(*August 27, 2001*)

Belyi's proof of a conjecture of Grothendieck

Paul Garrett, garrett@math.umn.edu, *©2001*

(This proof is due to Gennady Belyi, mid-to-late 1980's.)

Theorem: Let X be a complete connected curve defined over a number field. Then there is a morphism $\pi : X \to \mathbf{P}^1$ from X to the projective line $\mathbf{P}^1$ which is defined over $\mathbf{Q}$ and ramified at most at $0, 1$, and ∞.

Proof: For a non-constant meromorphic function f in $\overline{\mathbf{Q}}(X)$, view f as giving a Qb-morphism to $\mathbf{P}^1$. Let $S \subset \mathbf{P}^1$ be the points ramified for f. By composing with a linear fractional transformation with coefficients in $\overline{\mathbf{Q}}$, we may suppose without loss of generality that such a set S contains $0, 1, \infty$ whenever the cardinality of S is at least 3.

First we reduce to the case that the ramified points are *rational*, rather than merely *algebraic*. Let $\alpha \in S \cap \overline{\mathbf{Q}}$ be an algebraic number of maximal degree over Q among all such. Suppose that the degree $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ is greater than 1, and let P be the minimal polynomial of α over $\mathbf{Q}$. Then $P \circ f : X \to \mathbf{P}^1$ is ramified at

$$P(S) \cup \{ \text{ zeros of the derivative } P' \}$$

Thus, $P \circ f$ has fewer ramified points of degree $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ than did f, since $(P \circ f)(\alpha) = 0$ and since the degree of P' is less than that of P. Therefore, by induction, we may suppose that we are given $f : X \to \mathbf{P}^1$ ramified only at *rational* points and possibly ∞.

By composing with a linear fractional transformation, we may suppose without loss of generality that all the ramified points are ∞ or rational points in the interval $[0, 1]$. If the cardinality of S is strictly greater than 3, then there is an element of S of the form $m/(m + n)$ with $m \geq 1$, $n \geq 1$, both integers. Consider the map

$$g(z) = z^m \, (1 - z)^n$$

The derivative g' has zeros at most at $0, 1, m/(m + n)$. Thus, the composite map $g \circ f$ is ramified over

$$g(S - \{0, \frac{m}{m+n}, 1\}) \cup g(0, \frac{m}{m+n}, 1) = g(S - \{0, \frac{m}{m+n}, 1\}) \cup \{g(0), g(\frac{m}{m+n})\}$$

since $g(0) = g(1)$. In particular, $g \circ f$ has strictly fewer ramified points than does f.

Continuing the latter process, adjusting by linear fractional transformations over $\mathbf{Q}$ as necessary, by induction the desired result is achieved. ♣