The K-rational Fundamental Group

1. Introduction

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

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

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

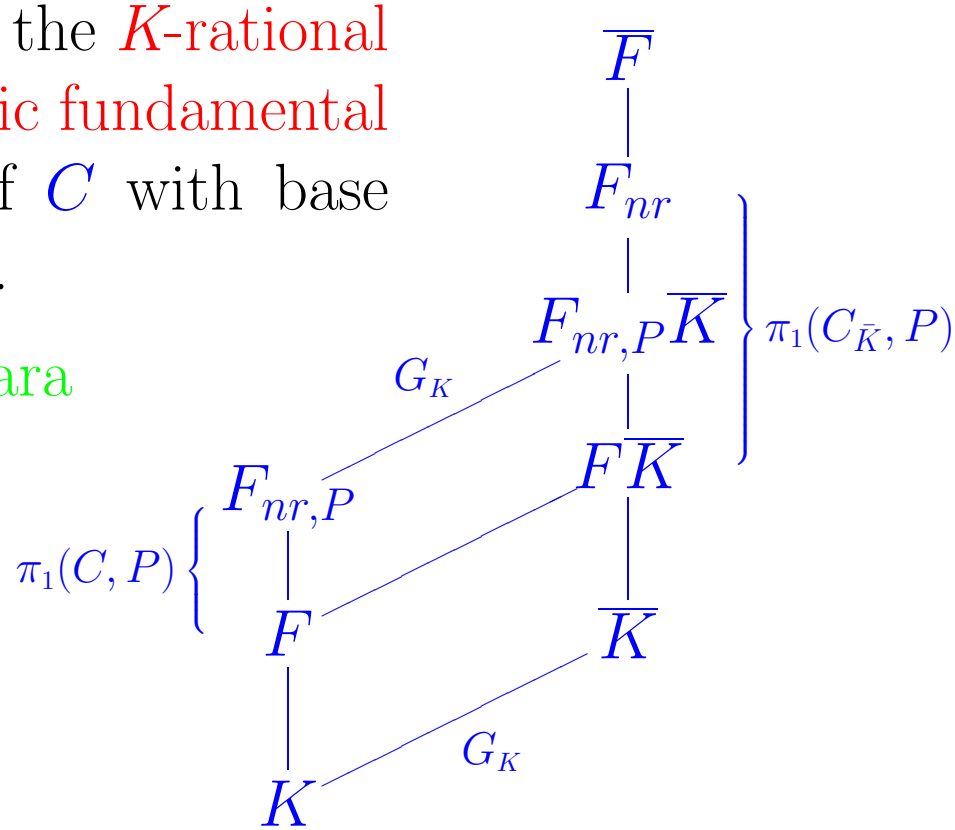
$P \in C(K)$ a K-rational point

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.

$\rightarrow$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 ($\rightarrow$ Class field towers: e.g. $K = Q(-30030.)$

3. Outline of the proof of Theorem 2

Theorem 2′: Let $b \in K^\times, b^4 \neq \pm 1$, and put $c = 1+b^4$ and $a = \frac{2b^2}{c}$. Let C/K be defined by

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

where $g(t) \in K[t]$ is any polynomial with $g(a) = 1$ and $g(0)g(1)g(-1) \neq 0$, and put $P = (a, 0) \in C(K)$. Then $\pi_1(C, P)$ is infinite; more precisely, for every prime $p \equiv 5 \pmod{12}$ (with $p \neq \mathrm{char}(K)$), the group $\mathrm{PSL}_3(p)$ is a factor of $\pi_1(C, P)$.

Step 1: If $T = \{(P_1, \ldots, P_4), (e_1, \ldots, e_4)\}$ is a given "type", construct, for each $p \equiv 5 \pmod{12}$, a $\mathrm{PSL}_3(p)$-extension $L_p/K(t)$ with ram. type T.

Consequence: if $F = \kappa(C)$ is any Galois cover of $K(t)$ with the same ramification type T, then $F_p = L_pF$ is unramified over F. (Abhyankar's Lemma).

$$\begin{tikzcd}
 & L_pF \arrow[d, dash, "\}\ \text{unramified}"] \\
L_p \arrow[ur, dash] \arrow[d, dash] & F \\
K(t) \arrow[ur, dash] &
\end{tikzcd}$$

Step 2: (hard) Investigate when a given $P \in C(K)$ with $P|P_i$ splits completely in L_pF.

4. Constructing PSL(p)-extensions

-via torsion points of Jacobians of curves over $K(t)$.

Theorem 3: Let $\tilde{C}/\tilde{K} = K(t)$ be the curve defined by

$$y^N = c(x-t_1)^{m_1}\cdots(t-t_r)^{m_r},$$

where: $t_1,\ldots,t_{r-1} \in K$ are distinct,
$t_r = t$, and $c \in K^\times$; $\zeta_N \in K$;
$\gcd(m_1,\ldots,m_r,N) = 1,\ 0 < m_i < N$,
$m_1 + \ldots + m_r \equiv 0 \pmod N$,
$m_i \neq N - m_r$, for $1 \leq i \leq r-1$.

Then the Jacobian $J_{\tilde{C}}$ of $\tilde{C}$ has an abelian subvariety $A = J^{new}$ of dimension $\frac{1}{2}\phi(N)n$, where $n = r-2$, such that for every $p \equiv 1 \pmod N$ we have:

(1) $A[p] = \oplus V_i$ is a direct sum of $\phi(N)$ irreducible $G_{\tilde{K}}$-modules V_i, each of dimension $\dim_{\mathbb{F}_p}(V_i) = n$.

(2) For each i, the extension $\tilde{L}_{p,i} = \tilde{K}(\mathbb{P}(V_i))$ is ramified over $\tilde{K}$ only at $t_1,\ldots,t_{r-1}$ with ramification order dividing N. Moreover, if $(n, p-1) = 1$, then $\mathrm{Gal}(\tilde{L}_{p,i}/\tilde{K}) \simeq \mathrm{PSL}_n(p)$.

(3) $\tilde{K}(A[p])$ is unramified over $\Pi\,\tilde{L}_{p,i}$.

Remarks: 1) J^{new} = complement of J^{old}, where:
J^{old} = sum of all Jacobians of proper subcovers of $f : \tilde{C} \to \mathbb{P}^1_{\tilde{K}}$.

2) The proof of (2) requires Völklein's theory of Thompson tuples which completely describes the ramification structure and Galois group of the extension $\tilde{L}_{p,i}/\tilde{K}$.

3) The proof of (3) uses a detailed analysis of the reduction of the Néron model of $J_{\tilde{C}}$ ($\to$ Grothendieck, SGA 7_I, Exposé IX).

Corollary. J^{new} has potentially good reduction everywhere; i.e. there is finite extension $F/\tilde{K}$ such that $J^{new} \otimes F$ has good reduction everywhere.

Remark. By imposing further (mild) restrictions on the m_i's, one can show by an inductive argument that J_C itself often has potentially) good reduction everywhere. We thus obtain many examples of curves having bad reduction at prescribed points but whose Jacobians have good reduction everywhere.

5. Thompson Tuples

Definition: A Thompson tuple is a set $\{g_1, \ldots, g_{n+1}\}$ of elements $g_i \in \mathrm{GL}_n(q)$ such that

(1) $G = \langle g_1, \ldots, g_{n+1} \rangle \leq \mathrm{GL}_n(q)$ is an irreducible subgroup;

(2) each g_i is a perspectivity (has an eigenspace of dimension $n-1$);

(3) $g_1 \cdot \ldots \cdot g_{n+1} = 1$.

Remarks. 1) Thompson tuples generalize Belyi triples (the case $n = 2$).

2) Each Thompson tuple is weakly rigid. If, in addition, we have

$$N_{GL_n(q)}(G) = G \cdot \mathbb{F}_q^*, \tag{1}$$

then the Thompson tuple is quasi-rigid.

Theorem (Völklein) Let $g_1, \ldots, g_{n+1}$ be a Thompson tuple and let $P_1, \ldots, P_{n+1} \in \mathbb{P}^1(\mathbb{C})$ be distinct points. Put $\underline{P} = (P_1, \ldots, P_{n+1})$ and $\underline{C} = (C_1, \ldots, C_{n+1})$, where C_i deotes the conjugacy class of g_i in $G = \langle g_1, \ldots, g_{n+1} \rangle$. Then we have:

(a) There is a unique Galois extension $L/\mathbb{C}(x)$ of ramification type $[G, \underline{P}, \underline{C}]$.

(b) If the tuple satisfies (1), and $L = \mathrm{Fix}(Z(G)$ denotes the fixed field of the centre $Z(G)$ of G, then the extension $L/\mathbb{C}(x)$ is defined over any subfield $K \subset \mathbb{C}$ containing all the P_i and all roots of unity of order $ord(g_i)$.

6. Study of K-rational points

In the situation of Theorem 3, suppose in addition:

$F/\tilde{K}$ is a finite Galois extension and

1) $P_0 \in \{P_1, \ldots, P_{r-1}\}$ is totally ramified in F;

2) $N | e_{F\tilde{K}}(P_0)$.

$\Rightarrow A := J^{new} \otimes F$ has good reduction $\bar{A}_P$ at $P|P_0$ (Serre-Tate).

Proposition. Let $S \subset A[p]$ be a G_F-submodule, and let $\bar{S} \subset \bar{A}_P[p]$ denote its image. If

$(\star)$ every $\bar{K}$-isogeny $\bar{\alpha}$ of the reduction $\bar{A}_P$ with kernel $\mathrm{Ker}(\bar{\alpha}) \subset \bar{S}$ is K-rational,

then P splits completely in $F(\mathbb{P}(S))$.

Theorem 4: In the situation of Theorem 2′, let $F = \kappa(C) \supset \tilde{K}$, and let $\tilde{C}/\tilde{K}$ be defined by

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

i.e. $(t_1, \ldots, t_4) = (0, 1, -1, a)$ and $(m_1, \ldots, m_5) = (1, 1, 1, 3, 2)$. Then for $P = (a, 0)$, the reduction $\bar{A}_P$ of $A = J^{new}_{\tilde{C}} \otimes F$ at P is K-isogeneous to E^3, i.e.

$$\bar{A}_P \sim E \times E \times E,$$

where E/K is the elliptic curve $y^2 = x^3 - x$. In particular, every $V_i \subset A[p]$ satisfies condition $(\star)$.

Remarks. 1) Without the judicious choice of a and c, viz. $c = 1 + b^4$ and $a = \frac{2b^2}{c}$, the above isogeny is not defined over K.

2) The proof of Theorem 4 depends on a careful analysis of the reductions of J^{new} and $J^{new} \otimes F$, and their relation to the reduction of the curve $\tilde{C}$ (which has bad reduction at P).