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 Γ is a finite group scheme over a number field K. Does there exists a connected Γ-torsor X over K?*

Example 1.2. If Γ is the constant group, this is the classical inverse problem of Galois theory [6].

Example 1.3. When Γ is the group scheme $\mu_n = \mathrm{Spec}(K[t]/(t^n - 1))$ for some $n \geq 1$, one can take $X = \mathrm{Spec}(K(\beta))$ when $\beta^n = \alpha \in K^*$ and α 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 $\rho : G \to \mathbf{O}(q)$ a homomorphism of group schemes from G as a constant group scheme to the orthogonal group scheme $\mathbf{O}(q)$ over K. The Pin group $\tilde{\mathbf{O}}(q)$ is a central extension of group schemes

$$1 \to \mathbb{Z}/2 \to \tilde{\mathbf{O}}(q) \to \mathbf{O}(q) \to 1$$

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 $\rho : G \to \mathbf{O}(q)$ gives an exact sequence of finite flat group schemes over K:

$$1 \to \mathbb{Z}/2 \to \Gamma \to G \to 1. \tag{1}$$

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

$$1 \to \mathbb{Z}/2 \to \Gamma' \to G \to 1. \tag{2}$$

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

We now consider Question 1.1 for the group Γ and also for the constant group Γ'. 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 Γ or Γ'. Here $T = \mathrm{Spec}(L)$ for a field L Galois over K with $G = \mathrm{Gal}(L/K)$.

The problem of lifting T to a Γ'-torsor X was considered by Serre [8] and by Fröhlich [5]. One has an exact cohomology sequence

$$H^1(\mathrm{Gal}(K^s/K), \Gamma') \longrightarrow H^1(\mathrm{Gal}(K^s/K), G) \longrightarrow H^2(\mathrm{Gal}(K^s/K), \mathbb{Z}/2) \qquad (3)$$

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

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 $\Phi = \mathrm{Hom}_K(E, K^s)$ induces a group homomorphism from G to the group of permutations of Φ that we identify with S_n. By composing this homomorphism with the obvious embedding $S_n \to \mathbf{O}(n)(K)$ we obtain a representation $\rho : G \to \mathbf{O}(n)$. He showed that

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

where $w_2(\mathrm{Tr}_{E/K})$ is the Hasse-Witt invariant of the trace form $\mathrm{Tr}_{E/K}$, $d_{E/K}$ is the discriminant of E and $(d_{E/K}, 2)$ is the Hilbert symbol in $H^2(\mathrm{Gal}(K^s/K), \mathbb{Z}/2)$ 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 Γ appearing in (1). One can show (see [1]) that Γ 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

$$H^1(\mathrm{Gal}(K^s/K), \Gamma) \longrightarrow H^1(\mathrm{Gal}(K^s/K), G) \xrightarrow{\delta^2} H^2(\mathrm{Gal}(K^s/K), \mathbb{Z}/2) \qquad (4)$$

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

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

[1] Ph. Cassou-Noguès, T. Chinburg, B. Morin and M. J. Taylor – *On the inverse problem of Galois theory for torsors*, in preparation.

[2] Ph. Cassou-Noguès, T. Chinburg, B. Morin and M. J. Taylor – *The classifying topos of a group scheme and invariants of symmetric bundles*, Proc. Lond. Math. Soc. (3) 109 (2014), no. 5, 10931136.

[3] Ph. Cassou-Noguès, B. Erez and M. J. Taylor – *Twists of symmetric bundles*, Proc. Lond. Math. Soc. (3) 95 (2007), no. 1, 248 - 272.

[4] H. Esnault, B. Kahn and E. Vieweg – *Coverings with odd ramification and Stiefel-Whitney classes*, J. reine angew. Math. 441 (1993), 145 -188.

[5] A. Fröhlich – *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. Reine Angew. Math. 360 (1985), 84 - 123.

[6] G. Malle and B. Matzat – *Heinrich Inverse Galois theory.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[7] J.-F. Mestre – *Extensions régulières de* $\mathbb{Q}(T)$ *de groupe de Galois* $\tilde{A}_n$ J. Algebra 131 (1990), no. 2, 483495.

[8] J.-P. Serre – *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (1984), no. 4, 651 - 676.