bigcup_j V_{\phi,j} = U_\phi$] such that the closure $\overline{V}_{\phi,j}$ in U_ϕ of each $V_{\phi,j}$ is *compact*. On the other hand, since Y is *proper*, it follows that $Y(L_V)$ is *compact*. We thus conclude that there exist *finitely many* $\phi_1, \ldots, \phi_N$ such that $Y(L_V)$ is *covered* by $V_{\phi_1,j_1}; \ldots; V_{\phi_N,j_N}$, where [by abuse of notation, as in the proof of

Corollary 3.1, we write]

$$\phi_i(V_{\phi_i,j_i}) \subseteq \phi_i(\overline{V}_{\phi_i,j_i}) \subseteq \phi_i(U_{\phi_i}) \subseteq \prod_{v \in V} (\mathbb{P}^1 \backslash \{0,1,\infty\})(L_v)$$

for $i = 1, \ldots, N$. Thus, we may take H_v to be the *image* in the factor $(\mathbb{P}^1 \backslash \{0,1,\infty\})(L_v)$ of the *union* of the compact subsets $\phi_i(\overline{V}_{\phi_i,j_i})$ of the product $\prod_{v \in V} (\mathbb{P}^1 \backslash \{0,1,\infty\})(L_v)$. $\square$

References

[1] G. V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43:2** (1979), pp. 269–276; English transl. in Math. USSR-Izv. **14** (1980), pp. 247-256.

Shinichi Mochizuki
Research Institute for Mathematical Sciences
Kyoto University
Kyoto, 606-8502 Japan
e-mail address: motizuki@kurims.kyoto-u.ac.jp

(*Received May 21, 2004*)