

Fundamental Groups in Characteristic p

Pete L. Clark

October 25, 2006

1 Introduction

Fundamental groups and Galois groups: Let X/k be a smooth, complete connected curve over an algebraically closed field k . We have defined the étale fundamental group $\pi_1(X/k)$ (in this lecture I abuse notation by ignoring geometric basepoints) as the \varprojlim of automorphisms of finite étale connected covers $Y \rightarrow X$. Recall also that every fundamental group can be interpreted as a Galois group: $\pi_1(X/k) = \text{Gal}(k(X)^{\text{unr}}/k(X))$, the Galois group of the maximal everywhere unramified extension of the function field $k(X)$. So it appears that a fundamental group is a special kind of Galois group. On the other hand, consider the process of *puncturing* the curve: write $X' = X - C$, C a finite set of points, so that X'/k is an affine curve. In this case we get $\pi_1(X - C) = \text{Gal}(k(X)^{C\text{-unr}}/k(X))$, the maximal extension ramified only at the points of C . Since every finite Galois cover of X is ramified at only finitely many points, the Galois group itself is obtained as a limit of fundamental groups via the puncturing process. To put this in a more picturesque way:

Theorem 1 (*Zen*) $\text{Gal}(k(X)^{\text{sep}}/k(X)) = \pi_1(X - X)$, the fundamental group of the curve punctured everywhere.

To summarize, when contemplating the fundamental group of an affine curve, it is often profitable to view it as the collection of generically unramified covers of the completed curve which are allowed to ramify at the “points at infinity.” Moreover, we expect to see Galois theory arising in our study of fundamental groups.

Now, recall how Romyar computed geometric fundamental groups in characteristic 0:

Theorem 2 (SGA 1) *Let S/k be a connected, finite-type scheme. Let k'/k be an algebraically closed extension field.*

- a) $\pi_1(S \otimes_k k') \rightarrow \pi_1(S/k)$ is surjective.
- b) If S is proper or if $\text{char}(k) = 0$, $\pi_1(S \otimes_k k') \cong \pi_1(S)$.
- c) if $k \hookrightarrow \mathbb{C}$ is a field embedding, then $\pi_1(S/k) \cong \pi_{1,\text{top}}(\widehat{S(\mathbb{C})})$.

The goal of this talk is to give some insight into why b) and c) *fail* for affine curves in characteristic $p > 0$. In particular, the problem of computing the fundamental group in the geometric case is sufficiently challenging that we (= the mathematicians of the world) are not yet ready to consider the case of k non-algebraically closed and the associated representation of G_k into the outer automorphism group of the fundamental group.

2 Complete curves

Throughout the rest of these notes, all curves are smooth and connected, and k denotes some algebraically closed field of characteristic p . We begin with the simplest possible question: What is the fundamental group of the projective line?

Theorem 3 $\pi_1(\mathbb{P}^1/k) = 0$.

First proof: In fact, there is a Riemann-Hurwitz formula valid for finite separable morphisms (a fortiori for étale covers) in characteristic p , which in the unramified case becomes the familiar $2 - 2g(Y) = d(2 - 2g(X))$ (see Hartshorne, IV.2 for a nice discussion).

In some sense, a more enlightening answer is provided by the following (significantly harder) result of Grothendieck:

Theorem 4 *Let C/k be a complete curve of genus g . Then there is a surjection $\Gamma_{g,0} \rightarrow \pi_1(C/k)$. In particular, $\pi_1(C/k)$ can be generated topologically by $2g$ generators.*

Sketch proof: Step 1 is the following result from SGA 1:

Theorem 5 *Let A be a complete Noetherian local ring with residue field k (remark: such an A always exists; we could e.g. take the ring of Witt vectors with coefficients in k). Let X_0/k be a smooth projective variety such that $H^2(X_0, \mathcal{O}_{X_0}) = H^2(X_0, \Omega_{X_0/k}^\vee) = 0$. Then there exists X/A a smooth projective scheme such that $X \otimes_A k \cong X_0$.*

Step 2: In particular, if X_0/k is a curve, 2-dimensional cohomology of coherent sheaves vanishes on it and we can lift X_0 to some X/A . We write X_s for the special fibre (which we were calling X_0), X_η for the generic fibre, and $X_{\overline{\eta}}$ for the geometric generic fibre. Now we have the following diagram:

$$[\pi_1(X_\eta)]\pi_1(X_{\overline{\eta}})e, \text{tspsse}\pi_1(X_s)s, r\alpha\pi_1(X_\eta)e\pi_1(X)$$

Here the diagonal map is just the composite of the left map and the bottom map. In fact the rightmost map, *alpha* is an isomorphism [see Orgogozo-Vidal], which enables us to define the *specialization* map *sp* by inverting α . The theorem (due to Grothendieck) is now that the specialization map is surjective. This completes the proof sketch.

An example to show that sp is not always an isomorphism: let E/k be an elliptic curve. It is part of the basic theory of abelian varieties [Mumford] that every etale cover is given by a separable isogeny. Composing any isogeny $E' \rightarrow E$ with its dual, we see that it is enough to consider the multiplication-by- n maps, so that $\pi_1(E/k) = \varprojlim_n E[n](k) = \prod_{l \neq p} T_l(E) \times T_{p,et}(E)$. Here $T_{p,et}(E)$ is the etale part of the Tate module of E , so is isomorphic to \mathbb{Z}_p^e , where e is the p -rank of E , i.e. 1 or 0 according to whether E is ordinary or supersingular. In no case is $e = 2$, which is what we see from characteristic zero. Remark: Indeed, working now with a curve C/k of any genus at least one, it is a fundamental result that $\pi_1(C/k)^{ab} \cong T(J(C))$ (see for example, Serre's *Groupes Algébriques et Corps de Classes*), and a similar argument to the above shows that the specialization map is never surjective (even) on the abelianization of π_1 .

On the other hand, from the above examples, it looks as if it is only the elements of p -power order in π_1 that are screwing us up. Indeed, for any profinite group G , let $G^{\not p}$ be the maximal prime-to- p quotient of G . Then:

Theorem 6 (*Grothendieck*) *The specialization map induces an isomorphism $\pi_1(X_{\bar{\eta}})^{\not p} \xrightarrow{\sim} \pi_1(X_s)^{\not p}$.*

We end our discussion of complete curves here, even though there is certainly more to be said. Very soon, however, we will find the state of our knowledge in this case to be enviable.

3 Affine curves

Question 7 $\pi_1(\mathbb{A}^1/k) = ???$

If one doesn't know any better, the guess $\pi_1(\mathbb{A}^1/k) = 0$, in analogy to the characteristic 0 case, might be made. In fact we can show that this is very far from the truth:

Proposition 8 $\pi_1(\mathbb{A}^1/k)$ *is not topologically finitely generated.*

Proof: It will be enough to exhibit a cover of \mathbb{A}^1/k with Galois group $(\mathbb{Z}/p\mathbb{Z})^n$ for all n , or equivalently, putting $q = p^n$, to exhibit a cover with Galois group \mathbb{F}_q . To do this we introduce the Artin-Schreier isogeny: $\phi_q : \mathbb{A}^1/k \rightarrow \mathbb{A}^1/k, x \mapsto x^q - x$. Due to the magic of characteristic p , this is a group homomorphism. Since its differential is -1 , which is an isomorphism on cotangent spaces, ϕ_q is etale. Since k is algebraically closed, it is surjective, and it follows that it is finite etale. Clearly the automorphism group of the cover is given by the kernel of ϕ_q , which is \mathbb{F}_q , qed.

Can we say anything in the direction of bounding the size of $\pi_1(\mathbb{A}^1/k)$? We can: for C/k an affine curve, say the points at infinity are the points $\overline{C} - C$, i.e. those points at which we punctured the completed curve to get C . We

can define the *tame fundamental group* $\pi_1(C)^{\text{tame}}$ as the inverse limit over all automorphisms of covers of the completed curve which are unramified over C and tamely ramified at all points at infinity. Clearly $\pi_1(C)^{\text{tame}}$ is a quotient of the full $\pi_1(C)$. It is for this quotient that we recover the considerations of the previous section:

Theorem 9 (*Grothendieck*) *There exists a canonical specialization map $sp : \pi_1(C_{\bar{\eta}})^{\text{tame}} \rightarrow \pi_1(C/k)^{\text{tame}}$ which is a surjection. Moreover the map induced by the specialization map on the prime-to- p quotients is an isomorphism:*

$$\pi_1(C_{\bar{\eta}})^{\not p} \xrightarrow{\sim} \pi_1(C/k)^{\not p}.$$

Applying this result in the case of the affine line, we see that the tame fundamental group is trivial, and indeed the maximal prime-to- p -quotient is trivial. Note well that for a group G , it is a much *weaker* condition to say $G^{\not p} = 1$ than to say G is a p -group. We analyze this a bit:

For any profinite group G , let $p(G)$ be the subgroup generated by all the p -Sylows of G , so $p(G)$ is normal in G and $G/p(G) = G^{\not p}$. We say that G is *quasi- p* if $G = p(G)$, i.e. if $G^{\not p} = 1$. Obviously every p -group is quasi- p . The converse is true for the class of groups with a normal p -Sylow, e.g. nilpotent groups and especially for abelian groups. It is certainly *not* true in general that quasi- p groups are p -groups: the symmetric group S_n is quasi-2 for all n (and not a 2-group for n at least 3), and $SL_n(\mathbb{F}_p)$ is quasi- p and not p for all p .

In the 1950s, Abhyankar conjectured the following, which in view of what we seen, is the most ambitious possible claim.

Conjecture 10 (*Abhyankar*)

- a) *Any finite quasi- p group arises as a quotient of $\pi_1(\mathbb{A}^1/k)$.*
- b) *More generally, if C/k is an affine curve of genus g and $n > 0$ punctures, then a finite group G arises as a quotient of $\pi_1(C/k)$ iff $G^{\not p}$ has free rank $\leq 2g+n-1$.*

Abhyankar’s conjecture was proven in the case of the affine line by Raynaud in 1993, and shortly thereafter in full generality by Harbater. Much use is made of the techniques of rigid analytic geometry. It is also very important to remark that the work of Raynaud/Harbater still does not “compute” $\pi_1(\mathbb{A}^1/k)$ for us; it only tells us what the finite quotients are. (By analogy, one can see after a first algebra course that the cyclotomic extensions and their subfields exhibit abelian extensions of \mathbb{Q} with any prescribed finite abelian group as Galois group, but this is much weaker than what we understand as classfield theory for \mathbb{Q} .)

Having laid out the basic results, I’d like now to look at some special cases of the conjecture, again in the \mathbb{A}^1/k case. Especially, there are interesting connections with the classfield theory of the complete field $k((t))$.

4 Digression on Witt vectors

The abelian case of Abhyankar's conjecture is especially easy, since, as we remarked above, quasi- p -abelian groups are p -groups. We have already shown how to realize $(\mathbb{Z}/p\mathbb{Z})^n$ as a Galois covering group of the affine line. If we could further realize $(\mathbb{Z}/p^a\mathbb{Z})^n$ for any a , then by basic Galois theory we will be able to get every abelian p -group. This realization is done in a very elegant way in Serre's *Groupes algebriques et corps de classes* (and is taken from work of Rosenlicht). We will just sketch the construction here as an advertisement for the book. First, let W_a/\mathbb{F}_p be the ring-scheme of Witt vectors of length a , i.e. as a scheme W_a/\mathbb{F}_p is just the a -fold product of the affine line, but has a functorial addition and multiplication law given by "universal" polynomials. By basechange, we can view W_a as being a commutative groupscheme over \mathbb{F}_q , and as such it has an Artin-Schreier isogeny $\phi_q : x \mapsto Fr(x) - x$, where $Fr(x)$ is the q -Frobenius map. As in the $a = 1$ case, ϕ_q gives exhibits W_a as a covering of itself with Galois group equal to $W_a(\mathbb{F}_q)$, which as an additive group is isomorphic to $(\mathbb{Z}/p^a\mathbb{Z})^n$. Now Rosenlicht constructs a morphism of schemes (not of groupschemes!) $\mathbb{A}^1 \rightarrow W_a$; we can use this map to pullback the Artin-Schreier covering to a covering $Y \rightarrow \mathbb{A}^1$:

$$Y \xrightarrow{\phi_q} W_a \xrightarrow{\phi_q} \mathbb{A}^1 \xrightarrow{\phi_q} W_a$$

To construct the morphism, we say that W_a is the generalized Jacobian of \mathbb{P}^1 corresponding to the modulus $\mathfrak{m} = m \cdot [\infty]$. More plainly, there exists an equivalence relation on the degree 0 divisor group of \mathbb{A}^1 : we mod out

by principal divisors congruent to 1 modulo $m \cdot [\infty]$ (i.e. by rational functions f such that $f - 1$ vanishes to order at least m at ∞ (this is a quotient of local unit groups at infinity, so should be reminiscent of local classfield theory!) One then shows that this divisorclassgroup has a natural algebraic structure, and that as an algebraic group it is isomorphic to W_a .

5 $\pi_1(\mathbb{A}^1/k)$ depends on k

In this section we will exploit the etale cohomology of the Artin-Schreier map, and as a result see that the fundamental group of the affine line depends upon the particular algebraically closed field k chosen.

View $\phi : x \mapsto x^p - x$ as a morphism $\phi : \mathbb{G}_a \rightarrow \mathbb{G}_a$. We then have an exact sequence of etale sheaves on $\text{Spec } k$:

$$0 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{G}_a \xrightarrow{\phi} \mathbb{G}_a \longrightarrow 0.$$

Basechanging to any $X = \text{Spec } A$ an affine k -scheme and taking etale cohomology, we get immediately

Theorem 11 *We have $H_{et}^1(X, \mathbb{F}_p) = \text{Ker}(\phi : A \rightarrow A)$, $H_{et}^1(X, \mathbb{F}_p) = \frac{A}{\phi A}$, and $H_{et}^q(X, \mathbb{F}_p) = 0$ for all $q \geq 2$.*

Applying this with $A = k[t]$, we get $H_{et}^1(\mathbb{A}^1/k, \mathbb{F}_p) = \text{Hom}(\pi_1(\mathbb{A}^1/k), \mathbb{F}_p) = \frac{k[t]}{\phi k[t]}$. But we can give an additive section $\psi : \frac{k[t]}{\phi k[t]} \rightarrow k[t]$ of the quotient map via the system of representatives $\sum_{N>0, (N,p)=1} a_N t^N$. In this way we see that the cardinality of $\text{Hom}(\pi_1(\mathbb{A}^1/k), \mathbb{F}_p)$ is that of a countably infinite-dimensional k -vector space, i.e. of k . To summarize, as we enlarge the cardinality of our algebraically closed field k , we get a larger (infinite) cardinality even of \mathbb{F}_p -covers of the affine line.

6 Links with the Galois group of $k((t))$

We are going to outline a relationship between $\pi_1(\mathbb{A}^1/k)$ and the absolute Galois group G_K , where $K = k((1/t)) (\cong k((t)))$. En route to this we will see that every finite p -group can be realized as a Galois covering group of the affine line (which generalizes the considerations of Section 4).

Consider the map $\Psi : \text{Spec } K \rightarrow \mathbb{A}^1$ given on rings as the evident inclusion $\Psi^* : k[t] \rightarrow k((1/t))$. We remark that one can view this map as giving some kind of formal basepoint at infinity (note, however, that it is actually the generic point of \mathbb{A}^1/k which is the image of Ψ); we will not attempt (or need) to make this notion precise.

Theorem 12 *The map Ψ^* induces an isomorphism*

$$H_{et}^1(\mathbb{A}^1/k, \mathbb{F}_p) \xrightarrow{\sim} H_{et}^1(\text{Spec } K, \mathbb{F}_p).$$

Proof: By Theorem 11, we need only show that the inclusion of rings $k[t] \hookrightarrow k((1/t)) = k[t] \oplus t^{-1}k[[t^{-1}]]$ induces a bijection on the Artin-Schreier quotients. Indeed, the Artin-Schreier map preserves the displayed direct sum decomposition, and since $\phi(t^{-1}k[[t^{-1}]])$ coincides with the restriction to the maximal ideal of the étale endomorphism of the local ring $k[[t^{-1}]]$, by definition of étale we must have $\phi(t^{-1}k[[t^{-1}]]) = t^{-1}k[[t^{-1}]]$.

Proposition 13 ([Gille, p.220]) *Let X/k be either a connected affine scheme or a complete curve. Then*

- a) $H^q(\pi_1(X), \mathbb{F}_p) \xrightarrow{\sim} H_{et}^q(X, \mathbb{F}_p)$ for all q .
- b) $cd_p(\pi_1(X)) = cd_p(\pi_1(X)^{(p)}) \leq 1$, so in particular $\pi_1(X)^{(p)}$ is a free pro- p -group. We omit the proof, which is not so hard. Part a) comes down to the Leray spectral sequence, and part b) uses facts about Galois cohomology of pro- p -groups developed in Serre's *Cohomologie Galoisienne*. In any event, we therefore have a homomorphism

$$\pi_1(\Psi)^{(p)} : G_K^{(p)} \rightarrow \pi_1(\mathbb{A}^1/k)^{(p)}$$

between two free pro- p -groups which induces an isomorphism on $H^1(\mathbb{F}_p)$. Using another result of Galois cohomology (which says, morally, that $H^1(\mathbb{F}_p)$ is a good cotangent space for free pro- p -groups), we may conclude

Theorem 14 $\pi_1(\Psi)^{(p)} : G_K^{(p)} \rightarrow \pi_1(\mathbb{A}^1/k)^{(p)}$ is an isomorphism.

If we consider the exact sequence

$$1 \rightarrow I_p \rightarrow G_K \rightarrow \lim_{\leftarrow (N,p)=1} \mu_N k \rightarrow 1$$

, I_p being the wild inertia, we see that G_K is in one sense larger than $\pi_1(\mathbb{A}^1/k)$, namely it has nontrivial prime-to- p -quotients. On the other hand, every quotient of G_K has a normal p -Sylow, whereas this is not the case for $\pi_1(\mathbb{A}^1/k)$.

Remark: As one might suspect, one can identify G_K with a certain quotient of $\pi_1(\mathbb{G}_m/k)$, namely those covers $f : Y \rightarrow \mathbb{G}_m$ such that

a) the pullback by some Kummer map

$$f \circ [N] : Y \rightarrow \mathbb{G}_m \xrightarrow{t \mapsto t^N} \mathbb{G}_m$$

is unramified at 0, and hence can be viewed as a cover of \mathbb{A}^1 ;

b) such that $\text{Aut}(f)$ has a normal p -Sylow.

For the proof, see [Gille, *Le groupe fondamental sauvage d'une courbe affine*].