# GEOMETRIC PROPERTIES OF CURVES DEFINED OVER NUMBER FIELDS

by F. Bogomolov and D. Husemöller

This article has its origins in the 6 March 1991 Haverford College Philips Lecture of F. Bogomolov on the subject of the relation between the geometry and arithmetic of algebraic curves. Among the curves defined over the complex numbers certain ones can be defined over $\overline{\mathbf{Q}}$, the field of all algebraic numbers. Since only a finite number of coefficients are involved, such a curve can be defined over a finite extension $k$ of the rational number field $\mathbf{Q}$, that is, $k$ a number field. The related geometric properties are described in terms of ramification properties of maps to the projective line $\mathbf{P}^1$, and a given map to the projective line can be modified by composing with a morphism from $\mathbf{P}^1$ to $\mathbf{P}^1$.

The basic assertion, which goes back to Belyi, is that a curve has a number field as field of definition if and only if it is a ramified covering of $\mathbf{P}^1$ with all ramification over the three points $\{0, 1, \infty\}$, or equivalently any set of three points for any triple of distinct points in $\mathbf{P}^1$ can be mapped by a projective transformation onto the triple $\{0, 1, \infty\}$. The aim of this article is to study the various techniques going into the proof of this characterization of curves defined over a number field by this geometric property of a ramified covering. The following is a precise statement of the main assertion relating arithmetic and geometry of algebraic curves.

**Main Theorem.** *Let $X$ be a smooth, complete algebraic curve over the complex numbers. Then $X$ can be defined over an algebraic number field if and only if there exists a ramified covering $\pi : X \to \mathbf{P}^1$ such that all ramification of $\pi$ is over $\{0, 1, \infty\}$.*

The proof of this theorem will be given in the next several sections. The direct implication is elementary and deals with reducing the number of ramification points. This reduction divides into two parts, namely the part which is special to the rational numbers and the part having to do with lowering the degree of field extensions. This second part will be discussed on a broader level than just the proof of the main theorem for it leads to other results. In section 3 and 4 we give two proofs of the converse. The first is a Galois group argument where the Galois group of the function field of the curve, the absolute Galois group $\mathrm{Gal}(\overline{\mathbf{Q}/\mathbf{Q}})$, and the fundamental group of the Riemann sphere minus the ramification points all play a basic role. This proof was shown to us by Joseph Oesterle at the Seminar Bourbaki on 19.VI.93, and he gave further details in a letter a week later. Then we present a second proof of the converse assertion based on scheme theory methods from D. Mumford, *Introduction to Algebraic Geometry*, Springer Lecture Notes 1358.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

In part 2 of the paper we discuss a number of ideas and problems which came up about the time that Belyi's original theorem was proved, in 1978. In the meantime some of these ideas where developed much further by several people, see the references at the end. We would like to mention in particular the work of Ihara and Drinfel'd on $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Grothendieck and Voevodsky and Shabat on drawings on curves, Deligne on the fundamental group of the projective line minus three points, R. Donagi on Hurwitz schemes, and N. Elkies on the connection between Mordell's conjecture and the ABC conjecture via the theorem on three points. There is also the general influence of this theory on the work of John Thompson connected with simple quotients of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Many recent developments in this direction are summarized in the LMS Lecture Notes Volume 200 and 242 edited by L. Schneps. Our goal is to give an exposition of the basic constructions going into the proof of the main theorem and related initial results and constructions.

## Contents

# Part I

## § 1. The construction of Belyi over rational numbers

*(1.1) Notation.* Let $f : X \to Y$ be a nonconstant algebraic map between two smooth algebraic curves or an analytic map between two Riemann surfaces. The ramification index $e(x)$ of $f$ at $x \in X$ is the natural number such that locally $y = f(x)$ is of the form $w = z^{e(x)}$ where $z$ is a local parameter at $x$ with $z(x) = 0$ and $w$ is a local parameter at $f(x)$ with $w(f(x)) = 0$.

*(1.2) Definition.* With the previous notations a point $x \in X$ is a singular point of $f$ provided $e(x) > 1$, and the value $f(x)$ at a branch point $x \in X$ is a ramification value of $f$. The singular locus $\mathrm{sing}(f)$ of $f$ is the set of all singular points of $f$ in $X$. The ramification locus $\mathrm{ram}(f)$ of $f$ is the set of all ramification values of $f$ in $Y$.

Observe that the points $x$ with $e(x) > 1$ are isolated in characteristic zero and in local coordinates are the points $x$ where the derivative $f'(x) = 0$. These points are finite in number on complete curves and compact Riemann surfaces, so that sing $(f)$ and $f(\mathrm{sing}(f)) = \mathrm{ram}(f)$ are finite sets. Nonconstant $f$ are surjective on points over an algebraic closed field. Like $C$ in the case of compact Riemann surfaces, and they are also called ramified coverings.

*(1.3) Remark.* We are concerned with the ramification of $\pi : X \to P^1$. That is, the set $\mathrm{ram}(\pi)$, and we simplify this set by considering maps $f : P^1 \to P^1$ and forming $f\pi : X \to P^1$. For this we use the relation $\mathrm{ram}(f\pi) = f(\mathrm{ram}(\pi)) \cup \mathrm{ram}(f)$ which follows from the chain rule $(f\pi)' = (f'\pi), \pi'$ when these morphisms are expressed in local coordinates. In particular we will reduce the number of points in $\mathrm{ram}(\pi)$ by replacing $\pi$ with $f\pi$.

Over the rational numbers we are able to do this as follows by a simple construction using polynomial maps $f : P^1 \to P^1$ where $f(\infty) = \infty$. When the degree of $f$ is strictly bigger than 1, we have

*(1.4) Proposition.* For each pair of nonzero natural numbers $m$ and $n$ there exists a polynomial $f(t) \in \mathbf{Q}[t]$ with $f : \mathbf{P}^1 \to \mathbf{P}^1$ having the property that $\mathrm{sing}(f) \subset \{0, \frac{m}{m+n}, 1, \infty\}$ and

$$\mathrm{ram}(f) = f(\{0, \frac{m}{m+n}, 1, \infty\}) = \{0, 1, \infty\}.$$

*Proof.* We have an explicit construction of $f$ as

$$f_{m,n}(t) = \frac{(m+n)^{m+n}}{m^m n^n} t^m (1-t)^n.$$

Observe that the formula for the derivative

$$f'_{m,n}(t) = \frac{(m+n)^{m+n}}{m^m n^n} t^{m-1} (1-t)^{n-1} \{m(1-t) - nt\}$$

shows that the singular $\mathrm{sing}(f) \subset \{0, \frac{m}{m+n}, 1, \infty\}$. Since $f(0) = f(1) = 0$ and $f(\frac{m}{m+n}) = 1$, it follows also that the branch locus $\mathrm{ram}(f) = \{0, 1, \infty\}$. This proves the proposition.

This allows us to prove the first step in the direct implication of the main theorem stated in the introduction.

*(1.5) Proposition.* Let $X$ be a complete smooth algebraic curve defined over the rational numbers $\mathbf{Q}$ with ramified covering $\pi' : X \to \mathbf{P}^1$ with $\mathrm{ram}(\pi') \subset \mathbf{P}^1(\mathbf{Q})$. Then there exists a ramified covering $\pi : X \to \mathbf{P}^1$ defined over $\mathbf{Q}$ such that $\mathrm{ram}(\pi) \subset \{0, 1, \infty\}$.

*Proof.* Consider $y_0, y_1, y_2, y_3 \in \mathbf{P}^1(\mathbf{Q})$ with all $y_i \in \mathrm{ram}(\pi')$ if $\sharp\mathrm{ram}(\pi') > 3$, and $\mathrm{ram}(\pi') \subset \{y_1, y_2, y_3\}$ if $\sharp\mathrm{ram}(\pi') \leq 3$. There exists a fractional linear automorphism $g(z) = \frac{az+b}{cz+d}$ of $\mathbf{P}^I(\mathbf{Q})$ with $g(y_1) = 0, g(y_2) = 1, g(y_3) = \infty$, and $g(y_0) = \frac{m}{n+m}$. Now composing $\pi'$ with this automorphism $g$ and the polynomial map $f$ of the previous proposition (1.4) we obtain a ramified covering $fg\pi' : X \to \mathbf{P}^1$ over $\mathbf{Q}$ with $\sharp\mathrm{ram}(fg\pi') < \sharp\mathrm{ram}(\pi')$ if $3 < \sharp\mathrm{ram}(\pi)$ and $\mathrm{ram}(fg\pi') \subset \{0, 1, \infty\}$ otherwise. Now continue inductively to reduce the ramification into a subset of $\{0, 1, \infty\}$. This proves the proposition.

Observe that the construction in the previous proposition really depends on the rational number field $\mathbf{Q}$ since an element of the field in question is written in the form $\frac{m}{n+m}$ and the natural numbers $m$ and $n$, in turn, are used to construct the related polynomial mapping. This is the part of the argument where the number of points in the ramification locus is decreased to three.

## § 2. The construction of Belyi for field extensions

In this section $k$ denotes an arbitrary field, and we choose an algebraic closure $\overline{k}$ of $k$. For $\alpha \in \overline{k}$ we wish to map $\alpha$ into $k$ under a polynomial map with a control on the branch locus. For a purely inseparable element this is very easy.

*(2.1) Proposition.* Let $h(t) \in k[t]$ be a purely inseparable polynomial for $k$ of the characteristic $p > 0$ with roots $R$ in $\overline{k}$. Then for each $\alpha \in k$ there exists a polynomial map $f : \mathbf{P}^1 \to \mathbf{P}^1$ over $k$ such that $f(R \cup \{a\}) = \{0\}$ and $\mathrm{ram}(f) = \{0, \infty\}$.

*Proof.* Let $f(t) = (t - \alpha)h(t)$ so that $f(R \cup \{\alpha\}) = \{0\}$. Observing that $f'(t) = h(t)$ since $h'(t) = 0$, we see that $\mathrm{ram}(f) = \{f(R), \infty\} = \{0, \infty\}$. Hence the roots of $f$ and $f'$ are all mapped to 0: This proves the proposition.

*(2.2) Corollary.* If $\pi : X \to \mathbf{P}^1$ is a ramified covering over $k$ of characteristic $p > 0$ with branch locus consisting of some of the roots of a purely inseparable polynomial $h$, any $\alpha \in k$, and $\infty$, then $f\pi : X \to \mathbf{P}^1$ has branch locus $\{0, \infty\}$ where $f$ is the polynomial map $f : \mathbf{P}^1 \to \mathbf{P}^1$ as in (2.1).

In order to map other roots of polynomials to zero with control of branch locus, we need the following measure of the algebraic degree of sets of elements in $\mathbf{P}^1(\overline{k})$.

*(2.3) Definition.* The reduced degree $rd(\alpha)$ of $\alpha \in \mathbf{P}^1(\overline{k})$ over $k$ is defined to be $rd(\alpha) = [k(\alpha) : k] - 1$ for $\alpha \neq \infty$ and $rd(\infty) = 0$. For a subset $S$ of $\mathbf{P}^1(\overline{k})$ the reduced degree $rd(S)$ of $S$ over $k$ is defined to be $rd(S) = \sum_{\alpha \in S} rd(\alpha)$.

Observe that for a subset $S \subset \mathbf{P}^1(\overline{k})$ we have $rd(S) = 0$ if and only if $S \subset \mathbf{P}^1(k) \subset \mathbf{P}^1(\overline{k})$.

*(2.4) Example.* Let $S$ be the set of roots of a polynomial $h(t) \in k[t]$. If $h(t)$ is irreducible, then $[k(\alpha) : k] = \deg(h)$, the degree of $h$, and hence, $rd(\alpha) = \deg(h) - 1$ and

$$rd(S) = (\sharp S), rd(\alpha) = (\sharp S), (\deg(h) - 1) \leq \deg(h)(\deg(h) - 1)$$

with $rd(S) = \deg(h)(\deg(h) - 1)$ for a separable polynomial $h(t)$.

In this general algebraic situation we are interested in polynomial maps $f : \mathbf{P}^1 \to \mathbf{P}^1$ which lower the reduced degree of a set $S \subset \overline{k}$ over $k$ so that by iteration we arrive at a set together with branch locus in $\mathbf{P}^1(k)$. Then we apply this to various situations including the case of $k = \mathbf{Q}$ together with results of the previous section.

*(2.5) Remark.* For a subset $S$ of $\mathbf{P}^1(\overline{k})$ the condition that $S$ is stable under the action of $\mathrm{Gal}(\overline{k}/k)$ is equivalent to the property that if $\alpha \in S$ is the root of an irreducible polynomial $h(t)$, then all roots of $h(t)$ are in $S$. Moreover, if $f : \mathbf{P}^1 \to \mathbf{P}^1$ is a polynomial map over $k$ and $S$ is stable under the action of $\mathrm{Gal}(\overline{k}/k)$, and the inequality $rd(f(S)) \leq rd(S)$ holds.

The following is the key proposition for lowering the reduced degree of a set $S \subset \mathbf{P}^1(\overline{k})$.

*(2.6) Proposition.* Let $S \subset \overline{k}$ be the roots of an irreducible polynomial $f(t) \in k[t]$ where $S$ is not contained in $k$, and let $S' \subset \overline{k}$ denote the roots of $f'(t)$, the derivative of $f(t)$. Then we have $rd(S') < rd(S) - 1$ and $rd(f(S \cup S')) = rd(\{0\} \cup \mathrm{ram}(f)) < rd(S)$.

*Proof.* Let $f_1(t), \ldots, f_r(t)$ denote the irreducible factors of the derivative $f'(t)$. In particular we have the inequality

$$\deg(f_1) + \ldots \deg(f_r) \leq \deg(f) - 1$$

which is an equality when no irreducible factors of $f'(t)$ are repeated. To see that the first inequality holds, we note that

$$d(d-1) - (d-1)(d-2) = 2(d-1) > 1 \quad \text{for} \quad d \geq 2.$$

ow for $\deg(f) = 1$ there is nothing to prove, and for $\deg(f) \geq 2$ we factor $f'$ and then use the following if there is at least two factors $d'd'')(d'd'' - 1) \geq d'(d'-1) + d''(d'-1)$. This gives the proof of the first inequality.

For the second assertion we use $f(S \cup S') = \{0\} \cup f(S') = \{0\} \cup \mathrm{ram}(f)$ and the inequality on the reduced degree under direct image contained as the last assertion in (2.5). This proves the proposition.

Using the previous proposition, we are lead to the following result.

*(2.7) Proposition.* Let $S$ be a finite subset of the algebraic closure $\overline{k}$ of $k$. Then there exists a polynomial map $f : \mathbf{P}^1 \to \mathbf{P}^1$ over $k$ with $f(S) \cup \mathrm{ram}(f) \subset \mathbf{P}^1(k)$.

*Proof.* By enlarging $S$ if necessary, we can assume that $S$ is $\mathrm{Gal}(\overline{k}/k)$ invariant. Using (2.6), we will show that there is a polynomial map $f : \mathbf{P}^1 \to \mathbf{P}^1$ over $k$ with $rd(f(S) \cup \mathrm{ram}(f)) < rd(S)$, and construct the map $f$ of the assertion as a composition of these maps until the result has reduced degree 0, that is, a subset of $\mathbf{P}^1(k)$, the $k$-rational points on the projective line.

Then $S = R \amalg T$ where $R$ is the roots of an irreducible $f(t) \in k[t]$. Then by (2.6) we have the $rd(f(R) \cup \mathrm{ram}(f)) < rd(R)$, and since $rd(f(T)) \leq rd(T)$, we have for the union the desired lowing of the reduced degree for $S$, that is, $rd(F(S) \cup \mathrm{ram}(f)) < rd(S)$. This proves the theorem.

This implies immediately the following theorem.

*(2.8) Theorem.* Let $X$ be a curve over a field $k$ and let $\pi : X \to \mathbf{P}^1$ be a generically surjective morphism over $k$. Then there exists polynomial morphism $f : \mathbf{P}^1 \to \mathbf{P}^1$ over $k$ which that $f\pi : X \to \mathbf{P}^1$ is ramified only over $k$-valued points.

As a first corollary we can complete the proof of the direct implication in the Main Theorem which was announced in the introduction.

*(2.9) Corollary.* Let $X$ be a smooth, complete algebraic curve over the complex numbers which is defined over an algebraic number field. Then there exists a ramified covering $\pi : X \to \mathbf{P}^1$ such that all the ramification of $\pi$ is over $\{0, 1, \infty\}$.

*Proof.* We apply (2.8) to $k = \mathbf{Q}$ so that the ramification is contained in $\mathbf{P}^1(\mathbf{Q})$, and then we apply (1.5) to obtain a ramified covering with the desired properties.

## § 3. Applications to higher dimensional varieties

We can apply the previous theorem (2.8) to an $n$ dimensional variety $X$ defined over an algebraically closed field $k'$ up to birational equivalence by viewing $X$ as a curve over

$$k = k'(t_1, \ldots, t_{n-1}),$$

the rational function field over $k'$ in $n-1$ variables.

*(3.1) Proposition.* Let $X$ be an $(n+1)$-dimensional projective variety over an algebraically closed $k'$. There exists a proper birational morphism $f : Y \to X$ and a finite cover $g : Y \to \mathbf{P}(\mathcal{O}_P \oplus \mathcal{O}_P(N))$ with $P = \mathbf{P}^n$ for some $N > 0$ which is ramified only over a set of images in $\mathbf{P}(\mathcal{O}_P \otimes \mathcal{O}_P(N))$ of sections $s \in \Gamma(\mathbf{P}^n, \mathcal{O}_P(N))$ under the natural inclusion $\mathcal{O}_P(N) \to \mathbf{P}(\mathcal{O}_P(N))$.

*Proof.* We take a finite generic projection $X \to \mathbf{P}^{n+1}$. By choosing an appropriate $P = \mathbf{P}^n$ in $\mathbf{P}^{n+1}$ we obtain $Y \to \mathbf{P}(\mathcal{O}_P \oplus \mathcal{O}_P(1))$ when we blow up inverse images of the generic points of $P = \mathbf{P}^n$. Now the ramification divisor of the new map $g' : Y \to \mathbf{P}(\mathcal{O}_P \oplus \mathcal{O}_P(1))$ is a horizontal divisor in $\mathcal{O}_P(1) \subset \mathbf{P}(\mathcal{O}_P \oplus \mathcal{O}_P(1))$. Now we apply (2.8) to this $\mathbf{P}^1$ over a functor field to obtain a polynomial morphism of degree $N$ defined $f_N : \mathbf{P}(\mathcal{O}_P \oplus \mathcal{O}_P(1)) \to \mathbf{P}(\mathcal{O}_P \oplus \mathcal{O}_P(N))$ where

$$(f_n)^*(\infty - \text{divisor} = d, (\infty) - \text{divisor}).$$

The desired morphism is $f_N g' = g$.

*(3.2) Remark.* This presentation provides a short proof of the weak Hironaka resolution of singularities theorem in characteristic zero, see Bogomolov and Pantev [1996]. This asserts that for any projective variety $X$ and closed subscheme $Z$ there exists a smooth variety $Y$ with a divisor $D$ with strict normal crossings and a proper birational map $f : Y \to X$ with $f(Z) \subset D$.

## § 4. Field of definition of ramified coverings: function field methods

The following with small modifications is a proof of the converse assertion in Belyi's theorem shown to us by Joseph Oesterlé at Seminar Bourbaki, 19.VI.93. This is an argument which takes place in a finite extension of the field of rational functions $\mathbf{C}(T)$ in one variable $T$.

*(4.1) Function field version.* A map of curves $f : X \to \mathbf{P}_1$ over the complex numbers $\mathbf{C}$ with $\mathrm{ram}(f) \subset \mathbf{P}_1(\overline{\mathbf{Q}})$ is equivalent to a finite extension $E$ over $\mathbf{C}(T) = \mathbf{C}(\mathbf{P}_1)$ unramified outside of the finite set $S = \mathrm{ram}(f)$. The proof is defined over the algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$, we have only to show that $E$ is generated by elements algebraic over $\overline{\mathbf{Q}}(T)$. With these algebraic elements over $\overline{\mathbf{Q}}(T)$ which generate $E$, we can find equations for $X$ defined over $\overline{\mathbf{Q}}$, and the function field $\overline{\mathbf{Q}}(T)$, the rational function field in one variable over the field $\mathbf{Q}$. The original function field $\mathbf{C}(T)$ is isomorphic to the composite of $\mathbf{C}$ and $\overline{\mathbf{Q}}(X)$ over $\overline{\mathbf{Q}}$.

*Proof of the function field assertion.* Let $\Omega$ be an algebraic closure of $E$, and consider the subgroup $G$ of $\mathrm{Aut}_{\overline{\mathbf{Q}}(T)}(\Omega)$ consisting of all $\sigma$ such that $\sigma(\mathbf{C}) = \mathbf{C}$. Observe that the fixed field under $G$ is $\mathbf{C}^G = \overline{\mathbf{Q}}$, the field of algebraic numbers.

1) The set of fields $\sigma(E)$ where $\sigma \in G$ is finite. In particular, the subgroup $G_E$ with $\sigma(E) = E$ has finite index in $G$. This follows from the observation that the fields $\sigma(E)$ are function fields of Riemann surfaces unramified over $\mathbf{P}^1 \setminus S$, and there are only a finite number of $n$-fold covers where $n = [E : \mathbf{C}(T)] = [\sigma(E) : \mathbf{C}(T)]$ with ramification at most over $S$.

   There is an algebraic argument: The profinite completion of the free group on $h$ generators where $h+1 = \sharp S$ is the algebraic fundamental group of $\mathbf{P}^1 \setminus S$, and there are only a finite number of subgroups of index $n = [E : \mathbf{C}(T)]$ in the free group on $h$ generators.

   Now we choose a point $a \in \mathbf{P}^1(\overline{\mathbf{Q}}) \setminus S$ with the corresponding valuation $\mathrm{ord}_a$ on $\mathbf{C}(T)$, $x \in X$ with $f(x) = a$, and $\pi_x = e_x$th-root of $z-a$, i.e. a local parameter at $x \in X$. Let $\mathrm{ord}_x$ be a valuation on $E$ at $x \in X$ extending $\mathrm{ord}_a$ on $\mathbf{C}(T)$ to $E$. We form the subgroup $G(x)$ of $\sigma \in G_E$ with $\sigma(\pi_x) = \pi_x$, and so $\mathrm{ord}_x\sigma = \mathrm{ord}_x$ for the valuation of $E$ at $x$.

2) The subgroup $G(x)$ is of finite index in $G$, for the relation $\sigma(\pi_x) = \pi_x$ defines the subgroup $G(x)$ of finite index of $G_E$. Since $G_E$ has finite index in $G$, the subgroup $G(x)$ is of finite index in $G$.

   Moreover, the fixed field $\mathbf{C}^{G(x)}$ under $G(x)$ is a finite extension of the fixed field $\mathbf{C}^G = \overline{\mathbf{Q}}$, but $\overline{\mathbf{Q}}$ is algebraically closed, hence we have $\mathbf{C}^{G(x)} = \overline{\mathbf{Q}}$.

3) For a natural number $N$ let $V(N)$ denote the vector space over $\mathbf{C}$ of all $f \in E$ with only one pole which is at $x$ and $\mathrm{ord}_x(f) \geq -N$. Choose $N \geq 1$ so large that $V(N)$ generates $E$. This is possible by Riemann-Roch.

   We define a $G(x)$-equivariant linear map $\theta : V \to \mathbf{C}[x]_{\leq N}$ by the property

$$\mathrm{ord}_x(\theta(f)(\pi_x) - f) > 0$$

   where $\theta(f)$ is the polar part of $f$.

We know that the subspaces $V$ of $\mathbf{C}[x]_{\leq N} = \mathbf{C}^{N+1}$ satisfying $\sigma(V) = V$ are generated by $G(x)$-invariant elements $f$ such that $\theta(f)$ is an $G(x)$ invariant and so $\theta(f) \in \overline{\mathbf{Q}}[x]$, see N. Bourbaki, Algèbre, Ch. II. 8, no 7, Theorème 1. Each such $f$

has a minimal polynomial over $\mathbf{C}(T)$ fixed by $G(x)$, and hence it is a polynomial over $\overline{\mathbf{Q}}(T)$.

If $f_1, \ldots, f_m$ is a $G(x)$-invariant basis of $V(N)$, then the field $K$ generated by $f_1, \ldots, f_m$ over $\overline{\mathbf{Q}}$ is a function field with the composite of $\mathbf{C}$ and $K$ over $\overline{\mathbf{Q}}$ equal to $\mathbf{C}(X)$, and $K$ defines the structure of $X$ over $\overline{\mathbf{Q}}$. This proves the converse of the main assertion.

## § 5. Field of definition of ramified coverings: scheme theory methods

The following theorem also contains the converse statement in the basic characterization of curves over a number field. It is included for the reader who has a familiarity with D. Mumford's "red book".

**(5.1) Theorem.** *Let $p : Y \to X$ be a ramified covering of a curve $X$ defined over a field $k_0$ such that the ramification locus of $p$ is contained in $X(k_0)$. Then $Y$ is a curve defined over a finite extension of $k_0$.*

*Proof.* Let $k$ be an algebraically closed field of definition for the curve $X$ and the curve $Y$. This means that they are schemes with structure maps $X \to \mathrm{Spec}(k)$ and $Y \to \mathrm{Spec}(k)$ commuting with $p$. Since $X$ is defined over $k_0$ there is a subscheme $X_0$ of $X$ such that the natural morphism

$$k \times_{k_0} X_0 \to X$$

is an isomorphism of schemes. Moreover, if $k_0(x)$ denotes the function field of $X_0$ over $k_0$, then there is an isomorphism $k \otimes_{k_0} k_0(X) \to k(X)$.

Let $S$ be the finite set of $k_0$ rational ramification points of $p$. For a nonempty set $S$, the scheme $X' = X \subset X$ is affine and defined over $k_0$ with affine ring of functions $k_0[X']$. Moreover, it is a generality on one dimensional functions fields that the function field $k_0(X)$ results from this affine ring $k_0[X']$ by inverting one function $g$.

The unramified covering $p : Y' = Y \setminus p^{-1}(S) \to X'$ is given by a finite tale extension $k_0[Y']$ of $k_0[X']$. There is a localization $K$ of $k_0[Y']$ by a product indexed by the ramification locus $S$ of local terms arising from roots of local parameters of the local rings at the points of the set $S$. In particular, $K$ is a finite extension of $k_0(X)$, and $K$ contains a field $k_1$ which is a finite extension of $k_0$ and a field of definition for $Y_0$. This proves the theorem. q.e.d.

*(5.2) Remark.* We have now established the main theorem (0.1) announced in the introduction.

# Part II

## § 6. Triangulations coming from ramified coverings

The comples projective line or Riemann sphere $\hat{C}$ has a cell decomposition which is almost a triangulation. There are three zero cells $\{0, 1, \infty\}$, there are three open one cells given by their boundary zero cells, $\{(-\infty, 0), (0, 1), (1, +\infty)\}$ given by their boundary zero cells, and there are two open two cells fitted in as triangles, the upper and lower half planes.

*(6.1) Definition.* A triangular cell decomposition of a real two dimensional manifold $M$ has a cellular fitration $M_0 - M_1 \subset M_2 = M$ where the closure in $M$ of each open 2-cell $e$ of $M \setminus M_1$ is $e$ together with exactly three 1-cells and three 0-cells as if it where a triangle.

A triangular cell decomposition is a triangulation if and only if the intersection of the closures of two distinct 2-cells is either empty or a closed 1-cell in their common boundary. The decomposition of $\hat{C}$ given by the upper and lower half planes is a triangular cell decomposition but not a triangulation. When the zero skeleton is the real axis, we call this the canonical cell decomposition.

*(6.2) Remark.* If $p : X \to Y$ is a ramified covering of real surfaces with branch locus $\mathrm{ram}(p)$ contained in the zero skeleton of $Y$, then the inverse image cell decomposition where

$$X_0 = p^{-1}(Y_0) \subset X_1 = p^{-1}(Y_1) \subset X = X_2$$

is a triangular cell decomposition. What is clear is that the closure of each 2-cell in $X$ contains exactly three 1-cells.

We are interested in determining when a given triangular cell decomposition on a real surface $X$ comes by inverse image using (6.2) with a ramified covering $p : X \to \hat{C}$ satisfying $\mathrm{ram}(p) \subset \{0, 1, \infty\}$ from the Riemann sphere $\hat{C}$ with its canonical triangular cell decomposition. If we can solve this, then we can construct some examples of ramified coverings over $\hat{C}$ with ramification contained in the set of three points $\{0, 1, \infty\}$.

*(6.3) Remark.* When the triangular cell decomposition arises from the Riemann sphere the three 0-cells and the three connecting 1-cells are arranged in a cyclic order, there are two possible such orderings. Further there is a function $\epsilon$ on the set of 2- cells to $\{\pm 1\}$ where $\epsilon(e) = +1$ if $p(e)$ is the upper half plane and $\epsilon(e) = -1$ if $p(e)$ is the lower half plane. If $\epsilon(e) = +1$, then the cyclic ordering of the 0-cells and of the 1-cells follows from the orientation. Hence the cyclic ordering of 0-cells and of 1-cells is determined by the orientation and the value of $\epsilon(e)$.

*(6.4) Definition.* A triangular cell decomposition of a real two dimensional manifold is signed provided there is a function $\epsilon$ on the set of 2-cells to $\{\pm 1\}$ such that if two 2-cells $e$ and $e'$ have an edge in common, then they have opposite signs $\epsilon(e) = -\epsilon(e')$.

*(6.5) Proposition.* Let $M$ be an oriented real two dimensional manifold with a signed triangular decomposition. Then there is a three fold unramified covering $M' \to M$ with induced signed triangular cell decomposition which is induced by a ramified cover $M' \to \hat{C}$ with ramification contained in $\{0, 1, \infty\}$.

*Proof.* Let $e$ be a 2-cell of $M$ with closure $e \cup \{c, c', c''\}$ with $c, c', c''$ closed 1-cells oriented into a circle. If $\epsilon(e) = +1$, then we map $e$ to the upper half plane, and there are three ways to extend the map to the boundary closed 1-cells to $\mathbf{P}_1(\mathbf{R})$ with a simplicial preserving orientation mapping. For $\epsilon(e) = -1$, then we map $e$ to the lower half plane, and again there are three ways to extend the map to the boundary closed 1-cells to $\mathbf{P}_1(\mathbf{R})$ by a simplicial map preserving orientation mapping. The three ways of extending to the boundary of the signed 2-cell generate a 3-fold covering $M' \to M$. It is $M'$ that maps to $\hat{C}$, and induces the signed triangular cell decomposition on $M'$ coming from $M$. This proves the proposition. q.e.d.

*(6.6) Remark.* (J. Alexander, 1920) Let $M$ be an oriented, triangulated surface. The first barycentric subdivision of $M$ has a unique sign decomposition where a 2- simplex $\sigma = (s_0, s_1, s_2)$ is made up of a 0-simplex, 1-simplex, and 2-simplex of the original subdivision. The simplex $\sigma$ has $\epsilon(\sigma) = +1$ when the ordered simplex $s_0, s_1, s_2$ is compatible with the orientation and $\epsilon(\sigma) = -1$ otherwise.

*(6.7) Remark.* Proposition (6.5) shows in particular that the decomposition of the sphere into a pair of triangles is universal in the sense that any signed triangulation of a sphere is induced by a map from this decomposition with a pair of triangles. It is interesting to remark that the famous 4-color theorem can be reformulated in a similar manner: The tetrahedral triangulation is universal among all triangulations of the sphere. Namely, if we have any triangulation $\Delta$ of the 2-sphere, then there exists a strict simplicial map $f : \mathrm{dual}(\Delta) \to (\text{tetrahedron})$, and hence, $\Delta$ is induced by $f$ from the tetrahedron. The dual triangulation $\mathrm{dual}(\Delta)$ exists under the assumption that $\Delta$ has at most three edges at a vertex and that the boundary between any two faces is connected.

## § 7. Modular curves and curves ramified over three points

Consider a Galois covering $X \to \mathbf{P}^1 \setminus \{0, 1, \infty\}$ which is finite of degree $n$. Then the local monodromy is given by natural numbers $(n_0, n_1, n_\infty)$ each dividing $n$.

*(7.1) Proposition.* (Manin, 1978) Let $X$ be a curve over the field of algebraic numbers $\overline{\mathbf{Q}}$. Then there exists a modular curve $X(2N)$, an unramified covering $X' \to X(2N)$, and a surjective map $X' \to X$.

*Proof.* Let $f : X \to \mathbf{P}^1$ be a ramified covering with $\mathrm{ram}(f) \subset \{0, 1, \infty\}$ and let $g : Y \to \mathbf{P}^1$ be a Galois map covering which is factored $Y \to X \to \mathbf{P}^1$ by $f$. All ramification indices over $g$ over a point are equal. Consider the natural projections on the modular curves $\pi : X(2N) \to X(2)$ and $\sigma : X(2) = \mathbf{P}^1 \to \mathbf{P}^1 = X(1)$. Note that $\sigma$ is a Galois covering of degree 6 with $\sigma^{-1}(\infty) = \{0, 1, \infty\} \subset \mathbf{P}^1 = X(2)$ with Galois group $\mathrm{Sym}_3$, the symmetric group on 3 elements. The multiplicities of $\pi$ are divisible by $N$. Now choose $N$ such that all of the three multiplicities of $\pi$ over $0, 1, \infty$ divide $N$. Then the fibre product $X' = Y \times_{X(2)} X(2N)$ is unramified over $X(2N)$ and maps surjectively onto $X$ by projecting through $Y$. The fact that $X' \to X(2N)$ is unramified is a local computation. We can check this by considering the fibre product of unit discs $D' \xrightarrow{N} D$ and $D'' \xrightarrow{n} D$ denotes the map $f(z) = z^q$. If $n \mid N$, then the projection $D' \times_D D'' \to D'$ is unramified. This proves the proposition.

*(7.2) Remark.* The unramified coverings of a curve over a number field $k$ preserve many of the arithmetic features of the curve itself. In particular, the inverse image of $x \in X(N)(k)$ in the above covering is a finite set of points $x'$ each corresponding to the arithmetic ramification of the covering map. This means that there exists a finite set of primes in $\overline{\mathbf{Q}}$ such that all ramification of $k'$ over $k$ is contained in this set where $k'$ is the field of definition of the point $x'$ over $x$.

*Remark.* There are many other classes of curves, for example, Fermat curves for which the above discussion applies in a similiar manner.

*(7.4) Remark.* Conjecturally the above result can be improved so that we can take one curve and its nonramified coverings in order to dominate all curves defined over number fields. Even further any curve of genus $\geq 2$ defined over a number field should have that property.

## § 8. Dominant classes of varieties

Manin's result shows in particular that unramified coverings of modular curves are sufficient to dominate any algebraic curve defined over $\overline{\mathbf{Q}}$. To pose a general question, we introduce the following definition.

*(8.1) Definition.* Let $\mathcal{V}(n,k)$ be the class of algebraic varieties of dimension $n$ over a field $k$. A subclass $\mathcal{M}$ of $\mathcal{V}(n,k)$ is dominant provided for any $X \in \mathcal{V}(n,k)$ we can find $Y \in \mathcal{M}$ and a surjective morphism $f : Y \to X$ defined over $k$.

Then a natural question arises.

*(8.2) Question.* For given $n$ and $k$ find a dominant class of varieties which is as small as possible.

*(8.3) Conjecture.* For $n \geq 2$ and $k = \overline{\mathbf{Q}}$ there exists a dominate class which is in the sense of topology smaller than any dominant class over $\mathbf{C}$.

The extreme variant of this conjecture, likely not true, is that the class of varieties of the form $D^n/\Gamma$ is dominant for $k = \overline{\mathbf{Q}}$. Here $D^n$ is the unit ball in $\mathbf{C}^n$ and $\Gamma$ is a discrete group of analytic automorphisms with finite covolume.

There are indications that the class of high dimensional Kobayashi varieties is dominate over $\mathbf{C}$. Recall that a Kobyashi variety is a smooth projective variety with a sequence of smooth nondegenerate projections between projective varieties $X_i$ of dimension $i$ lowering dimension by one

$$X = X_n \to \ldots \to X_i \to \ldots \to X_1.$$

## § 9. Ramification over more than three points

It is interesting to try to extend the Main theorem about three points to more points on $\mathbf{P}^1$ and other fields of definition. This is related to above discussion of dominant classes of varieties. For example, if $X$ is defined over the field $\overline{\mathbf{Q}}(t)$. This is the case for elliptic curves, but it does not seem likely for curves of genus two.

*(9.1) Remark.* Any curve defined over $K$ where $K$ is a field of algebraic functions over $\overline{\mathbf{Q}}$ of transcendence degree $\geq 3g-3$ and $g \geq 3$ can be obtained as a covering of $\mathbf{P}^1$ with $3+3g-3=3g$ points of ramification. Any Hurwitz scheme of such curves has dimension at most $3g-3$, and therefore, any curve of genus $g$ can be found in such a scheme.

*(9.2) Conjecture.* Let $X$ be a curve defined over a field $K$ where $K$ has transcendence degree $h$ over $\overline{\mathbf{Q}}$. Then there exists $X'$ defined over a finite extension $K'$ over $K$ such that

(1) there is a map $f : X' \to \mathbf{P}^1$ over $K'$ with at most $3+h$ points of ramification, and
(2) there is a surjective morphism $g : X' \to X$ over $K'$.

The above conjecture would imply in particular that dominant classes of algebraic varieties over $\overline{\mathbf{Q}}$ are rather small.

## § 10. Faithful action of $\mathrm{Gal}(\overline{\mathbf{Q}} \subset \mathbf{Q})$ on the profree group on two generators

*(10.1) Definition.* For a finite set $S \subset \mathbf{P}^1(\mathbf{Q})$ the quotient of $\mathrm{Gal}(\overline{\mathbf{Q}(t)}|\mathbf{Q})$ which describes those extensions which are ramified only over $S$ only over $S$ is denoted $\mathrm{Gal}_S(\mathbf{Q}(t))$.

*(10.2) Remark.* If $S$ has $h+1$ elements, then we have an exact sequence of groups where $\hat{F}^h$ is the profinite completion of the free group with $h$ generators

$$1 \to \hat{F}(h) \to \mathrm{Gal}_S(\mathbf{Q}(t)) \to \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to 1.$$

As in any group extension, the quotient $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts by conjugation, and this restricts to a group morphism

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Out}(\hat{F}(h)) = \mathrm{Aut}(\hat{F}(h))/\mathrm{Inn}(\hat{F}(h)).$$

From the Main theorem we have the following proposition.

*(10.3) Proposition.* For $h \geq 2$ the above morphism

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Out}(F(h)) = \mathrm{Aut}(\hat{F}(h))/\mathrm{Inn}(\hat{F}(h))$$

is an injection.

*Proof.* Each nontrivial $s \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts nontrivially on some finite extension $K$ of $\mathbf{Q}$, and therefore, we can find a pair of plane curves $X$ and $X^s$ such that the corresponding complex curves are not isomorphic. Plane curves are isomorphic if and only if they are related by a projective transformation. Then there are subgroups of finite index $\Gamma$ and $\Gamma^s$ in $F^h$ which are not conjugate where $\Gamma$ describes $X$ as a covering of $\mathbf{P}^1$ ramified in $S$ and $\Gamma^s$ describes $X^s$ as a covering of $\mathbf{P}^1$. Hence $s$ defines a nontrivial element in $\mathrm{Out}(\hat{F}^h)$. This proves the proposition.

*(10.4) Remark.* In the case of $S = \{0, 1, \infty\}$ the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ stabilizes conjugacy classes of topologically cyclic ramification subgroups, each isomorphic to $\hat{\mathbf{Z}}$, corresponding to $0, 1, \infty$. We choose generating elements $x \in \mathbf{Z}_0, y \in \mathbf{Z}_1$, and $z \in \mathbf{Z}_\infty$ such that $z = xy$. The action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ stabilizes any group relation. For $s \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ the image of $x$ in the abelianization has the form $s(x) = x^{\alpha(s)}$ where $\alpha(s) \in \hat{\mathbf{Z}}^*$. Further we may assume that $s(y) = y^{\alpha(s)}$ and $s(z) = z^{\alpha(s)}$ in the abelianization of $\hat{F}^2$.

By applying an inner automorphism, we can assume that $s(x) = x^{\alpha(s)}, s(y) = uy^{\alpha(s)}u^{-1}$ and $s(z) = vz^{\alpha(s)}v^{-1}$ in $\hat{F}^2$. Since $s(z) = s(x)s(y)$, we obtain a nontrivial relation for $u$, that is, $x^{\alpha(s)}uy^{\alpha(s)}u^{-1}$ is conjugate to $(xy)^{\alpha(s)}$. In this case $v$ is almost uniquely defined by $u$. Belyi raised the question: Does this equation in fact define $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ as a subgroup of $\mathrm{Out}(\hat{F}^2)$. ?

## References


[1] Alexander, *Note in Riemann spaces*, Bull. AMS, **26** (1920), 370-372.

[2] Belyi, G. V., *On Galois extensions of the maximal cyclotomic field*, Math. USSR Izvestija, **43**:2 (1979), pp. 269-276 or English translation, **14** (1980) no. 2, 247-256.

[3] Bogomolov, F.A. and T.G. Pantev, *Weak Hironaka theorem*, Mathematical Research Letters **3** (1996) 299-308.

[4] Bost, J-B., *Riemann surfaces*, Preprint of I.H.E.S. (1992).

[5] Deligne, P., *Le Groupe Fondamental de la Droite Projective Moins Trois Points, Galois groups over* **Q**, ed. K. Ribet and J-P. Serre, Springer-Verlag, 1989.

[6] Drinfel'd, V., *On quasitriangular quasi-Hopf algebras and a group closely connected with* $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$, Leningrad Math. J., **2** (1991), 829-860.

[7] Elkies, N., *ABC implies Mordell*, International Mathematics Research Notices, Duke, 1991, No. 7., p. 99.

[8] Grothendieck, A., *Esquisse d'un programme*, preprint (1984).

[9] Ihara, Yasutaka, *Arithmetic analogues of braid groups and Galois representations*, Contemporary Mathematics, volume 78 (1988), 245-257.

[10] Mumford, D., *Algebraic geometry: the red book*, Springer LN 1358.

[11] Schneps, L., *The Grothendieck Theory of Dessins d'Enfants*, LMS Lecture Notes, **200** (1994), Cambridge Univ. Press.

[12] Schneps, L. and Lochak P., *Geometric Galois Actions*, LMS Lecture Notes, **242** (1994), Cambridge Univ. Press.

[13] Shabat, G.B., *On the classification of plane trees by their Galois orbits*, LMS Lecture Notes **200** (1994), Cambridge Univ. Press.

[14] Shabat, G.B. and V.A. Voevodsky, *Drawing curves over number fields*, Grothendieck Festschrift, **3** (1990), 199-227.