Group III

Galois theory and the quadratic form $\mathrm{tr}(x^2)$ (according to Serre)

02.07.2010

The group $\mathrm{PGL}_2(\mathbb{F}_3)$ acts faithfully and transitively on $\mathbb{P}^1(\mathbb{F}_3)$, yielding an inclusion $\mathrm{PGL}_2(\mathbb{F}_3) \hookrightarrow S_4$.

If $f(x)$ is an S_4-polynomial with splitting field K, then the natural map $\bar{\rho} : G_{\mathbb{Q}} \to S_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$ is a *2-dimensional projective representation of* $G_{\mathbb{Q}}$.

Every representation $\bar{\sigma} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ with cyclotomic determinant comes from the 3-torsion on an elliptic curve.

Thus, $\bar{\rho}$ arises from the action of $G_{\mathbb{Q}}$ on $\mathbb{P}(E[3])$ if and only if $\bar{\rho}$ lifts to a representation $\bar{\sigma}$ with cyclotomic determinant.

$\det \bar{\rho} = \chi_{\text{cyc}}$ if and only if $\det \bar{\sigma} = \chi_{\text{cyc}}$ if and only if $\operatorname{disc} K = -3 \cdot (\text{square})$. We assume this is the case from now on.

To identify the obstruction to lifting $\bar{\rho}$, consider the long exact sequence in $G_{\mathbb{Q}}$-cohomology associated to the following sequence of trivial $G_{\mathbb{Q}}$-modules:

$$1 \to \{\pm 1\} \to \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{PGL}_2(\mathbb{F}_3) \to 1$$

$$\cdots \to \mathrm{Hom}(G_{\mathbb{Q}}, \mathrm{GL}_2(\mathbb{F}_3)) \to \\ \mathrm{Hom}(G_{\mathbb{Q}}, \mathrm{PGL}_2(\mathbb{F}_3)) \xrightarrow{\delta} H^2(\mathbb{Q}, \{\pm 1\}) \to \cdots .$$

So $\bar{\rho}$ lifts exactly when $\delta(\bar{\rho}) = 0$.

Let $E = \mathbb{Q}[x]/(f(x))$ and let q_E be the quadratic form

$$q_E(x) = \mathrm{tr}_{E/\mathbb{Q}}(x^2).$$

Serre* teaches us that $\delta(\bar{\rho})$ is related to the *Hasse-Witt invariant of* q_E, which we denote $w_2(q_E)$.

$$\delta(\bar{\rho}) = w_2(q_E) - (2) \cup (-3)$$

*J.-P. Serre, *L'invariant de Witt de la forme* tr(x^2), Comment. Math. Helv. 59 (1984), 651-676

The Hasse-Witt invariant:

The function $q_E : x \mapsto \mathrm{tr}_{E/\mathbb{Q}}(x^2)$ is a quadratic form of rank n over $\mathbb{Q}$. The set of isomorphism classes of such is $H^1(\mathbb{Q}, O(n))$.

Permutation matrices give an embedding $i : S_n \hookrightarrow O(n)$, and thus a map $i_* : H^1(\mathbb{Q}, O(n)) \to H^1(\mathbb{Q}, S_n)$.

Recall the coboundary map $\delta : H^1(\mathbb{Q}, S_n) \to H^2(\mathbb{Q}, \{\pm 1\})$.

Define the Hasse-Witt invariant by $w_2(q_E) = \delta(i_*(q_E))$.

The class $(2) \cup (-3)$:

By Kummer theory, $H^1(\mathbb{Q}, \{\pm 1\}) = \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$. We write (x) for the element of $H^1(\mathbb{Q}, \{\pm 1\})$ corresponding to $x \in \mathbb{Q}^\times$.

There is a cup product operation

$$\cup : H^1(\mathbb{Q}, \{\pm 1\}) \times H^1(\mathbb{Q}, \{\pm 1\}) \to H^2(\mathbb{Q}, \{\pm 1\}).$$

$H^2(\mathbb{Q}, \{\pm 1\})$ classifies quaternion $\mathbb{Q}$-algebras. The distinguished element of $H^2(\mathbb{Q}, \{\pm 1\})$ corresponds to $M_2(\mathbb{Q})$.

$$(x) \cup (y) = [\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij],$$

where $i^2 = x$, $j^2 = y$ and $ij = -ji$

$(2) \cup (-3)$ is the isomorphism class of quaternion $\mathbb{Q}$-algebras ramified at 2 and 3.

Let q_E^0 be the restriction of q_E to the trace-zero subspace of E.

Proposition.* $w_2(q_E) = (2) \cup (d_E)$ if and only if q_E^0 properly represents zero.

Thus, the lifting obstruction $\delta(\bar{\rho})$ vanishes if and only if there is an element $x \in \mathbb{Q}^\times$ such that

$$\mathrm{tr}_{E/F}(x) = \mathrm{tr}_{E/F}(x^2) = 0.$$

*Serre, loc. cit.