Inverse Galois problem for ordinary curves: construction of some examples

R. van Bommel

Monday 7 November 2016

Abstract. For curves over $\mathbb{Q}$ with good reduction at p, one can ask about the size of the p-torsion of the reduction of its Jacobian. If this p-torsion group has maximum size, the curve is called ordinary. In this talk, we will discuss an extension of this notion to (families of) semi-stable curves. We will use associated graphs to study the action of finite groups on ordinary semi-stable curves, giving rise to Galois covers of semi-stable curves. Using deformation theory, we will deform these covers into covers of smooth curves, keeping the ordinarity of the original curve, in an attempt to (partially) solve the inverse Galois problem for ordinary smooth curves. Finally, we will construct some explicit examples.

0 Introduction

The inverse Galois problem has been studied before for function fields. For the function fields $\mathbb{Q}_p(t)$ and $\overline{\mathbb{F}}_p(t)$ the problem has been solved constructively using rigid analytic methods, see for example [MaMa99, Ch. V]. Now, if we consider the geometric picture and consider the constructed covers as Galois covers of $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$, this method does not tell us much about the geometric properties of the covers. We are in particular interested to know when it is possible to construct ordinary Galois covers of $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$. The method discussed in this talk will provide a method construct such ordinary Galois covers of $\mathbb{P}^1$ for various Galois groups. In particular, it will allow us to constructively show that there exist ordinary hyperelliptic curve of any genus (cf. [GlPr05, Thm. 1, sect. 2, p. 301]).

0.1 Conventions and notation

Everywhere k is assumed to be a field of characteristic $p > 0$ and $\bar{k}$ is assumed to be an algebraic closure of k.

A *curve* over some base scheme S is defined to be a scheme which is fibre-wise geometrically reduced and geometrically connected, and projective, flat, of relative dimension 1 over S.

1 Ordinarity of semi-stable curves

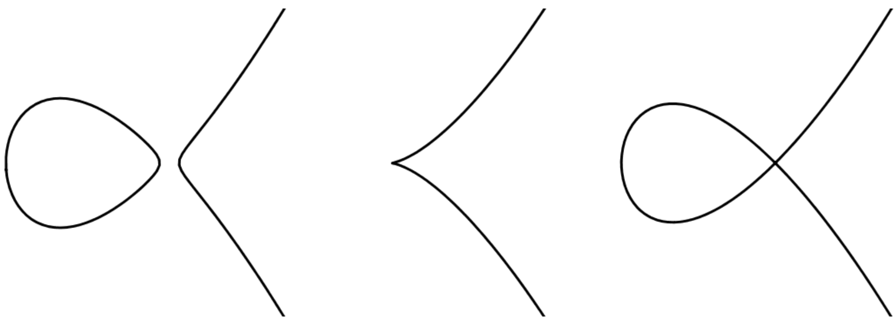
For smooth curves over a field k, there is a classical notion of ordinariness.

Definition 1. Let C/k be a smooth curve of genus g. Then C is called *ordinary* if its Jacobian J is ordinary, i.e. if $|J[p](\bar{k})|$ is maximal:

$$|J[p](\bar{k})| = p^g.$$

Now we will extend this definition in two ways: it will work for semi-stable curves, and it will work over arbitrary base schemes. Let us first quickly recall a definition.

Definition 2. A curve $C/\bar{k}$ is called *semi-stable* if all its singular points are nodal. More generally, a curve C/S is called *semi-stable* if all its geometric fibres are.



smooth (hence semi-stable) not semi-stable semi-stable

Definition 3. Let $C/\bar{k}$ be a semi-stable curve. Then C is called *ordinary* if the map $F : H^1(C, \mathcal{O}_C) \to H^1(C, \mathcal{O}_C)$ induced by the absolute Frobenius is an isomorphism. More generally, a semi-stable curve C/S is called *ordinary* is all its geometric fibres are.

This definition is chosen in such a way that the locus on S on which a curve C/S is ordinary is always open (cf. [FvdG04]) . The following proposition provides us with a more intuitive alternative definition.

Proposition 4. *Let $C/\bar{k}$ be a semi-stable curve, and let $C_1, \ldots, C_\ell$ be the components of its normalisation. Then C is ordinary if and only if $C_1, \ldots, C_\ell$ are.*

2 Graphs associated to semi-stable curves

To a semi-stable curve one can associate a graph by taking its irreducible components as vertices and its singular (nodal) points as edges. Next we want to consider finite groups acting on semi-stable curves. We want to formally define the associated graph in such a way that the categorical quotient by the group action commutes with taking the associated graph. The following two example will be used to (partially) motivate the definition that follows.

Example 5. Let C/k be a curve obtained by gluing three copies of $\mathbb{P}^1$ in a triangle shape. We let the group $G = \mathbb{Z}/3\mathbb{Z}$ act on C by cyclically permuting these curves. Then the quotient of C by G is one copy of $\mathbb{P}^1$ with two of its points glued together.

Example 6. Let C/k be the same curve as in the previous example. We let the group $G = S_3$ act on C, by cyclically permuting and mirroring the whole curve in its three symmetry axes. Then the quotient of C by G is isomorphic to $\mathbb{P}^1$.

Definition 7 (Graph)**.** A graph consists of the following data:

- a (finite) set of vertices V;
- for each vertex $v \in V$ a (finite) set of edge ends E_v together with a distinctive element $\emptyset_v \in E_v$;
- an involution $n : \bigsqcup E_v \to \bigsqcup E_v$, giving the opposite of each edge end, whose only fixed points are the $\emptyset_v$.

Definition 8. Let $C/\bar{k}$ be a semi-stable curve. Then its associated graph $\Gamma(C)$ is constructed as follows. Its set of vertices is the set of irreducible components of C. Besides the $\emptyset_v$, for each singular (nodal) point P of C there are two edge ends, sent to each other by n: one for each of the (possibly equal) components that intersect in P.

Example 9. The graph corresponding to the curve C from Examples 5 and 6 consists of three vertices C_1, C_2 and C_3. The set of edge ends for C_i is $\{C_{i,1}, C_{i,2}, C_{i,3}\}$, where $\emptyset_i = C_{i,i}$ and $n(C_{i,j}) = C_{j,i}$.

Remark 10. The $\emptyset_v$ may seem a bit arbitrary in Definition 7. They are put there to make sure that edge ends from one vertex to itself can be contracted, as they should in Example 6. One could also consider curves with marked points and consider edge ends linked to themselves as marked points. This might lead to a more natural interpretation.

Now, we are ready for the next main statement.

Theorem 11. *Let $C/\bar{k}$ be a semi-stable curve and let $G \subset \mathrm{Aut}_{\bar{k}}(C)$ be a finite group. Then there exists a semi-stable curve $D/\bar{k}$, which is the categorical quotient of C by G (in the category of schemes). Moreover, $\Gamma(D)$ is the categorical quotient of $\Gamma(C)$ by G (in the category of graphs).*

3 Galois covers and deformation

Let us first give a very general definition of a Galois cover of schemes.

Definition 12. Let $f : A \to B$ be an affine morphism of noetherian schemes and let G be a finite group of automorphisms of A. Then f is called a *G-Galois cover* if:

(i) for each open $U \subset B$ we have $\mathcal{O}_B(U) = \mathcal{O}_A(f^{-1}(U))^G$;

(ii) each $g \in G \setminus \{\mathrm{id}\}$ does not act as the identity on any of the irreducible components of A.

Example 13. Let $C/\bar{k}$ be a semi-stable curve and let $G \subset \mathrm{Aut}_{\bar{k}}(C)$ be a finite group of order coprime to p, satisfying property (ii) from Definition 12. Then the quotient $q : C \to D$ of C by G (cf. Theorem 11) is a G-Galois cover.

In the setup of Example 13 we want to add some extra condition that we need later. Locally at the completion the nodal singularities of C are of the form $\bar{k}[[a,b]]/(ab)$. We like to require the following for our action of G on C.

Definition 14. In the setup of Example 13, the action of G on C is called *exemplary* if for each node $P \in C$, there exists an identification $\widehat{\mathcal{O}}_{X,P} \cong \bar{k}[[a,b]]/(ab)$ such that the action of $\mathrm{Stab}(P) \subset G$ can be lifted to $\bar{k}[[a,b]]$, such that $\mathrm{Stab}(P)$ fixes ab.

Now we can state the main theorem of this section.

Theorem 15. *Suppose that we are in the setup of Example 13, that the action of G on C is exemplary and that C is ordinary. Then there exists a G-Galois cover $\mathfrak{q} : \mathcal{C} \to \mathcal{D}$ over $\bar{k}[[X]]$ and isomorphisms $\mathcal{C}_s \cong C$ and $\mathcal{D}_s \cong D$, where $s \in \mathrm{Spec}(\bar{k}[[X]])$ is the special point, such that*

- *the cover $\mathfrak{q}$ reduces to q on the special fibre (w.r.t. to the isomorphisms),*
- *the generic fibres $\mathcal{C}_\eta$ and $\mathcal{D}_\eta$ are smooth,*
- *$\mathcal{C}$ is ordinary.*

Proof outline. The idea is to extend the local cover

$$\mathrm{Spec}(\bar{k}[[a,b]]/(ab)) \cong \widehat{\mathcal{O}}_{C,P} \to \widehat{\mathcal{O}}_{D,q(P)}$$

for singular $P \in C$ to a cover over $\bar{k}[[X]]$ by extending the action of $\mathrm{Stab}(P)$ on $\bar{k}[[a,b]]/(ab)$ to $\bar{k}[[a,b,X]]/(ab - X)$. For this we need the exemplarity. Then we can glue these local deformations using a result of Saidi (see [Sai12]). □

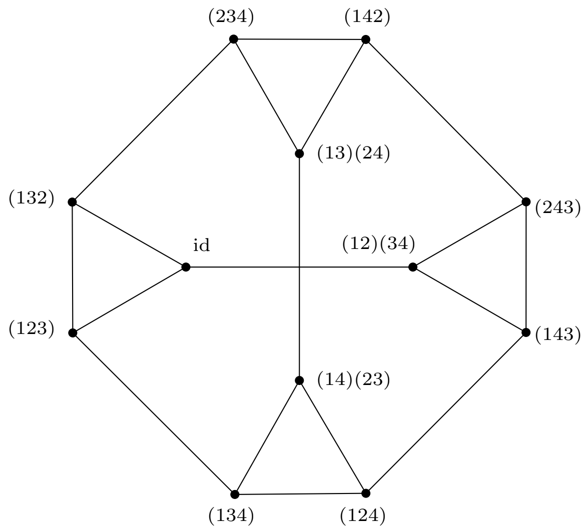
4 Examples

In this section we will discuss a few examples that illustrate how to use Theorem 15 in practice.

Example 16. Let $(E_1, O_1), (E_2, O_2)$ over $\bar{k}$ of characteristic $p > 2$ be two ordinary elliptic curves. They give rise to C_2-covers $\varphi_1 : E_1 \to \mathbb{P}^1$ and $\varphi_2 : E_2 \to \mathbb{P}^1$. Now consider the semi-stable curve E obtained by gluing E_1 and E_2 in O_1 and O_2 respectively, and the curve C obtained by gluing two copies of $\mathbb{P}^1$ in $\varphi_1(O_1)$ and $\varphi_2(O_2)$ respectively. Then we get a natural Galois cover $\varphi : E \to C$ and by deforming it and taking the generic fibre, we get an ordinary hyperelliptic curve of genus 2 over $\mathbb{P}^1$ over $\bar{k}((X))$.

Remark 17. There are certain specialisation techniques that allow us to find an ordinary hyperelliptic curve of genus 2 over $\bar{k}$ from this curve over $\bar{k}((X))$.

Example 18. Let G be a group generated by two elements h_1 and h_2 such that h_1 has order 2 and h_2 has higher order, e.g. A_4 with generators $(12)(34)$ and (123). Then we can consider the graph Γ whose vertices are the elements of G and with (single) edges between g and gh_1, gh_2 and gh_2^{-1} for each $g \in G$.



The graph for the group $G = A_4$ *with generators* $h_1 = (12)(34)$ *and* $h_2 = (123)$.

Now we can construct the curve C over $\bar{k}$ of characteristic coprime to $|G|$ by taking a copy of $\mathbb{P}^1$ for each vertex and glue the components in order to get $\Gamma = \Gamma(C)$. The group G naturally acts on this curve, as an automorphism of $\mathbb{P}^1$ is determined exactly by determining the images of three distinct points.

As all $\mathbb{P}^1$'s are ordinary, C is ordinary. Deforming this curve and then taking its generic fibre gives a G-cover of an elliptic curve over $\bar{k}((X))$.

Other examples which can be realised are: an ordinary D_n-cover of $\mathbb{P}^1$ and an ordinary A_5-cover of $\mathbb{P}^1$.

References

[FvdG04] C. Faber, G. van der Geer, Complete subvarieties of moduli spaces and the Prym map. *J. Reine Angew. Math.* **573** (2004), 117–137.

[GlPr05] D. Glass, R. Pries. Hyperelliptic curves with prescribed p-torsion. *Manuscripta Math.* **117** (2005), 299–317.

[MaMa99] G. Malle, B. H. Matzat, *Inverse Galois Theory.* Springer Verlag, Berlin Heidelberg (1999).

[Sai12] M. Saidi, Fake liftings of Galois covers between smooth curves. *Galois-Teichmuller theory and arithmetic geometry, Advanced Studies in Pure Mathematics* (2012), Tokyo, Mathematical Society of Japan, 457–501.