Questions in Arithmetic Algebraic Geometry

Frans Oort (Editor)

The inverse problem of Galois theory for torsors

(authors: Ph. Cassou-Noguès, T. Chinburg, B. Morin, M. J. Taylor)

Question 1.1. Suppose \( \Gamma \) is a finite group scheme over a number field \( K \). Does there exists a connected \( \Gamma \)-torsor \( X \) over \( K \)?

Example 1.2. If \( \Gamma \) is the constant group, this is the classical inverse problem of Galois theory [6].

Example 1.3. When \( \Gamma \) is the group scheme \( \mu_n = \text{Spec}(K[t]/(t^n - 1)) \) for some \( n \geq 1 \), one can take \( X = \text{Spec}(K(\beta)) \) when \( \beta^n = \alpha \in K^* \) and \( \alpha \) has order \( n \) in \( K^*/(K^*)^n \).

We now discuss one case of Question 1.1 which pertains to the work of Serre [8] and Fröhlich [5] on the Hasse-Witt invariants of quadratic forms.

Let \( K \) be any field of characteristic \( \neq 2 \). Suppose \( G \) is an abstract finite group, \( q \) is a quadratic form over \( K \) and \( \rho : G \to O(q) \) a homomorphism of group schemes from \( G \) as a constant group scheme to the orthogonal group scheme \( O(q) \) over \( K \). The Pin group \( \tilde{O}(q) \) is a central extension of group schemes

\[
1 \to \mathbb{Z}/2 \to \Gamma \to G \to 1
\]

in which \( \mathbb{Z}/2 \) is the constant group of order 2. This extension may be constructed using Clifford algebras; see [5, Appendix I] and [3, eq. (0.1)]. Pulling back this sequence via the morphism \( \rho : G \to O(q) \) gives an exact sequence of finite flat group schemes over \( K \):

\[
1 \to \mathbb{Z}/2 \to \tilde{O}(q) \to O(q) \to 1
\]

By evaluating the terms of (1) on points over a separable closure \( K^s \) of \( K \), we also obtain an exact sequence of constant groups

\[
1 \to \mathbb{Z}/2 \to \Gamma' \to G \to 1
\]

in which \( \Gamma' \) is the constant group-scheme associated to the group of points \( \Gamma(K^s) \).

We now consider Question 1.1 for the group \( \Gamma \) and also for the constant group \( \Gamma' \). A natural approach is to first construct a connected \( G \)-torsor \( T \) for \( G \) over \( K \) and to then try to lift \( T \) to a connected torsor for either \( \Gamma \) or \( \Gamma' \). Here \( T = \text{Spec}(L) \) for a field \( L \) Galois over \( K \) with \( G = \text{Gal}(L/K) \).
The problem of lifting $T$ to a $\Gamma'$-torsor $X$ was considered by Serre [8] and by Fröhlich [5]. One has an exact cohomology sequence

$$H^1(\text{Gal}(K^*/K), \Gamma') \longrightarrow H^1(\text{Gal}(K^*/K), G) \longrightarrow H^2(\text{Gal}(K^*/K), \mathbb{Z}/2) \quad (3)$$

arising from the trivial action of $\text{Gal}(K^*/K)$ on the terms of (2). The lifting question (without considering connectedness of the lift) is the same as asking if the element $[T] \in H^1(\text{Gal}(K^*/K), G)$ of the middle term of (3), is in the image of $H^1(\text{Gal}(K^*/K), T)$. Here $[T]$ denotes the cohomology class of the $G$-torsor $T$; it can be seen as a continuous group homomorphism $[T] : \text{Gal}(K^*/K) \rightarrow G$ well defined up to an inner automorphism of $G$. The obstruction to having such a lift is thus the triviality of the image $w_2(\rho \circ [T]) \in H^2(\text{Gal}(K^*/K), \mathbb{Z}/2)$ of $[T]$ under the boundary map in (3). Here $w_2(\rho \circ [T])$ is the classical second Stiefel-Whitney class associated to the orthogonal Galois representation $\text{Gal}(K^*/K)$ [7] $G \xrightarrow{\rho} \mathbb{O}(q)$.

Serre and Fröhlich determined explicit formulas for $w_2(\rho \circ [T])$. For example Serre considered the case where $G$ is the Galois group of the Galois closure of a separable extension $E/K$ of degree $n$. The natural action of $G$ on the set $\Phi = \text{Hom}_K(E, K^*)$ induces a group homomorphism from $G$ to the group of permutations of $\Phi$ that we identify with $S_n$. By composing this homomorphism with the obvious embedding $S_n \rightarrow \mathbb{O}(n)(K)$ we obtain a representation $\rho : G \rightarrow \mathbb{O}(n)$. He showed that

$$w_2(\rho \circ [T]) = w_2(\text{Tr}_{E/K}) - (d_{E/K}, 2),$$

where $w_2(\text{Tr}_{E/K})$ is the Hasse-Witt invariant of the trace form $\text{Tr}_{E/K}$, $d_{E/K}$ is the discriminant of $E$ and $(d_{E/K}, 2)$ is the Hilbert symbol in $H^2(\text{Gal}(K^*/K), \mathbb{Z}/2)$ associated to $d_{E/K}$ and 2. When $G$ is the alternating group $A_n$ and $n \geq 4$, Mestre used this approach in [7] to construct infinitely many distinct field extensions of $K = \mathbb{Q}$ with Galois group the constant group $\Gamma = \tilde{A}_n$. (Mestre in fact showed that there is a regular $\tilde{A}_n$ extension of the rational function field $\mathbb{Q}(t)$ by applying the work of Serre over the field $\mathbb{Q}(t)$.)

Consider now the problem of lifting $T$ to a (connected) torsor for the possibly non-constant group scheme $\Gamma$ appearing in (1). One can show (see [1]) that $\Gamma$ is a constant group scheme if and only if either $\rho(G)$ is contained in the alternating group $A_n \subset S_n$ or $\sqrt{2} \in K$. As above the short exact sequence

$$H^1(\text{Gal}(K^*/K), \Gamma) \longrightarrow H^1(\text{Gal}(K^*/K), G) \xrightarrow{\delta^2} H^2(\text{Gal}(K^*/K), \mathbb{Z}/2) \quad (4)$$

arising from the Galois action on the terms of (1) shows that $\delta^2(T) \in H^2(\text{Gal}(K^*/K), \mathbb{Z}/2)$ is the obstruction for the existence of a (possibly non-connected) $\Gamma$-torsor $X$ which lifts $T$. For example, in the case considered by Serre, it turns out that $\delta^2(T) = w_2(\text{Tr}_{E/K})$. So there will be a (possibly non-connected) $\Gamma$-torsor lifting $L/K$ if and only if $w_2(\text{Tr}_{E/K}) = 0$.

In the same way Mestre’s work relied on results over $\mathbb{Q}(t)$, it may be useful to work over more general schemes. For generalizations to schemes of the work of Serre and Fröhlich, see, for example, [4], [3], [2] and their references.
References


