Another proof of three points theorem

G.V.Belyi

April 25, 1997

In the paper *"On Galois Extensions of a Maximal Cyclotomic Field"* we proved the following theorem.

1. Theorem. *A complete nonsingular algebraic curve X defined over a field of characteristic zero can be defined over $\overline{\mathbb{Q}}$ if and only if it can cover $\mathbb{P}^1$ with three branching points $0\,,\ 1\,,\ \infty$.*

See Izvestiya Ak.Nauk SSSR, ser. mat. **43**(**2**) (1979), 269-276. The aim of this notice is to give a new proof of this theorem. We adduce the both proofs because they are very short and explicit, in order to the reader can easily compare them.

Old Proof. The "if" part of the theorem follows from the Weil criterion, so we have to show the "only if" part. We do it in three steps.

Step 1: Suppose that X is defined over $\overline{\mathbb{Q}}$. We choose an arbitrary nonconstant rational function $t \in \overline{\mathbb{Q}}(X)$. It defines a covering of $\mathbb{P}^1$ with branching in some finite set of points B_1 that are defined over $\overline{\mathbb{Q}}$.

Step 2: Let $h_i(t)$ be the minimal polynomial over $\mathbb{Q}$ for the set of finite points in the set B_i and let

$$B_{i+1} = \{ h_i(\xi) \,|\, h_i{}'(\xi) = 0 \}$$

be the set of finite branching points for the polynomial $h_i(t)$. It is clear that

$$\deg h_{i+1} \leq (\deg h_i) - 1\,.$$

Consequently, in no more than $\deg h_1$ steps we must obtain a linear polynomial h_l. We now take

$$f(t) = h_{l-1}(h_{l-2}(\ldots(h_1(t))\ldots))\,.$$

By construction the covering $f(t):\ X \to \mathbb{P}^1$ branches in some rational points set A.

Step 3: If we find a polynomial $g_A(f) \in \mathbb{Q}[f]$ that is only ramified over $\{0, 1, \infty\}$, and such that $g_A(A) \subseteq \{0, 1, \infty\}$, then the composition $g_A(f(t))$ will give us the required covering. We shall say that such a polynomial satisfies the condition (b_A).

If $A = A_1 \cup \{s\}$ and $g_{A_1}(f)$ has already been constructed we denote by A_2 the set $\{0\,,\ 1\,, \infty\,,\ g_{A_1}(s)\}$. Now we can take $g_A(f)$ to be the polynomial $g_{A_2}(g_{A_1}(f))$. Hence it suffices to construct the polynomial $g_{A_3}(f)$ for a set A_3 consisting of three finite rational points and ∞. Making a linear change of variables, we may assume that $A_3 = \{0, s, 1, \infty\}$, where $0 < s < 1$. If $s = m/(m+n)$, where m and n are natural numbers, then we set

$$g_{A_3}(f) = \frac{(m+n)^{m+n}}{m^m \cdot n^n} \cdot f^m \cdot (1-f)^n .$$

New Proof. It differs from the old one only in the third step. We take a rational function instead of the polynomial $g_A(f) \in \mathbb{Q}[f]$. Let now

$$g_A(f) = \prod_{i=1}^{n} (f - \lambda_i)^{r_i} \in \mathbb{Q}(f) , \quad \text{where} \quad \sum_{i=1}^{n} r_i = 0 ,$$

and $A = \{\lambda_1, \ldots, \lambda_n, \infty\}$. We may suppose without loss of generality that all these λ are integers, $0 = \lambda_1 < \lambda_2 < \cdots < \lambda_n$, and $\gcd(\lambda_2, \ldots, \lambda_n) = 1$. Note that the function $g_A(f)$ ramifies only at zeros and poles of its logarithmic derivative

$$\frac{g'_A(f)}{g_A(f)} = \sum_{i=1}^{n} \frac{r_i}{f - \lambda_i} .$$

Denote by $W = W(\lambda_1, \ldots, \lambda_n)$ the Vandermonde determinant; and let

$$w_i = (-1)^{n-1} W(\lambda_1, \ldots, \widehat{\lambda_i}, \ldots, \lambda_n)$$

be the Vandermonde determinant, where the hat $\widehat{\lambda_i}$ means that the corresponding λ_i is omitted. Besides, we denote by $N = \gcd(w_1, \ldots, w_n)$. We see that the function

$$\sum_{i=1}^{n} \frac{w_i}{f - \lambda_i} = W \cdot \prod_{i=1}^{n} (f - \lambda_i)^{-1}$$

has the unique n-multiple zero at the infinity. Setting $r_i = w_i / N$ we see that the rational function $g_A(f)$ satisfies the condition (b_A). In more detail, the function $g_A(f)$ takes $\lambda_1, \lambda_3, \ldots$ to 0; it sends $\lambda_2, \lambda_4, \ldots$ to ∞. Besides, $g_A(f)$ takes ∞ to 1 and does not ramifies outside A.

We obtain the new function $g_A(f)$ in much more explicit way comparatively to the old way, where we used induction; and where the polynomial g_A depended on a choice of some ordering on the set A. Although, we lose the property of the function to be a polynomial; nevertheless, we won something; now we can control the bad reduction points for the covering $g_A : \mathbb{P}^1 \to \mathbb{P}^1$.

2. Claim. *A rational prime number p is the bad reduction point for the covering g_A iff p divides the Vandermonde determinant $W_A = W(\lambda_1, \ldots, \lambda_n)$.*

Proof. Evident.

We suppose n is even now and define the hyperelliptic curve Y_A by the equation

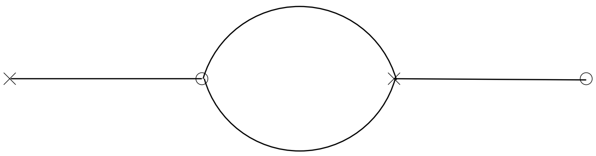
$$y^2 = (x - \lambda_1)(x - \lambda_2) \ldots (x - \lambda_n) .$$

Let X be a Galois closure of the covering g_A, $H_A = Gal\,(X/\mathbb{P}^1)$, and h_A be the order of the group H. An interesting question arises: It seams should exist a connection between this order h_A and the hight of this hyperelliptic curve $h\,(Y_A)$?

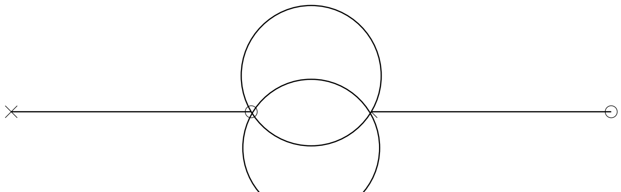
3. Examples: Let A' be the finite part of A. We list the all covering g_A for $A' \subset \{\pm 1,\, \pm 3,\, \pm 5\} \cong \{0,\, 1,\, 2,\, 3,\, 4,\, 5\}$ with $n = \#\,(A') = 4,\, 5,\, 6$. Besides, we draw corresponding Grothendieck's "dessins d'enfants" in the cases they are symmetric. We understand them as inverse images of the segment $g_A^{-1}\,(-\infty\,,\, 0)$.

1) $g = \dfrac{(t+2)(t-1)^2}{(t-2)(t+1)^2}$

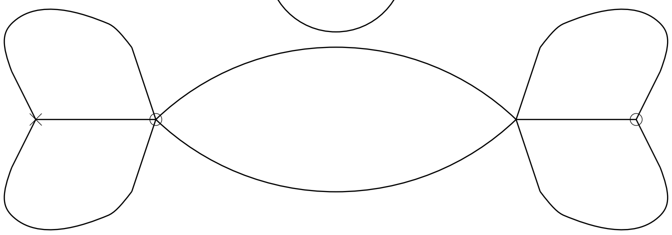
2) $g = \dfrac{(t+3)(t-1)^3}{(t-3)(t+1)^3}$



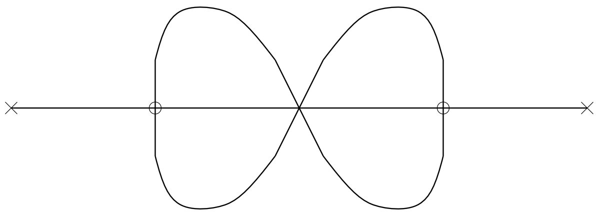
3) $g = \dfrac{(t+5)(t-1)^5}{(t-5)(t+1)^5}$



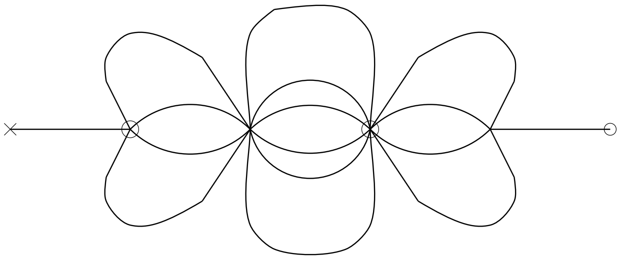
4) $g = \dfrac{(t+5)^3(t-3)^5}{(t-5)^3(t+3)^5}$



5) $g = \dfrac{(t^2-4)\,t^6}{(t^2-1)^4}$



6) $g = \dfrac{(t+5)(t-3)^5(t+1)^{10}}{(t-5)(t+3)^5(t-1)^{10}}$



Under the restrictions mentioned above we have five more cases: g is equal to

$$\frac{t\,(t-3)^8}{(t-4)^3\,(t-2)^6}\,, \qquad \frac{(t-5)^2\,t^3\,(t-2)^{10}}{(t-3)^5\,(t-1)^{10}}\,, \qquad \frac{t\,(t-4)^{15}}{(t-5)^6\,(t-3)^{10}}\,,$$

$$\frac{t^8\,(t-3)^{10}}{(t-5)^3\,(t-1)^{15}}\,, \qquad \text{or} \qquad \frac{(t-5)\,t^4\,(t-2)^{20}}{(t-3)^{10}\,(t-1)^{15}}\,.$$

We leave it to the reader to make pictures. It is not hard to check that the Galois groups H corresponding to the coverings in this list either are the symmeric groups S_n or are the alternating groups A_n.

Finally, I should like to thank the MPI for hospitality.