<table>
<thead>
<tr>
<th>Title</th>
<th>Lecture I: Liftings of Galois covers of smooth curves (Rigid Geometry and Group Action)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Matignon, Michel</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 1998, 1073: 98-105</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1998-12</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/62597">http://hdl.handle.net/2433/62597</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>
Lecture I : Liftings of Galois covers of smooth curves

by Michel Matignon

These two lectures are a report on the lifting problem of Galois covers of smooth curves from char. $p > 0$ to char. 0. The references are listed as [G-M 1], [G-M 2], [M].

The first lecture will focus on lifting problems, the main results are a local global principle and the positive answer to the lifting problem for $p^2$-cyclic covers generalizing a former result in $p$-cyclic case due to F.Oort, T.Sekiguchi, N.Suwa.

The second lecture will focuss on the geometry of order $p$-automorphisms of an open disc over a $p$-adic field.

I would like to thank Professors T.Sekiguchi and N.Suwa for inviting me to Japan and for organizing this symposium which gives me the opportunity for this report. I am very grateful to T.Ito and M.Yato for writing the TeX version of my notes of the lectures.

Finally I would like to dedicate this work to Michel Raynaud who has so much influenced us.

Notations:

$k$ is an algebraicaly closed field of char. $p > 0$.
$R$ is a complete DVR finite over $W(k)$.
$\pi$ is a uniformising parameter for $R$.
$FrR =: K \subset K^{alg}$ is endowed with the unique polongation of the valuation $v$.

0. Introduction

Let $C/k$ be a smooth irreducible complete curve of genus $g$.

We are interested in the following:

Global lifting problem. Let $G \subset Aut_k C$. Is it possible to find an $R$ as above and $C/R$ finite a relative smooth R-curve such that $G \subset Aut_R C$ and $(C, G)$ gives $(C, G) \mod \pi$; i.e. we have a commutative diagramm:

\[
\begin{array}{ccc}
\text{Aut}_k C & \subset & \text{Aut}_R C \\
\downarrow & \uparrow & \\
G & \rightarrow & \\
\end{array}
\]
It is possible to formulate this in terms of $G$-covers. Let

\[
\begin{array}{ccc}
C & \xrightarrow{f} & C/G = D \\
\downarrow & & \downarrow \\
\Spec k & \sim & \Spec R
\end{array}
\]

$I_y = \text{Inertia group at } y \in C$; then

\[I_y \subset \text{Aut}_k \hat{O}_{C,y} \simeq \text{Aut}_k k[[z]]\]

In the lifting process then $I_y$ is lifted as $I_y \subset \text{Aut}_R \hat{O}_{C,y} \simeq \text{Aut}_R R[[Z]]$.

**Results.**

- If $(|G|, p) = 1$ the answer is yes by Grothendieck (SGA I). In fact he proves that the answer is yes under the condition that the ramification in $C \xrightarrow{f} C/G$ is tame; i.e. $I_y$ has prime to $p$ order for any $y \in C$.

So the main problem occurs when the ramification is wild. Recall that any $p$-group can occur as an inertia group moreover in infinitely many ways.

- If $|G| > 84(g(C) - 1)$ the answer is no due to a trivial contradiction using Hurwitz bound for automorphism group in char $0$.

- If $G$ is cyclic of order $pe$ (resp. $p^2e$) with $(e, p) = 1$, the answer is yes for $R$ large enough namely $W(k)[\zeta_{(n)}]$ (resp. $W(k)[\zeta_{(2)}]$), where $\zeta_{(n)} \in K_{\text{alg}}$ is a primitive $p^n$-th root of 1. See [O-S-S] resp. [G-M1].

We have seen that the global lifting problem induces the:

**Local lifting problem.** Let $G \subset \text{Aut}_k k[[z]]$; can we find $R$ as above and a commutative diagram

\[
\begin{array}{ccc}
\text{Aut}_k k[[z]] & \leftarrow & \text{Aut}_R R[[Z]] \\
\downarrow & & \downarrow \\
G & \leftarrow &
\end{array}
\]

I. Local global principle

We prove the following

**Theorem ([G-M1]).** The global lifting problem over $R$ for any $(C, G)$ is equivalent to the local lifting problem over $R$ for any $(\hat{O}_{C,y}, I_y \subset \text{Aut}_{k} \hat{O}_{C,y})$ where $y$ runs the branch locus of $C \xrightarrow{f_s} C/G$.

**Proof.** Sketch

We use rigid analytic geometry

First Step: Lift $D/k$ as $D/R$ (SGA I). Let $B_r :=$ the branch locus for $f_s$. 
The lifting is unique up to isomorphism. In fact the morphism $f_{(K)}$ extends (use Krasner-lemma) at the boundary of the formal fiber at $x$. And the germ of prolongation is unique so it is a Galois $I_y$-cover.

The main problem is so to compactify in a Galois way. The local lifting problem says that we have Galois cover of open disks lifting

$$\text{Spec } k[[z]] \rightarrow \text{Spec } k[[z]]^{I_y} = k[[t]]$$
Second Step: We prove a gluing lemma using Newton’s theorem (the main point is that the extension \(k((z))/k((t))\) is separable !). Conclude to the algebraicity using GAGA.

II. Local lifting for order \(p\) or \(p^2\) automorphisms

It is possible to “lift” \(k[[z]]/k[[t]]^G = k[[t]]\) in a Galois way as \(A/R[[T]] = A^G\) for some \(A\) finite normal over \(R[[T]]\)(see Garuti [Ga]). The main problem is here to do this with a smooth \(A/R\) i.e. with good reduction over \(R\).

For this purpose we need a numerical criteria for smoothness which is a particular case of a formula due to K.Kato (Duke M.J. 81 [Ka]).

**Theorem (Kato).** Let \(A/R[[T]]\) be a finite normal local ring such that \(A/\pi\) is reduced. We assume that \(k((z)) = \text{Fr}(A/\pi)/k((t))\) is separable and \(\text{rank}_{R[[T]]}A = \dim_{k((t))} k((z)) = n\). Let \(d_\sigma\) be the degree of the different in the extension \(k((z))/k((t))\). and \(d_\eta\) be the degree of the different in the extension \(A \otimes_R K/R[[T]] \otimes_R K\). Then \(A\) is smooth over \(R\) i.e. \(A \simeq R[[Z]]\) iff \(d_\eta = d_\sigma\).

**Application.**

Order \(p^n\) case: We have Sekiguchi-Suwa [S-S] theory which shows the existence of a generic way to deform geometrically and in a Galois way a \(p^n\)-cyclic cover over \(\text{Spec} k((z)) \rightarrow \text{Spec} k((z))^{<\sigma>}\). In order to deform in a smooth way we should be able to calculate different; this is the main obstacle at the present to go further than \(n = 2\).

Order \(p\) case ([O-S-S]):

Let \(\sigma\) be an order \(p\) \(k\)-automorphism of \(k[[z]]\). By Artin-Schreier theory (abbreviation A-S) there exists \(x \in k((z))\) such that \(\sigma(x) = x + 1\) and \(x^p - x = f(t)\). After a translation on \(x\) and a change of parameter we can take

\[
\begin{align*}
\sigma(x) &= x + 1 \\
x^p - x &= \frac{1}{m}
\end{align*}
\]

for some \(m\), \((m,p) = 1\); we call \(m + 1\) the Hasse-conductor or Weierstrass degree for \(\sigma\).

Note that \(z := x^{-\frac{1}{m}}\) is a parameter and that \(\sigma(z) = z(1 + z^m)^{-\frac{1}{m}} = z(1 - \frac{1}{m}z^m + \cdots)\).

By O-S-S theory we deform the A-S isogeny

\[
\begin{align*}
0 &\longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{G}_a \longrightarrow \mathbb{G}_a \longrightarrow 0 \\
x &\mapsto x^p - x
\end{align*}
\]

to

\[
\begin{align*}
0 &\longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{G}^{(\lambda)} \longrightarrow \mathbb{G}^{(\lambda^p)} \longrightarrow 0 \\
x &\mapsto \frac{(\lambda x + 1)^{p-1}}{\lambda^p}
\end{align*}
\]

Let \(R = W(k)[\zeta_{(1)}], \lambda = \zeta_{(1)} - 1\). Let \(A\) be the integral closure of \(R[[T]]\) in \(F := \text{Fr}R[[T]](X)\) where \(\frac{(\lambda x + 1)^{p-1}}{\lambda^p} = \frac{1}{m}\) (this is a \(p\)-cyclic cover of \(\mathbb{P}^1\) ramified in \(T = 0\) and \(T^m = -\lambda^p\) inside the open disc \(|T| > 1\). So the generic different is

\[d_\eta = (m + 1)(p - 1)\]

which is known to be the different in the extension \(k((z))/k((t))\). It is possible here to show that \(Z := X^{-\frac{1}{m}}\) is a parameter for the open disc over \(R\) then \(\sigma(Z) := \zeta Z(1 + (\zeta Z)^m)^{-\frac{1}{m}}\) lifts \(\sigma\).
Remarks. 1. We could consider a lifting
\[
\frac{(\lambda X + 1)^p - 1}{\lambda^p} = \frac{1}{(T - t_1) \cdots (T - t_m)}
\]
with \(t_i \in \pi R\), 2 by 2 distinct then \(d_\eta = 2m(p - 1) > d_\sigma\). This cover has bad reduction and induces at the special fiber a cover with a cusp.

2. We will see in the next lecture that there are other non equivalent ways to lift an order \(p\)-automorphism.

Order \(p^2\) case: Artin-Schreier-Witt theory (abbreviation A-S-W) gives

\[
\begin{align*}
0 & \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow W_2 \longrightarrow F^{-1} W_2 \longrightarrow 0 \\
(x_1, x_2) & \mapsto (x_1^p - x_1, x_2^p - x_2 - c(x_1^p, -x_1))
\end{align*}
\]

where \(c(x_1^p, -x_1) := \frac{(x_1^p - x_1)^p - (x_1^{p^2} + (-x_1)^p)}{p} \in \mathbb{Z}[[x_1]]\). After some translation we can find an Artin-Schreier representant

\[
\begin{cases}
\frac{x_1^p - x_1}{p} = \frac{1}{m_1} \\
x_2^p - x_2 - c(x_1^p, -x_1) = f_2 \left( \frac{1}{t} \right)
\end{cases}
\]

in such a way that \(f_2 \left( \frac{1}{t} \right) \in k \left[ \frac{1}{t}, x_1^p - x_1 \right] \) is written in a way which gives the different of the extension (see [G-M1] lemma 5.1).

Our main contribution was first to give an explicit formula for deforming A-S-W as the existence was proved in [S-S]; and secondly to provide in each case a lifting with the good different. We prove

**Theorem ([G-M1]).** Let \(\lambda := \zeta_{(1)} - 1, \pi := \zeta_{(2)} - 1, \mu = \log_p(1 + \pi)\) the truncated logarithm in degree \(p\) (\(\zeta_n\) is a compatible system of \(p^n\) th roots of 1).

\[
(y_1, y_2) = \left( \frac{(\lambda x_1 + 1)^p - 1}{\lambda^p}, 1 - \frac{\mu x_1^p}{\lambda^p} \right)
\]

lifts A-S-W isogeny. (*)

Application:

\[
\begin{cases}
y_1 = \frac{1}{m_1} \\
y_2 = 0
\end{cases}
\]

lifts the cover above with \(f_2 \left( \frac{1}{t} \right) = 0\).

In order to prove the smoothness it is sufficient to proceed by stage in the \(p^2\)-cyclic extension. We have only to look at the second stage above the open disc \(|x_1| > 1\) (\(x_1^{\frac{1}{m_1}}\) is a parameter for the open disk in the first stage). It is easy to bound the generic different

\[(*)\text{In particular} \left| (\exp_p \mu x_1^p) - (\lambda x_1 + 1) \exp_p \mu y_1 \right|^{1/p} \text{ lifts the cocycle } c(x_1^p, -x_1)\). In proving this we have to prove the congruence } \mu \nu - \lambda - p \frac{\nu_1^{p^2}}{\lambda^{p^2}} \equiv 0 \mod \pi^{p^2+1}.
$d_\eta \leq [1 \text{ (for } \infty \text{ pt}) + 1 \text{ (for } x_1 = -\frac{1}{\lambda}) + d_{\eta}^1 \text{Exp}_p(\mu^p y_1)](p-1) = (2 + p(p-1))(p-1).

The special differential is $d_s = (m_2 + 1)(p-1)$ where $m_2 = d^2 c(x_1^p, x_1) = p(p-1) + 1$. So $d_\eta \leq d_s$ and as always $d_\eta \geq d_s$ we conclude.

The general $p^2$-cyclic extension needs a good choice of $f_2$ in such a way we can read the different and for the lifting other involved formulas.

III. Other $p$-groups and Galois Inverse type conjecture

a) Obstructions to local lifting for $G = (\mathbb{Z}/p\mathbb{Z})^2$.

**Theorem**([G-M1]). Let $G = \langle \sigma_1, \sigma_2 \rangle \cong (\mathbb{Z}/p\mathbb{Z})^2 \subset \text{Aut}_k k[[z]]$ then we have the picture with $p + 1$ intermediate $p$-cyclic extensions with Hasse conductors in the lower level $m_1 + 1 \leq m_2 + 1 = m_3 + 1 = \ldots = m_{p+1} + 1$ and in the upper level $m'_1 = m_2 p - m_1(p-1)$ and $m'_i = m_1$ for $i > 1$.

\[
\begin{array}{c}
\text{k[[z]]} \\
\downarrow m'_1 \\
\text{k[[z_1]]} \\
\downarrow \ldots \\
\text{k[[z_{p+1}]}} \\
\downarrow m_{p+1} \\
\text{k[[t]]}
\end{array}
\]

If there is a local lifting then $p|m_1 + 1$ (this is stronger than Hasse-Arf congruences). Moreover, if

\[
\begin{array}{c}
\text{Spec } R[[Z_1]] \\
\downarrow f_1 \\
\text{Spec } R[[T]] \\
\downarrow f_2 \\
\text{Spec } R[[Z_2]]
\end{array}
\]

are liftings then the branch locus for $f_1(K)$ and $f_2(K)$ meet in $\frac{m_1+1}{p}(p-1)$ and this condition is an iff condition.

The proof is elementary, the congruence can be seen as follows. We know that $m'_1 + 1$ is the number of fix points for a lifting for $\sigma_1$, then the lifting of $\sigma_2$ acts freely on the $m'_1 + 1$ points (because the inertia groups are at most cyclic of order $p$) and so $p|m'_1 + 1$ and so $p|m_1 + 1$. The end is an application of Kato's criterion.

**Remark.** The congruences above have been generalised by J.Bertin [Be] for general groups. Moreover he proves that the Artin representation can be expressed in term of the regular representation and a representation of permutation (given by the action on the ramification locus) in particular it is rational.

b) We end this lecture by what we call:

"**Inverse Galois type property**".

Let $G$ be a $p$-group; we say that $G$ has the "Inverse Galois type property" if there is an $R$ as above and a commutative diagram

\[
\begin{array}{c}
\text{Aut}_k k[[z]] \xrightarrow{\text{Aut}_R R[[z]]} \\
\downarrow \\
G
\end{array}
\]
This is in some respect a strong form of Abhyankar's conjecture ([Ra]) and we prove Theorem ([M]). Abelian $p$-groups of type $(p, \ldots, p)$ have the Galois type property.

**Proof.** In case $p = 2$, $G = (\mathbb{Z}/2\mathbb{Z})^3$. The general case will be considered in next lecture.

**Lemma.** The elliptic curve

$$y^2 = (1 + \alpha_1 x)(1 + \alpha_2 x)(1 + (\sqrt{\alpha_1} + \sqrt{\alpha_2})^2 x)$$

where $\alpha_i \in \mathbb{Z}_{2}^{ur}$ are such that $\alpha_1 \alpha_2 (\alpha_1 + \alpha_2) \neq 0$ mod 2, has potentially good reduction at 2, an equation for the special fiber is

$$z^2 - z = \alpha_1 \alpha_2 (\alpha_1 + \alpha_2) s^3$$

(a supersingular elliptic curve as an étale 2-cyclic cover of $\mathbb{A}^1$).

**Proof.** Write

$$y^2 = 1 + (\alpha_1 + \alpha_2 + (\sqrt{\alpha_1} + \sqrt{\alpha_2})^2) x + \alpha_1 \alpha_2 (\sqrt{\alpha_1} + \sqrt{\alpha_2})^2 x^2 + \alpha_1 \alpha_2 (\sqrt{\alpha_1} + \sqrt{\alpha_2})^2 x^3.$$

Let $\gamma = \alpha_1 + \alpha_2 + \sqrt{\alpha_1} \sqrt{\alpha_2}$ then

$$y^2 = (1 + \gamma x)^2 + \alpha_1 \alpha_2 (\sqrt{\alpha_1} + \sqrt{\alpha_2})^2 x^3.$$

Call

$$\left\{ \begin{array}{l}
x = 2^{\frac{3}{2}} s \\
y = 1 + \gamma x - 2z \\
\end{array} \right.$$

For the theorem consider the 3 elliptic curves

$$y_1^2 = (1 + \alpha_1 x)(1 + \alpha_2 x)(1 + (\sqrt{\alpha_1} + \sqrt{\alpha_2})^2 x)$$

$$y_2^2 = (1 + \alpha_2 x)(1 + \alpha_3 x)(1 + (\sqrt{\alpha_2} + \sqrt{\alpha_3})^2 x)$$

$$y_3^2 = (1 + \alpha_3 x)(1 + \alpha_1 x)(1 + (\sqrt{\alpha_3} + \sqrt{\alpha_1})^2 x)$$

where $\alpha_i \in \mathbb{Z}_{2}^{ur}$ and if $A_1 = \alpha_1 \alpha_2 (\alpha_1 + \alpha_2)$, $A_2 = \alpha_2 \alpha_3 (\alpha_2 + \alpha_3)$, $A_3 = \alpha_3 \alpha_1 (\alpha_3 + \alpha_1)$ then if

$$\prod (\varepsilon_1 A_1 + \varepsilon_2 A_2 + \varepsilon_3 A_3) \neq 0 \quad (\varepsilon_1, \varepsilon_2, \varepsilon_3) \in (\mathbb{Z}/2\mathbb{Z})^3 - (0,0,0)$$

they have simultaneously good reduction and the normalisation of the composition over $\mathbb{P}_{2}^{ur}$ is a $(\mathbb{Z}/2\mathbb{Z})^3$-cover with good reduction and gives mod 2 the $(\mathbb{Z}/2\mathbb{Z})^3$ étale cover of the affine line generated by the three equations

$$\left\{ \begin{array}{l}
z_1^2 + z_1 = A_1 s^3 \\
z_2^2 + z_2 = A_2 s^3 \\
z_3^2 + z_3 = A_3 s^3 \\
\end{array} \right..$$

Calculate $d_s = 4(2 - 1)(1 + 2 + 2^2), d_\eta = \#\{\text{branch points}\} 2^2(2 - 1)$ and the brach locus is $\{\infty, \alpha_1, \alpha_2, \alpha_3, (\sqrt{\alpha_i} + \sqrt{\alpha_j})_{i \neq j}\}$ so $d_s = d_\eta$. 

104
IV. References


**Remark.** (see [G-M2] II. 3.3.3) The "Inverse Galois type conjecture" is true for $p^n$-cyclic groups. The proof uses Lubin-Tate formal groups, we will indicate the method in the next lecture.

M. Matignon
UPRS-A 5467 CNRS
351, cours de la Libération
France

Mathématiques Pures de Bordeaux
Université de Bordeaux I
33405 – Talence, Cédex
email: matignon@math.u-bordeaux.fr