Clay Mathematics Proceedings
Volume 8, 2009

Non-abelian descent

David Harari

Abstract. These notes are the written version of three one hour talks presented at the 2006 Clay summer school in Goettingen. They address the application of the technique of non-abelian descent for rational points to bielliptic and Enriques surfaces.

For any field k of characteristic zero, we fix an algebraic closure $\bar{k}$ of k and we set $\Gamma := \mathrm{Gal}\,(\bar{k}/k)$ (we will sometimes write Γ_k for Γ if several fields are involved). The group Γ is the inverse limit of the groups $\mathrm{Gal}\,(L/k)$ when L runs over all finite Galois extensions of k. If k is a number field, we let Ω_k denote the set of all places of k, and k_v the completion of k at v.

1. Review of non-abelian cohomology

In this section k is any field of characteristic zero. The main reference for the non-abelian cohomology of groups is Serre's book [**Ser94**], chapter I.5.

Let G be an algebraic group over k (all k-groups are assumed to be linear, but not necessarily connected), and set $\overline{G} = G \times_k \bar{k}$.

Examples :

- G finite (defining G is the same as giving the abstract finite group $G(\bar{k})$, equipped with a continuous action of Γ for the profinite topology on Γ and the discrete topology on $G(\bar{k})$), e.g., $\mathbf{Z}/n$ (cyclic group of order n with trivial Galois action), μ_n (group of nth-roots of unity in $\bar{k}$ with the natural Galois action).
- G can be a k-torus (this means that $\overline{G}$ is isomorphic to some power of the multiplicative group $\mathbf{G}_m$), e.g., the 1-dimensional torus $R^1_{K/k}\mathbf{G}_m$ defined by the affine equation $x^2 - ay^2 = 1$, where $a \in k^*$ is a constant and $K := k(\sqrt{a})$. More generally, if L is a finite extension of k with k-basis $(\omega_1, ..., \omega_r)$, the $(r-1)$ dimensional torus $R^1_{L/k}\mathbf{G}_m$ is defined by the affine equation
$$N_{L/k}(x_1\omega_1 + \cdots + x_r\omega_r) = 1$$
where $x_1, ..., x_r$ are the variables.

2000 *Mathematics Subject Classification.* Primary 11E72, Secondary 14G05, 11G35 .

- $G = \mathrm{PGL_n}$ (it is semi-simple and *adjoint*, that is, the center is trivial), $G = \mathrm{SL_n}$ (it is semi-simple and simply connected).
- $G = \mathrm{O(q)}$ (orthogonal group of a quadratic form q); this group is not connected, there is an exact sequence of k-groups

  $$1 \to \mathrm{SO(q)} \to \mathrm{O(q)} \to \mathbf{Z}/2 \to 0$$

  If the rank of q is at least 3, then SO(q) is semi-simple (but not simply connected : its universal covering is $\mathrm{Spin}(q)$); if $q = \langle 1, -a \rangle$ is of rank 2, then SO(q) is just the torus $R^1_{K/k}\mathbf{G}_m$ with $K = k(\sqrt{a})$.

We define the group $H^0(k, G) = H^0(\Gamma, G(\bar{k})) = G(k)$. For example $H^0(\mathbf{Q}, \mu_n)$ is trivial if n is odd. The *Galois cohomology set* $H^1(k, G) = H^1(\Gamma, G(\bar{k}))$ is the quotient of the set of 1-*cocycles* $Z^1(k, G)$ by an equivalence relation defined as follows. The set $Z^1(k, G)$ consists of continuous maps $f : \Gamma \to G(\bar{k})$ satisfying the cocycle condition

$$f(\gamma_1\gamma_2) = f(\gamma_1) \cdot {}^{\gamma_1}f(\gamma_2)$$

for each $\gamma_1, \gamma_2 \in \Gamma$. Two cocycles f, g are equivalent if there exists $b \in G(\bar{k})$ such that $f(\gamma) = b^{-1}g(\gamma)^{\gamma}b$ for every $\gamma \in \Gamma$. There is no canonical group structure on $H^1(k, G)$ if G is not commutative, but there is a distinguished element (denoted 0), namely, the class of the trivial cocycle. Therefore $H^1(k, G)$ is a pointed set.

Remark: The continuity assumption implies that

$$H^1(k, G) = \varinjlim_{L} H^1(\mathrm{Gal}\,(L/K), G(L))$$

where L runs over the finite Galois extensions of k.

Other definition of $H^1(k, G)$. It is also possible to define $H^1(k, G)$ as the set of isomorphism classes of *principal homogeneous spaces* (p.h.s.) of G over k. By definition such a p.h.s. is a non-empty set A, equipped with a left action of Γ and a simply-transitive right action of $G(\bar{k})$, such that the compatibility formula

$$\gamma(x.g) = \gamma(x) \cdot \gamma(g)$$

holds for every $\gamma \in \Gamma$, $x \in A$, $g \in G(\bar{k})$.

The correspondence between the two definitions goes as follows :

Let $\gamma \mapsto c_\gamma$ be a cocycle in $Z^1(k, G)$. Then define A as the p.h.s. with underlying set $G(\bar{k})$, but the *twisted* action of Γ defined by $\gamma(x) = c_\gamma \cdot {}^{\gamma}x$ (and $G(\bar{k})$ acts on the right on A). One checks that cohomologous cocycles give isomorphic p.h.s.

Conversely if A is a p.h.s. of G over k, choose a point $x_0 \in A$; then for each $\gamma \in \Gamma$, there exists a unique $c_\gamma \in G(\bar{k})$ such that $\gamma(x_0) = x_0 \cdot c_\gamma$. This defines a cocycle in $Z^1(k, G)$, and the cohomology class of this cocycle does not depend on x_0; moreover isomorphic p.h.s. also give cohomologous cocycles.

Remark: In the case we consider, any p.h.s. A is *representable* by the k-variety X defined as the quotient of $G \times_k \bar{k}$ by the action of Γ corresponding to A (the quotient exists because a group variety is quasi-projective). The k-variety X is a *k-form* of $\overline{G} := G \times_k \bar{k}$ (that is $\overline{X} \simeq \overline{G}$), and the p.h.s. A is trivial iff $X(k) \neq \emptyset$; the latter is also equivalent to the existence of $x_0 \in A$ such that $\gamma(x_0) = x_0$ for all $\gamma \in \Gamma$.

Properties of $H^1(k, G)$.

- The set $H^1(k,G)$ is covariant in G (easy with the cocycle definition), and in k (it is contravariant in $\operatorname{Spec} k$): if $k \subset L$ is an inclusion of fields, then there is a map $H^1(k,G) \to H^1(L,G)$, induced by the map $X \mapsto X \times_k L$ from isomorphism classes of k-p.h.s. to isomorphism classes of L-p.h.s.
- If

  $$1 \to G_1 \to G_2 \to G_3 \to 1$$

  is an exact sequence of k-groups (this means that the sequence of groups $1 \to G_1(\bar{k}) \to G_2(\bar{k}) \to G_3(\bar{k}) \to 1$ is exact), then there is an exact sequence of pointed sets

  $$1 \to G_1(k) \to G_2(k) \to G_3(k) \to H^1(k,G_1) \to H^1(k,G_2) \to H^1(k,G_3).$$

  In the special case when G_1 is central in G_2, this sequence can be extended with a map $H^1(k,G_3) \to H^2(k,G_1)$, but this map is not a morphism of groups in general, even if G_1 and G_3 are abelian.

Remark: "Exact sequence" of pointed sets means that the image of a map is the kernel of the following map; it can happen that a map has trivial kernel but is not injective.

Examples.

- By Hilbert's Theorem 90, we have $H^1(k,\mathrm{GL}_n) = H^1(k,\mathrm{SL}_n) = 0$.
- If T is a non-split torus, it can happen that $H^1(k,T) \neq 0$. For example if $T = R^1_{K/k}\mathbf{G}_m$, we have $H^1(k,T) = k^*/NK^*$; to see this, write T as the kernel of the norm map $R_{K/k}G_m \to \mathbf{G}_m$ (where $R_{K/k}$ stands for Weil's restriction), and use Hilbert's Theorem 90 (by Shapiro's lemma, the cohomology group $H^1(k,R_{K/k}\mathbf{G}_m)$ is isomorphic to $H^1(K,\mathbf{G}_m)$ (hence it is zero) because $(R_{K/k}G_m)(\bar{k})$ is the Galois module induced by $\bar{k}^*$ and the inclusion $\Gamma_K \to \Gamma_k$).
- Suppose G is a semi-simple, connected and simply connected group. Then $H^1(k,G) = 0$ when k is a p-adic field. For a number field k, the natural map

  $$H^1(k,G) \to \bigoplus_{v \in \Omega_{\mathbf{R}}} H^1(k_v,G)$$

  is an isomorphism (Kneser/Harder/Chernousov). These are special cases of "Serre's conjecture II" (see [**Ser94**], III.3).
- The exact sequence $1 \to \mathbf{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1$ is central. It induces an exact sequence

  $$1 \to H^1(k,\mathrm{PGL}_n) \to H^2(k,\mathbf{G}_m) = \operatorname{Br} k$$

  Actually the theory of central simple algebras implies that the map from $H^1(k,\mathrm{PGL}_n)$ to the Brauer group $\operatorname{Br} k$ is injective, its image is a subset of the n-torsion $(\operatorname{Br} k)[n]$, and the union of the images of $H^1(k,\mathrm{PGL}_n)$ in $\operatorname{Br} k$ is the whole $\operatorname{Br} k$. By class field theory, the image of $H^1(k,\mathrm{PGL}_n)$ is the whole $(\operatorname{Br} k)[n]$ when k is a p-adic field or a number field, but not in general.