ARTU Spring 2016 Report *

Philip Bonneville

June 6, 2016

My goal for completing this ARTU project is, at a minimum, to produce a report clarifying and generalizing the correspondence between trinomials with small Galois group and rational points on a curve used by Elkies and Bruin in [1]. Recently I have been working to use the tools of scheme theory (as described in my Spring 2015 report) to better understand this correspondence.

To every function field K over $\mathbb{Q}$, we associate, canonically, a non-singular, projective curve C_K, which we will view as a scheme (cf. [2]): For each discrete valuation ring R that containing $\mathbb{Q}$ and having quotient field K, there is a closed point at which the stalk of the sheaf is R. At the generic point, the stalk is simply K.

Let $f : L \to K$ be a $\mathbb{Q}$-homomorphism. If R is a discrete valuation ring containing $\mathbb{Q}$ and having quotient field K, then $f^{-1}[R]$ is a discrete valuation ring containing $\mathbb{Q}$ and having quotient field L. We may thus obtain a canonoical morphism from C_K to C_L.

Given any irreducible polynomial p over $\mathbb{Q}(t)$, define the field E by appending a variable x satisfying $p(x) = 0$ to $\mathbb{Q}(t)$, i.e. $E = \mathbb{Q}(t)[x]/(p(x))$. Then we have an embedding $\mathbb{Q}(t) \to E$. Let Γ be the Galois closure of E over $\mathbb{Q}(t)$. Using the functor given above, we obtain from the embedding $\mathbb{Q}(t) \to \Gamma$ a cover γ of $C_{\mathbb{Q}(t)} \simeq \mathbb{P}^1_{\mathbb{Q}}$ by C_Γ. By looking at the intermediate fields between $\mathbb{Q}(t)$ and Γ, we may obtain intermediate covers of $\mathbb{P}^1$. Elkies and Bruin study this system of covers when $p(x) = x^n + tx + t$, for n equal to 7 or 8.

Analyzing the morphisms obtained from the covers of curves *after* specialization has sufficed to prove the desired correspondence. Indeed, after taking fibered products along a map $\operatorname{Spec} \mathbb{Q} \to \mathbb{P}^1_{\mathbb{Q}}$ specifying a rational value for t, we are left with a system of affine schemes over $\mathbb{Q}$ containing only finitely many points. The residue field at a point in one of these fibers is equal to $\mathbb{Q}$ if and only if that point is rational.

By specifying a point q on the most general fiber $C_\Gamma \times_{\mathbb{P}^1_{\mathbb{Q}}} \operatorname{Spec} \mathbb{Q}$ (and, indeed, all the points in this fiber are equivalent up to a permutation), we are able to obtain a system of individual points over $\operatorname{Spec} \mathbb{Q}$. Looking at the stalks of these points, we end up with a system of field extensions of $\mathbb{Q}$ that we would like to study.

For each subgroup H of the Galois group of Γ, let Λ_H by the corresponding field extension in the above system. Then with some work it can be shown that, if q is not a branch point, Λ_H is equal to the fixed field $\Lambda_1^{H \cap K}$, where K is the Galois group of Λ_1. (The necessary identification of groups is performed by using the functor described earlier to map the Galois group of Λ to the automorphism group of C_Λ, which in turn can be mapped to the automorphism group of $C_\Gamma \times_{\mathbb{P}^1_{\mathbb{Q}}} \operatorname{Spec} \mathbb{Q}$ via a fibered product argument. If an element of this automorphism group fixes the specified point q, then it induces a $\mathbb{Q}$-automorphism of the field Λ_1.)

*This material is based upon work supported by the National Science Foundation under agreement No. DMS-1055897. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Future directions for study include generalizing the above result to branch points and checking whether the Galois group of Γ is always S_n (as it is in Elkies and Bruin's case).

References

[1] Nils Bruin and Noam D. Elkies. Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois groups of order 168 and $8 \cdot 168$. *Algorithmic Number Theory*, 2369:172–188, 2002.

[2] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, 1977.