Étale cohomology of fields

by Johan M. Commelin, December 5, 2013

Étale cohomology

The canonical topology on a Grothendieck topos

Let $\mathcal{E}$ be a Grothendieck topos. The *canonical topology* $\mathcal{T}$ on $\mathcal{E}$ is given in terms of coverings by the collection of all families $\{X_i \to X\}_i$ of universal effective epimorphisms, *i.e.*, for every $X' \to X$, the family $\{X'_i \to X'\}_i = \{X_i \times_X X' \to X \times_X X'\}_i$ makes the diagram

$$\mathrm{Hom}(X', Z) \to \prod_i \mathrm{Hom}(X'_i, Z) \rightrightarrows \prod_{i,j} \mathrm{Hom}(X'_i \times_{X'} X'_j, Z)$$

exact for all $Z \in \mathcal{E}$.

Theorem. —— The Yoneda embedding gives an equivalence of categories $\mathcal{E} \cong \mathrm{Sh}(\mathcal{E}, \mathcal{T})$.

Profinite groups; G-sets

A *profinite group* is by definition a group that is the limit of a diagram of finite groups. Every profinite group is the limit of the diagram of its finite quotients. A profinite group is a topological group in a natural way: the finite index normal subgroups form a fundamental system of neighbourhoods of the identity. In particular, open subgroups are of finite index.

Let G be a profinite group. Let S be a set with a G-action. The following are equivalent:

- The G-action is continuous for the discrete topology on S.
- For every point $s \in S$, the stabiliser of s is an open subgroup of G.
- The set S equals $\bigcup_H S^H$, where H runs over the open normal subgroups of G, and S^H denotes the H-invariants of S.

The category of G-sets satisfying the above equivalent condition is a Grothendieck topos, denoted G-set.

THE TOPOS $\mathrm{Sh}(\mathrm{Spec}(k)_{\text{ét}})$

Let k be a field. Fix a separable closure $\bar{k}/k$. Write G for the absolute Galois group, which is by definition the profinite group $\lim_{l/k} \mathrm{Gal}(l/k)$, where l/k runs over the finite Galois extensions contained in $\bar{k}$.

Let X/k be an étale k-scheme. Observe that G acts on $X(\bar{k})$. For every open normal subgroup $H \subset G$, we have $X(\bar{k})^H = X(\bar{k}^H)$. Consequently $X(\bar{k}) = \bigcup_H X(\bar{k})^H$, and therefore the G-action is continuous.

Theorem. —— The functor

$$\begin{aligned} \mathrm{Spec}(k)_{\text{ét}} &\to G\text{-set} \\ X &\mapsto X(\bar{k}) \end{aligned}$$

is an equivalence of categories, and the étale topology on the left corresponds to the canonical topology on the right.

Proof. We construct a quasi-inverse. Let S be a continuous G-set. Let $s \in S$ be a point. Write H for the stabiliser of s. It is a open subgroup. By elementary group theory, we have an isomorphism of G-sets $G/H \to Gs$. This shows that S is the disjoint union of finite orbits. We map Gs to $\mathrm{Spec}(\bar{k}^H)$, and since $\mathrm{Spec}(k)_{\text{ét}}$ has arbitrary disjoint unions, this define a functor $G\text{-set} \to \mathrm{Spec}(k)_{\text{ét}}$. It is left as an exercise to show that these functors are actually quasi-inverse.

Since we are working with the small étale site $\mathrm{Spec}(k)_{\text{ét}}$, every morphism in $\mathrm{Spec}(k)_{\text{ét}}$ is étale. It is then immediate that the étale topology coincides with the canonical topology. QED

Corollaries. ——

1. Every sheaf on $\mathrm{Spec}(k)_{\text{ét}}$ is representable.

2. Global sections on $\mathrm{Spec}(k)_{\text{ét}}$ correspond with G-invariants on G-set.

3. Abelian étale sheafs on $\mathrm{Spec}(k)_{\text{ét}}$ correspond to étale commutative k-group schemes, and correspond to abelian G-modules.

Group cohomology

Injective objects

Let G be a discrete group. The category G-mod consists of commutative group objects in G-set. For an object A we denote with A^G the G-invariant elements of A. Observe that G-mod is equivalent to $\mathbb{Z}[G]$-mod. Let $H \to G$ be a group homomorphism. Then there is an adjunction

$$\mathrm{Hom}_G(A, \mathrm{Ind}_H^G(B)) \equiv \mathrm{Hom}_H(A, B)$$

where $\mathrm{Ind}_H^G(B)$ is the G-module $\mathrm{Map}(G, B)^H$.

In the category of abelian groups, the injective objects are the divisible groups (abelian groups such that multiplication by n is surjective for all $n \in \mathbb{Z}_{>0}$). It follows from the adjunction that, if A is a divisible group, then $\mathrm{Ind}_1^G(A)$ is an injective object in G-mod. In particular, this gives a method to construct injective resolutions in G-mod from injective resolutions in Ab.

Computation with cochains

For $r \in \mathbb{Z}_{\geq 0}$, let P_r be the free abelian group generated by G^{r+1}. Naturally P_r comes with a G-action, by coordinatewise multiplication. Define boundary operators $d_r \colon P_r \to P_{r-1}$, by

$$d_r(g_0, \ldots, g_r) = \sum_{i=0}^{r} (-1)^i (g_0, \ldots, \hat{g}_i, \ldots, g_r),$$

where $\hat{\ }$ denotes the usual 'ommision'. One may check that $P_\bullet$ is a complex. If we denote with $\varepsilon \colon P_0 \to \mathbb{Z}$ the map that sends every basis element to 1, we can prove:

Lemma. —— The complex $P_\bullet \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ is exact.

Proof. Define $\delta_r \colon P_r \to P_{r+1}$ by

$$\delta_r(g_0, \ldots, g_r) = (e, g_0, \ldots, g_r).$$

By construction $d_{r+1} \circ \delta_r + \delta_{r-1} \circ d_r = 0$. If $d_r(x) = 0$, this implies $x = d_{r+1}(\delta_r(x))$. QED

Corollary. —— For every G-module A, we have

$$\mathrm{H}^n(G, A) \cong \mathrm{H}^n(\mathrm{Hom}_G(P_\bullet, A)).$$

Observe that $\mathrm{Hom}_G(P_r, A)$ consists of maps $\phi\colon G^{r+1} \to A$ satisfying

$$\phi(gg_0, gg_1, \dots, gg_r) = g\phi(g_0, g_1, \dots, g_r).$$

Consequently, to know the value of $\phi(g_0, g_1, \dots, g_r)$, it is enough to know the value of $\phi(g_0^1 g_0, g_0^{-1} g_1, \dots, g_0^{-1} g_r)$. Therefore, it is enough to know the value of ϕ on tuples of the form $(1, g_1', g_1' g_2', \dots, g_1' g_2' \cdot \cdot g_r')$. In this way, we obtain a map

$$\begin{aligned} G^{r+1} &\to G^r \\ (g_0, g_1, \dots, g_r) &\mapsto (g_1', g_2', \dots, g_r') \\ g_i' &= g_{i-1}^{-1} g_i, \end{aligned}$$

and this map induces an identification of $\mathrm{Hom}_G(P_r, A)$ with $\mathrm{Map}(G^r, A)$. If we write $C^r(G, A)$ for $\mathrm{Map}(G^r, A)$, we find that the induced boundary maps are given by

$$\begin{aligned} d^r\colon C^r(G, A) &\to C^{r+1}(G, A) \\ \phi &\mapsto d^r\phi, \end{aligned}$$

where

$$\begin{aligned} d^r\phi(g_1, g_2, \dots, g_{r+1}) = \quad & g_1\phi(g_2, \dots, g_{r+1}) \\ & + \sum_{i=1}^{r} (-1)^i \phi(g_1, \dots, g_i g_{i+1}, \dots, g_r) \\ & + (-1)^{r+1} \phi(g_1, \dots, g_r). \end{aligned}$$

Writing $Z^r(G, A)$ for $\ker(d^r)$, and $B^r(G, A)$ for $\mathrm{im}(d^{r-1}$, we find

$$\mathrm{H}^r(G, A) \cong Z^r(G, A)/B^r(G, A).$$

This allows for pretty explicit descriptions of $\mathrm{H}^n(G, A)$ for small n. We give the descriptions for $n = 1$. The elements of $Z^1(G, A)$ are called *crossed homomorphisms.* They are maps $\phi\colon G \to A$ satisfying

$$g\phi(h) - \phi(gh) + \phi(g) = 0.$$

On the other hand, elements of $B^1(G, A)$ are called *principal homomorphisms.* They are the maps ϕ_a for each $a \in A$, with

$$\phi_a(g) = ga - a.$$

We will now put this description to use.

Hilbert's theorem 90

If l/k is a finite Galois extension, and G its Galois group, then $\bar{l}^*$ is a G-module. The following theorem by Hilbert goes by the name

Hilbert's theorem 90. —— We have $\mathrm{H}^1(G, \bar{l}^*) = 0$.

Proof. For this proof, we need the following fact, known as *Dedekind's theorem on the independence of characters*: Let l be a field, and G a group. Every finite set of homomorphisms $\phi_i \colon G \to L^*$ is linearly independent over l. In other words, if $\sum_i c_i\phi_i(g) = 0$ for all $g \in G$, then $c_i = 0$ for all i.

With this fact we can proceed with the proof of Hilbert's theorem 90. Let $\phi \colon G \to l^*$ be a crossed homomorphism:

$$\phi(gh) = g\phi(h) \cdot \phi(g), \text{for all } g, h \in G.$$

For all $a \in l^*$, write

$$b_a = \sum_{g \in G} \phi(g) \cdot ga.$$

Apply the above fact to the finite set of homomorphisms $(g\cdot) \colon l^* \to l^*$. Since $\phi(g) \neq 0$ for all $g \in G$, the fact shows that $\sum_{g \in G} \phi(g)g$ is not the zero-map. We conclude that there is an a such that b_a is non-zero. Fix such an a, and write $b = b_a$. For all $h \in G$ we have

$$hb = \sum_{g \in G} h\phi(g) \cdot hga = \sum_{g \in G} \phi(hg)\phi(h)^{-1}hga = \phi(h)^{-1}b.$$

But this means that $\phi(h) = b/hb = hb^{-1}/b^{-1}$, which is to say that ϕ is principal. QED

Galois cohomology

For profinite groups, all the above remains true, except that we need to ask most of the maps to be continuous. In particular, we replace $C^r(G,A)$, $Z^r(G,A)$, and $B^r(G,A)$ by their subsets of continuous maps; denoted respectively $C^r_{\mathrm{cts}}(G,A)$, $Z^r_{\mathrm{cts}}(G,A)$, and $B^r_{\mathrm{cts}}(G,A)$. In particular

$$\mathrm{H}^r_{\mathrm{cts}}(G,A) \cong \frac{Z^r_{\mathrm{cts}}(G,A)}{B^r_{\mathrm{cts}}(G,A)}.$$

Observe that there is a natural map

$$\mathrm{colim}_H C^r(G/H, A^H) \to C^r_{\mathrm{cts}}(G,A),$$

given by the compositions with $G \to G/H$, and $A^H \to A$. (The colimit runs over the open normal subgroups of G.) We claim this map is an isomorphism. Injectivity is clear. For surjectivity, take a continuous map $\phi: G^r \to A$. Then $\phi(G^r)$ is discrete, and compact because G^r is compact. Hence $\phi(G^r)$ is finite, and thus contained in M^{H_0} for some normal open subgroup $H_0 \subset G$. On the other hand, for every $a \in \phi(G^r)$, the inverse image $\phi^{-1}(a)$ is open, and thus contains a translate of H_a^r, for some normal open subgroup $H_a \subset G$. Now $H_1 = \bigcap_{a\in\phi(G^r} H_a$ is an normal open subgroup of G, and by construction ϕ factors via $(G/H_1)^r$. Finally, write $H = H_0 \cap H_1$, so that ϕ lifts to a map $(G/H)^r \to A^H$. This proves surjectivity.

Because the system of normal open subgroups of G is filtered, the colimits indexed by this system commute with kernels and cokernels, and therefore with cohomology. We thus obtain:

$$\mathrm{H}^r_{\mathrm{cts}}(G, A) \cong \mathrm{colim}_H \mathrm{H}^r(G/H, A^H).$$

Corollary —— We also have a statement of Hilbert's theorem 90 for the absolute Galois group: If k is a field, with absolute Galois group G, then $\mathrm{H}^1(G, \bar{k}^*) = 0$.