p-adic Representations of the K-rational Geometric Fundamental Group

1. Introduction

Let K be a number field (or any fin. gen. field)

C/K a (smooth...) curve of genus g

$F = \kappa(C)$ its function field ($\Rightarrow F/K$ regular)

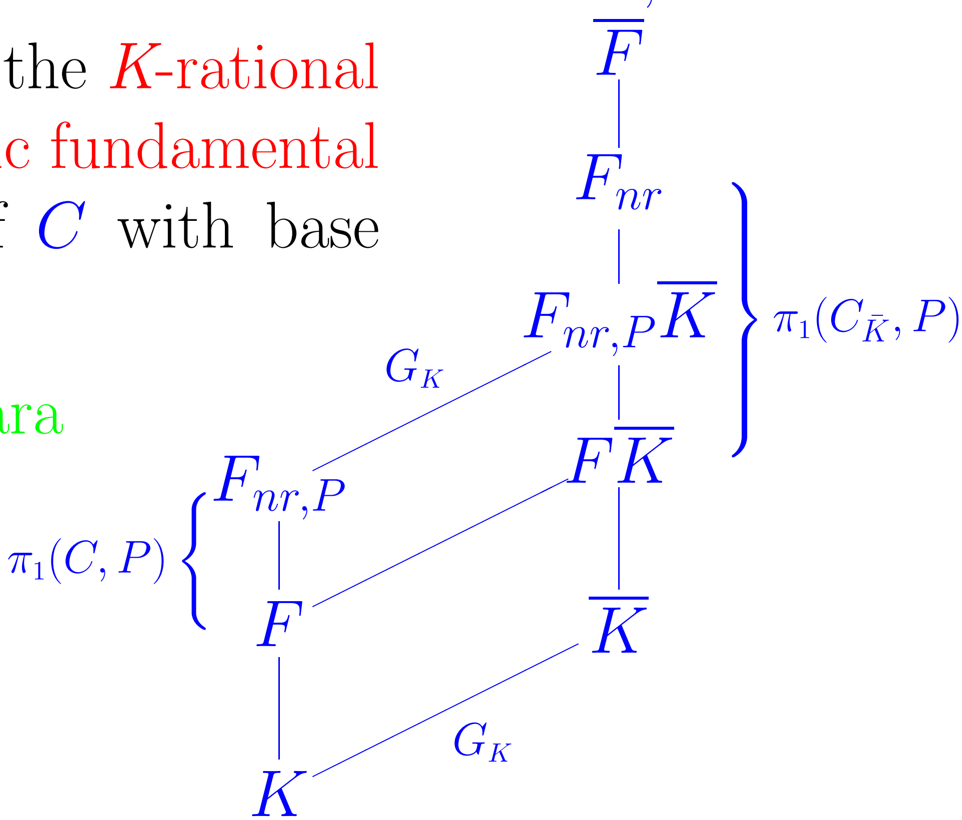
$P \in C(K)$ a K-rational point

Definition Let $F_{nr,P}$ be the field generated by the finite unramified Galois extensions F'/F such that P splits completely in F'. Then its Galois group

$$\pi_1(C,P) = \mathrm{Gal}(F_{nr,P}/F)$$

is called the K-rational geometric fundamental group of C with base point P.

→Y. Ihara



2. Some Results about $\pi_1(C, P)$

–joint work with G. Frey and H. Völklein

Note: $g = 0 \Rightarrow \pi_1(C, P) = \pi_1(C_{\bar{K}}, P) = \{1\}$.

Theorem 1 (Merel) There is c_K such that for all elliptic curves E/K and $P \in E(K)$ we have

$$|\pi_1(E, P)| \leq c_K.$$

Mazur: $c_{\mathbb{Q}} = 12$.

Proposition 1: $\pi_1(C, P)^{ab}$ is always finite.

Theorem 2: Let $K \supset \mathbb{Q}(i)$ (or $K \supset \mathbb{F}_p(i)$). Then for every $g \geq 3$ there exist (many!) curves C/K of genus g with a point $P \in C(K)$ such that $\pi_1(C, P)$ is infinite.

Remark: The above situation for $\pi_1(C, P)$ is very similar to that of the fundamental group $\pi_1(K)$ of a number field K:

$\pi_1(K) = \{1\}$ for some K's ($K = \mathbb{Q}, \mathbb{Q}(i)$, etc.)

$|\pi_1(K)^{ab}| = h(K)$ is always finite.

$\pi_1(K)$ is often infinite ($\longrightarrow$ Class field towers: e.g. $K = \mathbb{Q}(\sqrt{-30030})$.)

3. p-adic Representations

So far, the theory for $\pi_1(C, P)$ and for $\pi_1(K)$ seem to be very similar. ($\rightarrow$ M. Rosen (Hilbert class fields).) However, this picture changes if we look at p-adic representations, particularly in view of the Fontaine-Mazur Conjecture:

Fontaine-Mazur Conjecture (1993): Any p-adic representation

$$\rho : \pi_1(K) \rightarrow \mathrm{GL}_n(\mathbb{Q}_p)$$

factors through a finite quotient group.

In particular:

Any quotient group of $\pi_1(K)^{(p)}$, which is a p-adic analytic group, is finite.

Remark: The above conjecture is actually only a special case of a more general conjecture (also due to Fontaine and Mazur):

The Main F-M Conjecture: Every irreducible p-adic representation on G_K which is potentially semistable (at all $v|p$) comes from algebraic geometry, i.e. is isomorphic to a subquotient of an étale cohomology group $H^q(X_{\overline{K}}, \mathbb{Q}_p(r))$, for some projective smooth variety X/K.

The analogues of these conjectures for $\pi_1(C,P)$ are false, as the following theorem and its corollary show[1]:

Theorem 2′: Let $b \in K^\times, b^4 \neq \pm 1$, and put $c = 1+b^4$ and $a = \frac{2b^2}{c}$. (As before, $\sqrt{-1} \in K$). Let C/K be the curve defined by the equation

$$s^4 = ct(t^2-1)(t-a)g(t),$$

where $g(t) \in K[t]$ is any polynomial with

$$g(a) = 1 \quad \text{and} \quad g(0)g(1)g(-1) \neq 0,$$

and put $P = (a,0) \in C(K)$. Then the K-rational geometric fundamental group $\pi_1(C,P)$ is infinite; more precisely, for every prime $p \equiv 5 \pmod{12}$ (with $p \neq \mathrm{char}(K)$), the group $\mathrm{PSL}_3(\mathbb{Z}_p)$ is a factor of $\pi_1(C,P)$, i.e. there is a surjection

$$\rho : \pi_1(C,P) \to \mathrm{PSL}_3(\mathbb{Z}_p).$$

Corollary. In the above situation, let C_p denote the finite cover of C corresponding to a pro-p-Sylow subgroup U_p of $\mathrm{PSL}_3(\mathbb{Z}_p)$. Then for any point P' over P, the fundametal group $\pi_1(C_p,P')$ has a quotient which is isomorphic to the p-adic analytic group U_p.

[1] This also shows that J. Holden's generalization of the Fontaine-Mazur Conjecture to curves over finite fields is false as well.

4. The Basic Construction: Motivation

Basic Idea: Construct unramified extensions of F via (towers of) torsion points of abelian varieties $A/F = \kappa(C)$, i.e. look at the p-adic Galois representation

$$\rho_{A,p} : G_F = \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}(T_p(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_p).$$

Remark: In the language of Fontaine-Mazur this means that we are looking at p-adic representations that are subquotients of $H^1(X_{\overline{F}}, \mathbb{Q}_p(1))$, where X is some curve (or abelian variety) over F.

Want: A to have good reduction everywhere over C.

Criterion of Neron-Ogg-Shafarevich:

A/F has good reduction everywhere
$\Leftrightarrow F(A[m])$ is unramified over $F, \forall m \geq 1$
$\Leftrightarrow F(T_p(A)) = \bigcup F(A[p^n])$ is unramified over $F, \forall p$.

Assume this from now on.

Unfortunately: $F(A[m]) \not\subset F_{nr,P}$ for $m >> 0$, so in particular $F(T_p(A)) \not\subset F_{nr,P}$, fo all p.

For: $\zeta_m \in F(A[m]), \forall m$ but $\zeta_m \notin K$ (hence $\zeta_m \notin F_{nr,P}$), for $m >> 0$.

1^{st} Modification: In place of $\rho_{A,p}$, consider instead its associated projective representation:

$$\tilde{\rho}_{A,p} : G_F \to \mathrm{PGL}(T_p(A)) = \mathrm{Aut}(\mathbb{P}(T_p(A))),$$

i.e. consider the subfield

$$F(\mathbb{P}(T_p(A))) = F(T_p(A))^{Z(GL(T_p(A)))},$$

of $F(T_p(A))$ which is fixed by the centre Z of the group $\mathrm{GL}(T_p(A))$.

Then we have: $F(\mathbb{P}(T_p(A))) \subset F_{nr,P}$

$\overset{\text{def}}{\Leftrightarrow}$ $P \in C(K)$ splits completely in $F(\mathbb{P}(T_p(A)))$

$\Leftrightarrow$ G_K operates centrally (diagonally) on $T_p(\overline{A}_P)$,

$\overset{\text{Tate}}{\Leftrightarrow}$ $\mathrm{End}_K(\overline{A}_P) \otimes \mathbb{Q}_p = M_{2g}(\mathbb{Q}_p)$,

where $\overline{A}_P$ denotes the reduction of A at P.

Note: Here we have used the Tate Conjecture for endomorphisms of abelian varieties (which was proved by G. Faltings).

However: The theory of abelian varieties shows that this is impossible (in characteristic 0); i.e. there is no abelian variety of dimension $g \geq 1$ whose endomorphism ring is a full $2g \times 2g$ matrix algebra.

2^{nd} Modification: Look for $\mathbb{Z}_p[G_F]$-decompositions:

$$(1) \qquad T_p(A) = \bigoplus_{i=1}^{r} S_i,$$

and let $\overline{S}_i$ = image of S_i in $T_p(\overline{A}_P)$.

Then: $F(\mathbb{P}(S_i)) \subset F_{nr,P}$, for all i

$\Leftrightarrow G_K$ operates centrally on each $\overline{S}_i$

$\overset{\text{Tate}}{\Rightarrow} \overline{A}_P$ is of CM-Type.

Remark: If we assume the existence of a decomposition (1) and require the CM-type of $\overline{A}_P$ to be compatible with the $\overline{S}_i$, then the converse to the last implication is also true.

Proposition: Let A/F be an abelian variety with good reduction everywhere. If p is a prime such that we have a decomposition (1) such that G_K acts centrally on each $\overline{S}_i \subset T_p(\overline{A}_P)$, then each projective p-adic subrepresentation

$$\tilde{\rho}_{S_i} : G_F \to \mathrm{PGL}(S_i) = \mathrm{Aut}(\mathbb{P}(S_i))$$

of $\tilde{\rho}_{A,p}$ factors over $\pi_1(C, P)$, i.e. induces a homomorphism

$$\tilde{\rho}_{S_i} : \pi_1(C, P) \to \mathrm{PGL}(S_i) = \mathrm{Aut}(\mathbb{P}(S_i)).$$

5. The Basic Construction: Some Details

Aim: For $F = K(t, s)$ and P as in Theorem $2'$, construct an abelian variety A/F satisfying the hypotheses of the previous proposition.

Consider: the cyclic covering $\phi : X \to \mathbb{P}^1_F$ defined by the equation

$$y^4 = x(x^2 - 1)(x - a)^3(x - t)^2.$$

Then: 0) X has genus 4, $\exists \sigma \in \mathrm{Aut}(X)$ of order 4, and ϕ factors over the elliptic curve $E = X/\langle \sigma^2 \rangle$.

1) The Jacobian $J_X \sim E \times A$, where $A = J^{new}$ is an abelian subvariety of J_X of dimension 3.

2) σ acts on A and hence on $T_p(A)$, and if $p \equiv 1 \pmod 4$, then we have the G_F-decomposition into σ-eigenspaces

$$T_p(A) = S_1 \oplus S_2, \quad \text{where } \dim S_i = 3.$$

3) A/F has good reduction everywhere.

4) $\tilde{\rho}_{S_i} : G_F \to \mathrm{PGL}_3(\mathbb{Z}_p)$ is surjective if $p \equiv 5\ (12)$.

5) $\overline{A}_P \sim E_1 \times E_1 \times E_1$, where E_1/K is an elliptic curve with CM by $\mathbb{Q}(i)$, so $\tilde{\rho}_{S_i}$ factors over $\pi_1(C, P)$.

Proof Sketch: 0) - 2) Easy.

3) Note first that X, ϕ, A etc. are defined over $F_0 := K(t) \subset F$. By Völklein's theory of Thompson tuples, the ramification structure of $F_0(\mathbb{P}(S_i[p]))/F_0$ can be described precisely (for all $p \equiv 1\ (4)$), and so it follows from the Serre–Tate criterion that A has potentially good reduction. By analyzing the Neron model of J_X more closely, it follows that A already has good reduction over F.

4) Völklein's theory of Thompson tuples shows that $\mathrm{Gal}(F(\mathbb{P}(S_i[p]))/F) \simeq \mathrm{PGL}_3(p)$. By an argument due to Serre, it follows that $\tilde{\rho}_{S_i}$ is surjective.

5) Here we work out the structure of the fibre C_P at P of the minimal model of C in some detail. It is here that the judicious choice of c and a become important.

Remark: Most of the above program (i.e. steps 0)-4)) can be generalized to (almost arbitrary) cyclic coverings $\phi : X \to \mathbb{P}^1_{K(t)}$. In this case one works with what we call the new part J_X^{new} of the Jacobian J_X of X, i.e. the part of J_X that is orthogonal to the Jacobians of proper subcovers of ϕ.

Proof Sketch of 3):

I. Völklein's theory of Thompson tuples + choice of F

$\Rightarrow$ 1) $F(\mathbb{P}(S_i))/F$ is unramified

2) $e_P(F(A[p])/F) \le N^r$, for $p \equiv 5(12)$ and some r (indep. of p)

II. The Serre-Tate Criterion:

A/F has potentially good reduction at P

$\Leftrightarrow \exists c : e_P(F(A[m])/F) \le c$, for all m

$\Leftrightarrow \exists c : e_P(F(A[p])/F) \le c$, for ∞'ly many pr.'s p.

III. A Good reduction criterion:

Show: $F(A[p])/F$ is unramified (Ne-O-Sh).

Enough: $F(S_i[p])/F(\mathbb{P}(S_i[p]))$ is unramified (by I.)

Criterion: $S_i^I \ne \{0\} \Rightarrow F(S_i[p])/F(\mathbb{P}(S_i[p]))$ is unramified. (I = inertia group.)

Recall (Grothendieck, SGA 7_I): $T_p(A)^I \simeq T_p(\overline{A}_P^o)$, where $\overline{A}_P^o$ = connected component of the identity of the reduction of the Neron model at P.

(Thus: $T_p(A)^I = \{0\} \Leftrightarrow \overline{A}_P^o$ is unipotent, i.e. an extension of additive groups.)

Note: The above criterion applies to $A = J^{new}$ for $\overline{A}_P^o$ has a large abelian part which meets each $\overline{S}_i$.

Reference: G. Frey, E. Kani, H. Völklein, Curves with infinite K-rational geometric fundamental group. In: Aspects of Galois Theory (H. Völklein et al., eds.), LMS Lecture Notes 256 (1999), 85–118.