Questions Concerning the Regular Realizability of Groups over the Projective Line over Various Fields

Hilaf Hasson

May 19, 2011
Introduction

Temporary Motivation
Cute Topology Problem
$\mathbb{C}((t))$
$\mathbb{Q}^{un}$

Some Global Results

Global Results: Arbitrary Branch Points
Global Results: $\mathbb{Q}$-Rational Branch Points

Introducing: $\mathbb{F}_p$
Analogy
Back to $\mathbb{Q}_p^{un}$

More
Temporary Motivation

- What is the étale fundamental group of $\mathbb{P}^1_\mathbb{Q}$ minus some points?
Temporary Motivation

- What is the étale fundamental group of $\mathbb{P}_\mathbb{Q}^1$ minus some points?
- Very hard...
Cute Topology Problem

Say that we are given \( B_2(0) \setminus \{0\} \times \mathbb{P}^1_{\mathbb{C}} \setminus \{0, t, 2, 3\} \), where \( B_2(0) \) is an open disc of radius 2 in \( \mathbb{C} \) with parameter \( t \). What is its fundamental group?
Cute Topology Problem

Say that we are given $B_2(0) \setminus \{0\} \times \mathbb{P}_\mathbb{C}^1 \setminus \{0, t, 2, 3\}$, where $B_2(0)$ is an open disc of radius 2 in $\mathbb{C}$ with parameter $t$. What is its fundamental group?

Look at the fiber $t = 1$. Here we can take loops $\alpha_1, \ldots, \alpha_4$ coming up from $-3i$ and looping counter-clockwise around $0, 1, 2, 3$ respectively. These generate the fundamental group of that fiber, and the relations between the $\alpha_i$ are generated by the sole relation $\alpha_1 \ldots \alpha_4 = 1$. 
Cute Topology Problem

Say that we are given $B_2(0) \setminus \{0\} \times \mathbb{P}_{\overline{C}}^1 \setminus \{0, t, 2, 3\}$, where $B_2(0)$ is an open disc of radius 2 in $\mathbb{C}$ with parameter $t$. What is its fundamental group?

Look at the fiber $t = 1$. Here we can take loops $\alpha_1, \ldots, \alpha_4$ coming up from $-3i$ and looping counter-clockwise around 0, 1, 2, 3 respectively. These generate the fundamental group of that fiber, and the relations between the $\alpha_i$ are generated by the sole relation $\alpha_1 \ldots \alpha_4 = 1$.

$1 \to \pi_1(\mathbb{P}_{\overline{C}}^1 \setminus \{0, 1, 2, 3\}) \to \pi_1(B_2(0) \setminus \{0\} \times \mathbb{P}_{\overline{C}}^1 \setminus \{0, t, 2, 3\}) \to \pi_1(B_2(0) \setminus \{0\})(\cong \mathbb{Z}) \to 1$
Cute Topology Problem

- Say that we are given $B_2(0) \setminus \{0\} \times \mathbb{P}^1_{\mathbb{C}} \setminus \{0, t, 2, 3\}$, where $B_2(0)$ is an open disc of radius 2 in $\mathbb{C}$ with parameter $t$. What is its fundamental group?

- Look at the fiber $t = 1$. Here we can take loops $\alpha_1, \ldots, \alpha_4$ coming up from $-3i$ and looping counter-clockwise around $0, 1, 2, 3$ respectively. These generate the fundamental group of that fiber, and the relations between the $\alpha_i$ are generated by the sole relation $\alpha_1 \cdots \alpha_4 = 1$.

- $1 \to \pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, 2, 3\}) \to \pi_1(B_2(0) \setminus \{0\} \times \mathbb{P}^1_{\mathbb{C}} \setminus \{0, t, 2, 3\}) \to \pi_1(B_2(0) \setminus \{0\})(\cong \mathbb{Z}) \to 1$

- This is split, by, say, using the functoriality of $\pi_1$ and the section $t \mapsto (t, -3i)$. 

Hilaf Hasson

Questions Concerning the Regular Realizability of Groups over Various Fields
Cute Topology Problem

Say that we are given $B_2(0) \setminus \{0\} \times \mathbb{P}_C^1 \setminus \{0, t, 2, 3\}$, where $B_2(0)$ is an open disc of radius 2 in $\mathbb{C}$ with parameter $t$. What is its fundamental group?

Look at the fiber $t = 1$. Here we can take loops $\alpha_1, \ldots, \alpha_4$ coming up from $-3i$ and looping counter-clockwise around 0, 1, 2, 3 respectively. These generate the fundamental group of that fiber, and the relations between the $\alpha_i$ are generated by the sole relation $\alpha_1 \ldots \alpha_4 = 1$.

$1 \rightarrow \pi_1(\mathbb{P}_C^1 \setminus \{0, 1, 2, 3\}) \rightarrow \pi_1(B_2(0) \setminus \{0\} \times \mathbb{P}_C^1 \setminus \{0, t, 2, 3\}) \rightarrow \pi_1(B_2(0) \setminus \{0\})(\cong \mathbb{Z}) \rightarrow 1$

This is split, by, say, using the functoriality of $\pi_1$ and the section $t \mapsto (t, -3i)$.

The action in this splitting is:

$\alpha_1 \mapsto \alpha_1^{\alpha_1^{\alpha_2}}, \alpha_2 \mapsto \alpha_2^{\alpha_1^{\alpha_2}}, \alpha_3 \mapsto \alpha_3, \alpha_4 \mapsto \alpha_4$.
So \( \pi_1(B_2(0) \setminus \{0\}) \times \mathbb{P}^1_C \setminus \{0, t, 2, 3\} \) \( \cong \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \delta \mid \alpha_1 \cdots \alpha_4 = 1, \alpha_1^\delta = \alpha_1^{\alpha_1 \alpha_2}, \alpha_2^\delta = \alpha_2^{\alpha_1 \alpha_2}, \alpha_3^\delta = \alpha_3, \alpha_4^\delta = \alpha_4 \rangle \)
This is analogous to the following question: what is the étale fundamental group of $\mathbb{P}^1_{\mathbb{C}((t))} \setminus \{0, t, 2, 3\}$?
This is analogous to the following question: what is the étale fundamental group of $\mathbb{P}^1_{\mathbb{C}((t))} \setminus \{0, t, 2, 3\}$?

The (profinite completion of) the same!
This is also analogous to the following question: what is the prime-to-$p$ étale fundamental group of $\mathbb{P}^1_{\mathbb{Q}_p} \setminus \{0, p, 2, 3\}$?
This is also analogous to the following question: what is the prime-to-$p$ étale fundamental group of $\mathbb{P}^1_{Q_p \setminus \{0, p, 2, 3\}}$?

(The maximal prime-to-$p$ quotient of) the same!
Global Results: Arbitrary Branch Points

∀ finite $G \exists$ points $\{a_1, \ldots, a_r\}$ in $\mathbb{P}^1_C$ such that $\forall X_C \rightarrow \mathbb{P}^1_C$ that is $G$-Galois with branch points $\{a_1, \ldots, a_r\}$, descends to a field $K$ such that $K$ over $\mathbb{Q}$ is branched at most at the primes that divide $|G|$. 
Global Results: Arbitrary Branch Points

- \( \forall \) finite \( G \exists \) points \( \{a_1, \ldots, a_r\} \) in \( \mathbb{P}^1_{\mathbb{C}} \) such that \( \forall \mathcal{X}_{\mathbb{C}} \rightarrow \mathbb{P}^1_{\mathbb{C}} \) that is \( G \)-Galois with branch points \( \{a_1, \ldots, a_r\} \), descends to a field \( K \) such that \( K \) over \( \mathbb{Q} \) is branched at most at the primes that divide \( |G| \).

- In particular, \( \forall \) finite \( G \), \( \exists K \) such that \( G \) is realizable as a Galois group over \( K \), and \( K \) over \( \mathbb{Q} \) is branched at most at the primes that divide \( |G| \).
Global Results: Arbitrary Branch Points

∀ finite $G \exists$ points $\{a_1, \ldots, a_r\}$ in $\mathbb{P}^1_{\mathbb{C}}$ such that $\forall \chi_{\mathbb{C}} \rightarrow \mathbb{P}^1_{\mathbb{C}}$ that is $G$-Galois with branch points $\{a_1, \ldots, a_r\}$, descends to a field $K$ such that $K$ over $\mathbb{Q}$ is branched at most at the primes that divide $|G|$.

In particular, $\forall$ finite $G$, $\exists K$ such that $G$ is realizable as a Galois group over $K$, and $K$ over $\mathbb{Q}$ is branched at most at the primes that divide $|G|$.

Far-reaching goal: continue looking prime-to-$p$, and hope to construct a cover of $\mathbb{P}^1_{\mathbb{C}}$ that descends to a number field $K$ such that $K$ over $\mathbb{Q}$ has all but finitely many primes split. This will imply that $K$ is $\mathbb{Q}$.  

More immediate goal: understand locally and globally the condition that the branch points be rational.
Global Results: Arbitrary Branch Points

- \( \forall \) finite \( G \) \( \exists \) points \( \{a_1, \ldots, a_r\} \) in \( \mathbb{P}^1_{\mathbb{C}} \) such that \( \forall X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}} \) that is \( G \)-Galois with branch points \( \{a_1, \ldots, a_r\} \), descends to a field \( K \) such that \( K \) over \( \mathbb{Q} \) is branched at most at the primes that divide \( |G| \).

- In particular, \( \forall \) finite \( G \), \( \exists K \) such that \( G \) is realizable as a Galois group over \( K \), and \( K \) over \( \mathbb{Q} \) is branched at most at the primes that divide \( |G| \).

- Far-reaching goal: continue looking prime-to-\( p \), and hope to construct a cover of \( \mathbb{P}^1_{\mathbb{C}} \) that descends to a number field \( K \) such that \( K \) over \( \mathbb{Q} \) has all but finitely many primes split. This will imply that \( K \) is \( \mathbb{Q} \).

- More immediate goal: understand locally and globally the condition that the branch points be rational.
Global Results: $\mathbb{Q}$-Rational Branch Points

This more nuanced view can for example prove the following global results:

- Theorem: For any finite group $G$ such that it is generated by two elements and $Z(G)$ (for example, any simple or quasi-simple group), $\exists$ a number field $K$ such that $G$ is regularly realizable over $K$ with $\mathbb{Q}$-rational branch points and such that $K$ over $\mathbb{Q}$ is branched only at primes that divide $|G|$.
This more nuanced view can for example prove the following global results:

- Theorem: For any finite group $G$ such that it is generated by two elements and $Z(G)$ (for example, any simple or quasi-simple group), $\exists$ a number field $K$ such that $G$ is regularly realizable over $K$ with $\mathbb{Q}$-rational branch points and such that $K$ over $\mathbb{Q}$ is branched only at primes that divide $|G|$. 

- Theorem: For any finite group $G$, and for any finite set of primes $S$ that don’t divide $|G|$, $\exists$ a number field $K$ such that $G$ is regularly realizable over $K$ with $\mathbb{Q}$-rational branch points and such that $K$ over $\mathbb{Q}$ is unramified over the primes of $S$. 
Introducing: $\mathbb{F}_p$

- $\mathbb{C}((t))$ and $\mathbb{Q}^{un}_p$ are analogous because they are both cohomological dimension 1 fields with isomorphic prime-to-$p$ absolute Galois groups ($\cong \hat{\mathbb{Z}}(p)$). $\mathbb{F}_p$ also satisfies this.
Introducing: $\mathbb{F}_p$

- $\mathbb{C}(t))$ and $\mathbb{Q}_p^{un}$ are analogous because they are both cohomological dimension 1 fields with isomorphic prime-to-$p$ absolute Galois groups ($\cong \hat{\mathbb{Z}}(p)$). $\mathbb{F}_p$ also satisfies this.

- Differences: it is not the quotient field of a complete DVR, let alone of a complete DVR with an algebraically closed residue field. Further, it has very few roots of unity.
Introducing: $\mathbb{F}_p$

- $\mathbb{C}((t))$ and $\mathbb{Q}_p^{un}$ are analogous because they are both cohomological dimension 1 fields with isomorphic prime-to-$p$ absolute Galois groups ($\cong \widehat{\mathbb{Z}}(p)$). $\mathbb{F}_p$ also satisfies this.

- Differences: it is not the quotient field of a complete DVR, let alone of a complete DVR with an algebraically closed residue field. Further, it has very few roots of unity.

- The Galois action $Gal^{(p)}(\mathbb{F}_p)$ on $\pi_1^{(p)}(\mathbb{P}^1_{\mathbb{F}_p} \setminus \{a_1, ..., a_r\})$ is now much less well understood.
Introducing: $\mathbb{F}_p$

- $\mathbb{C}((t))$ and $\mathbb{Q}_p^{un}$ are analogous because they are both cohomological dimension 1 fields with isomorphic prime-to-$p$ absolute Galois groups ($\cong \hat{\mathbb{Z}}(p)$). $\mathbb{F}_p$ also satisfies this.

- Differences: it is not the quotient field of a complete DVR, let alone of a complete DVR with an algebraically closed residue field. Further, it has very few roots of unity.

- The Galois action $Gal(p)(\mathbb{F}_p)$ on $\pi_1^{(p)}(\mathbb{P}^1_{\mathbb{F}_p} \setminus \{a_1, ..., a_r\})$ is now much less well understood.

- Still, one can say a lot using this analogy!
Let $\delta$ denote a (topological) generator of $Gal(p)(\mathbb{Q}_{p}^{un})$.

For $\pi_{1}(\mathbb{P}^{1}_{\mathbb{Q}_{p}} \setminus \{a_{1}, ..., a_{r}\})$ (with $a_{1}, ..., a_{r}$ $\mathbb{Q}_{p}^{un}$-rational), in the analogy with geometry, one can observe:

$$\exists h_{i} \in \langle \alpha_{1}, ..., \alpha_{r} | \prod \alpha_{i} = 1 \rangle. \alpha_{i}^{\delta^{n}} = \alpha_{i}^{h_{i}^{n}}.$$
Let $\delta$ denote a (topological) generator of $Gal^{(p)}(\mathbb{Q}^{un}_p)$.

- For $\pi_1(\mathbb{P}^1_{\mathbb{Q}^{un}_p} \setminus \{a_1, \ldots, a_r\})$ (with $a_1, \ldots, a_r$ $\mathbb{Q}^{un}_p$-rational), in the analogy with geometry, one can observe:
  \[ \exists h_i \in \langle \alpha_1, \ldots, \alpha_r \mid \prod \alpha_i = 1 \rangle \cdot \alpha_i^{\delta^n} = \alpha_i^{h_i^n}. \]

- This implies: any Galois branched cover of $\mathbb{P}^1_{\mathbb{Q}_p}$ with $\mathbb{Q}^{un}_p$-rational branch points is already defined over $\mathbb{Q}^{un}_p \left( \frac{1}{|G|/|Z(G)|} \right)$. 
Let $\delta$ denote a (topological) generator of $\text{Gal}^{(p)}(\mathbb{Q}_{p}^{un})$.

- For $\pi_1(\mathbb{P}^1_{\mathbb{Q}_{p}} \setminus \{a_1, \ldots, a_r\})$ (with $a_1, \ldots, a_r \mathbb{Q}_{p}^{un}$-rational), in the analogy with geometry, one can observe:
  \[ \exists h_i \in \langle \alpha_1, ..., \alpha_r | \prod \alpha_i = 1 \rangle. \alpha_i^{\delta_n} = \alpha_i^{h_i^n}. \]

- This implies: any Galois branched cover of $\mathbb{P}^1_{\mathbb{Q}_{p}}$ with $\mathbb{Q}_{p}^{un}$-rational branch points is already defined over $\mathbb{Q}_{p}^{un}(p \frac{1}{|G|/|Z(G)|})$.

- For example: If the branch points are $\{0, p, \infty\}$ then the Galois action is:
  \[
  \alpha_1^{\delta_n} = (\alpha_1 \alpha_2)^n \\
  \alpha_2^{\delta_n} = (\alpha_1 \alpha_2)^n \\
  \alpha_3^{\delta_n} = \alpha_3
  \]
It is not true that any Galois branched cover over $\mathbb{P}^1_{\mathbb{F}_p}$ with $\mathbb{F}_p$-rational branch points is defined over $\mathbb{F}_p^{G/Z(G)}$. But:
It is not true that any Galois branched cover over $\mathbb{P}^1_{\mathbb{F}_p}$ with $\mathbb{F}_p$-rational branch points is defined over $\mathbb{F}_p^{|G/\mathbb{Z}(G)|}$. But:

Let $K$ be a finite field of characteristic $p$.

Theorem: $\forall G$ which is solvable and prime-to-$p$, and $\forall$ chief series $1 = G_0 \triangleleft \ldots \triangleleft G_m = G$ (where $G_i \triangleleft G$ and $G_i/G_{i-1} \cong (\mathbb{Z}/l_i\mathbb{Z})^{n_i}$ where the $l_i$’s are prime), and $\forall G$-Galois extension with $K$-rational branch points and with branch cycle description $(g_1, .., g_r)$, $X \to \mathbb{P}^1_{K}$:

Then the cover descends to the $L$ such that $(L : K(\zeta_{|G|})) = |G| \prod_i \exp(Sp_{2u_i}(\mathbb{Z}/l_i\mathbb{Z}))$ where $u_i := (1 - |G/G_i| + \frac{1}{2}|G/G_i| \sum_{j=1}^r (1 - \frac{1}{a_{ij}}))$ and $a_{ij} :=$ the order of $g_j$ in $G/G_i$. 
There is more to say, so if you're interested, ask me later..