COMPUTING A GALOIS CLOSURE

FRANÇOIS GATINE

1. Statement

Let K be a field of characteristic 0 containing a primitive p-th root of unity ζ. Let $F = K(t)$ with t an indeterminate, let $y = t^{1/p}$ be a p-th root of t. Let $L = F((1+y)^{1/p})$, then the Galois closure of L/F is the extension M/F generated by elements

$$(1+\zeta^i y)^{1/p}, \qquad 0 \le i \le p-1.$$

In other words, M decomposes the polynomial $P = (x^p - 1)^p - t \in F[x]$. We are interested in computing $[M : F]$, as well as the Galois group of this extension.

Proposition 1. *We have $[M : F] = p^{p+1}$, and*

$$\mathrm{Gal}(M/F) = (\mathbb{Z}/p\mathbb{Z})^p \rtimes \mathbb{Z}/p\mathbb{Z}$$

where $\mathbb{Z}/p\mathbb{Z}$ acts on $(\mathbb{Z}/p\mathbb{Z})^p$ via cyclic permutations of the coordinates.

We provide a (mostly) geometric proof[1].

2. Proof

Notice that $F = K(t)$ is the function field of the curve $S := \mathbb{P}^1_K$. Thus any finite extension K'/K corresponds to a finite branched connected cover S'/S; the extension is Galois if and only if the cover is too. The Kummer extension $F(y)/F$ corresponds to the Galois cover

$$\begin{aligned} f : C := \mathbb{P}^1_K &\to S \\ z &\mapsto z^p \end{aligned}$$

totally ramified at 0 and ∞. Similarly, for all $0 \le i \le p-1$ the extension $F((1+\zeta^{-i}y)^{1/p})/F(y)$ corresponds to the branched cover

$$\begin{aligned} \pi_i : C_i := \mathbb{P}^1_K &\to C \\ z &\mapsto \zeta^i(z^p - 1) \end{aligned}$$

totally ramified at $-\zeta^i$ and ∞. Let $X \to S$ be the Galois closure of any $\pi_i \circ f$, which factors through $C \to S$. Define $Z_i = C_0 \times_C \cdots \times_C C_i$, then

Claim 1. *We have $X \simeq Z_{p-1}$ as covers of C.*

Assume for now that this identification holds, we deduce Proposition 1 from it. Observe that for ay $1 \le i \le p-1$, the branched Galois cover

$$Z_i = Z_{i-1} \times_C C_i \to Z_{i-1}$$

is connected (otherwise X would not be connected) and has degree p, as base change of $C_i \to C$ which has degree p. We find that $X \to C$ has degree p^p, and with the additional p-cover $C \to S$, we have $[M : F] = \deg(X/S) = p^{p+1}$. It remains to compute $\mathrm{Gal}(M/F)$.

Lemma 1. *We have $\mathrm{Gal}(M/F(y)) = \mathrm{Gal}(X/C) \simeq (\mathbb{Z}/p\mathbb{Z})^p$.*

Proof. The cartesian diagram of connected Galois covers

$$\begin{array}{ccc} Z_i & \longrightarrow & C_i \\ \big\downarrow & & \big\downarrow \\ Z_{i-1} & \longrightarrow & C \end{array}$$

[1] I was asked this question by Felipe Gambardella, who had solved it using valuations on the ring $F[t]$ and its extensions. This note is essentially a repeat of his argument, from a geometric standpoint.

shows that $\mathrm{Gal}(Z_i/C) = \mathrm{Gal}(Z_{i-1}/C) \times \mathrm{Gal}(C_i/C)$ so $\mathrm{Gal}(X/C) \simeq (\mathbb{Z}/p\mathbb{Z})^p$ by induction. □

Consider now the short exact sequence

$$1 \longrightarrow \mathrm{Gal}(M/F(y)) \longrightarrow \mathrm{Gal}(M/F) \longrightarrow \mathrm{Gal}(F(y)/F) \longrightarrow 1.$$

A generator of $\mathrm{Gal}(F(y)/y) \simeq \mathbb{Z}/p\mathbb{Z}$ is $\sigma : y \to \zeta y$. The element $\tilde{\sigma} \in \mathrm{Gal}(M/F)$ defined by

$$\tilde{\sigma}((1+\zeta^i y)^{1/p}) = (1+\zeta^{i+1}y)^{1/p}$$

defines a section $\mathrm{Gal}(F(y)/F) \to \mathrm{Gal}(M/F)$ by sending σ^j to $\tilde{\sigma}^j$, which induces an identification

$$\mathrm{Gal}(M/F) = \mathrm{Gal}(M/F(y)) \rtimes \mathrm{Gal}(F(y)/Y) \simeq (\mathbb{Z}/p\mathbb{Z})^p \rtimes (\mathbb{Z}/p\mathbb{Z}).$$

From there it is straightforward to compute that $\mathbb{Z}/p\mathbb{Z}$ acts on $(\mathbb{Z}/p\mathbb{Z})^p$ by cyclic permutations of the coordinates.

All that remains is to prove Claim 1. Recall

Fact 1. *Let Y be a smooth connected curve over K. There is an equivalence between smooth connected branched covers of Y and regular finite field extensions of its function field $K(Y)$.*

Such a cover $Y' \to Y$ corresponds to the field extension $K(Y')/K(Y)$. If $Y'' \to Y$ is a second cover, then the extension $K(Y')K(Y'')/K(Y)$ corresponds to the cover defined by a connected component of $Y' \times_Y Y''$. In particular, looking at degrees we see that $Y' \times_Y Y''$ is connected if and only if $K(Y')$ and $K(Y'')$ are linearly disjoint extensions of $K(Y)$.

Lemma 2. *Let Y be a smooth connected curve over K, let a, b be two closed points of Y. Let $Y' \to Y$ (resp. $Y'' \to Y$) be a smooth connected branched cover of Y which is unramified (resp. ramified) at a, and ramified (resp. ramified) at b. Then $Y' \times_Y Y''$ is connected.*

Proof. We may assume that $Y = \operatorname{Spec} R$ is the spectrum of a Dedekind ring with only two closed points (given by a and b). Denote R' and R'' the finite ring extensions defined by Y' and Y'', let K' and K'' be their fraction fields. Observe that the assumption on ramification implies that $K' \cap K'' = K$, and so that K' and K'' are linearly disjoint. □

Lemma 2 shows that all covers $Z_i \to C$ are connected. Thus $Z_{p-1} \to X$ is a connected cover with function field extension M/F which is the Galois closure of L/F. This shows Claim 1.