Group Cohomology, Galois Cohomology and Elliptic Curves

Yonatan Harpaz

1 Group Cohomology

Let G be a group. By a G-module we mean an abelian group A with an action of G on it (i.e. homomorphism $G \to Aut(A)$). The G-modules form a category called G-Ab with morphisms being homomorphisms of groups which respect the G-action.

The category G-Ab is considerably more complicated then the (fairly simple) category Ab of abelian groups. Hence sometimes it is useful to consider functors G-$Ab \to Ab$ which simplify our G-modules into abelian groups. This functors will of course forget a lot of the information, but they will provide us with rather systematic way of understanding G-modules through abelian groups.

Two basic functors which one might consider are the quotient functor

$$A \mapsto A/G = A/ < ga - a | g \in G, a \in A >$$

and the invariants functor

$$A \mapsto A^G = \{a \in A | ga = a\}$$

These functors are dual in some sense: formally, they are the left adjoint and right adjoint of the functor $Ab \to G$-Ab which sends an abelian group A to the G-module A with trivial G-action. They are also known as taking the **limit** and **colimit** (respectively) of A with respect to G.

We will see that the first leads to construction of a **homology** theory while the latter leads to a dual notion of a **cohomology** theory. Since we will be intereseted more in the cohomology setting (which is better suited for galois groups as we will see later), we will work out the intire formalism for cohomology only, and the intereseted reader can make the analogous construction for homology.

1.1 Derived Functors

Consider a short exact sequence of G-modules:

$$0 \to A \xrightarrow{f} B \xrightarrow{p} C \to 0$$

Note that exactness of a sequence of G-modules is just the exactness of the underlining sequence of abelian groups, i.e. the image of each map is the kernel of the next.

What happens if we try to apply the invariants functor to this sequence? It is not hard to see that

$$0 \to A^G \overset{i^G}{\to} B^G \overset{p^G}{\to} C^G$$

will remain exact, where $i^G = i|_{A^G}, p^G = p|_{B^G}$. Indeed

$$ker(i|_{A^G}) = 0$$

and

$$ker(p|_{B^G}) = Im(i|_{A^G})$$

because i is injective. However, the map p^G will no longer be onto C^G in general, thus preventing the intire sequence from remaining exact.

Consider some $c \in C^G$. We know that p itself is onto, so there exists a $b \in B$ such that $p(b) = c$. But b might not be G-invariant. However, it is not intirely general either: since $p(b)$ is G-invariant, we know that $p(b) = p(gb)$ for each $g \in G$, i.e. $gb - b$ is in $ker(p) = Im(i)$. Thus for each g there exists a unique (because i is injective) element $a_g \in A$ such that $b - gb = i(a_g)$.

Let $\varphi_b : G \to A$ be the function $\varphi_b(g) = a_g$. This function measures the **obstruction** of the element b from being G-invariant, i.e. it is invariant if and only if $\varphi_b = 0$. But what if we had chosen a different $b' \in B$ such that $g(b') = c$ (rememeber that g is not injective)? Then $b - b'$ whould be in $ker(p) = Im(i)$ i.e. there would exist an $a \in A$ such that $b - b' = i(a)$. We will then have:

$$(\varphi_b - \varphi_{b'})(g) = ga - g$$

We thus wish to say that our obstruction function φ_b is defined only up to function of the form $ga - a$. Let us make this notion precise. The functions φ_b constructed above all satisfy

$$\varphi_b(g \cdot h) = i^{-1}(gh(b) - b) = i^{-1}(gh(b) - g(b) + g(b) - b) = g\varphi_b(h) + \varphi_b(g)$$

This relation is called the **coycle** relation. Define the group of **1-cocycles** in A to be the subgroup of functions $\varphi : G \to A$ satisfying

$$\varphi(g \cdot h) = g\varphi(h) + \varphi(g)$$

Note that this condition is indeed linear so we get a subgroup which we denote by $Z^1(G, A)$.

We now wish to formalize the equivalence relation we had between φ_b and $\varphi_{b'}$. Define the group of **1-coboundries** in A to be the subgroup of functions $\varphi : G \to A$ of the form

$$\varphi(g) = ga - a$$

for some $a \in A$. This condition also defines a subgroup which we call $B^1(G, A)$. It is straight forward to verify that $B^1(G, A) \subseteq Z^1(G, A)$. We define the **first cohomology group** of G with coefficients in A to be the group

$$H^1(G, A) = Z^1(G, A)/B^1(G, A)$$

Our construction above associates to each $c \in C^G$ a well defined object $[\varphi_b] \in H^1(G, A)$ which measures the obstruction of c from being in the image of p^G. This construction actually gives us a homomorphism $\partial : C^G \to H^1(G, A)$ and we get that the kernel of ∂ is exactly the image of p^G. This allows us to naturally continue the sequence

$$0 \to A^G \to B^G \to C^G \overset{\partial}{\to} H^1(G, A)$$

In fact, the construction of $H^1(G, A)$ is easily seen to be functorial in A, i.e. we can think of $H^1(G, -)$ as a functor from G-Ab to Ab. This functor can be shown to be exact in the middle, i.e. when we apply it to a short exact sequence the middle map remains exact. This means that we can even continue the above sequence to:

$$0 \to A^G \to B^G \to C^G \overset{\partial}{\to} H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to ?$$

It turns out that we can define functors $H^n(G, -)$ for each $n \geq 0$ such that $H^0(G, A) = A^G$, $H^1(G, A)$ is what we defined above and in such a way that we get a (functorial) long exact sequence

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to$$

$$H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to$$

$$H^2(G, A) \to H^2(G, B) \to H^2(G, C) \to ...$$

These functors are called the **right derived functors** of the invariants functor, and for each G-module A the abelian group $H^n(G, A)$ is called the n'th cohomology group of G with coefficients in A. The concrete construction of these functors is as follows:

Let A be a G-module. Define $C^k(G, A)$ to be the group of all (set-theoretic) functions from G^k to A. These functions are called k-cochains with coefficients in A. For $k = 0$ we set $C^k = A$. Define the map $d_k : C^k \to C^{k+1}$ by:

$$d_k(\varphi)(g_1, ..., g_{k+1}) =$$

$$g_1(\varphi(g_2, ..., g_{k+1})) + \sum_{i=1}^{k} (-1)^i \varphi(g_1, ..., g_i g_{i+1}, ..., g_k) + (-1)^{k+1} \varphi(g_1, ..., g_k)$$

In particular we see that

$$d_0(a)(g) = ga - a$$

so that $ker(d_0) = A^G$. Further we get that

$$d_1(\varphi)(g_1, g_2) = g_1(\varphi(g_2)) - \varphi(g_1 g_2) + \varphi(g_1)$$

Note that our cocycle condition on φ defined above can be rephrased now by requiring that $d_1(\varphi) = 0$. Thus we see that the first cohomology group we defined can be written as

$$H^1(G, A) = ker(d_1)/Im(d_0)$$

By setting $C^{-1} = 0$ and $d_{-1} = 0$ we can also write $H^0(G,A)$ like that:

$$H^0(G,A) = ker(d_1)/Im(d_0)$$

This calls for the general definition to be

$$H^n(G,A) = ker(d_n)/Im(d_{n-1})$$

For each short exact sequence $0 \to A \to B \to C \to 0$ one can show that there exist boundary maps $\partial_n : H^n(G,C) \to H^{n+1}(G,A)$ which give the long exact sequence in the cohomology groups.

If we take $A = \mathbb{Z}$ with the trivial G-action then the cohomology groups $H^1(G,A)$ are called the cohomology groups of G and are sometimes written $H^n(G)$. Note that whenever A is a trivial G-module the cohomology group $H^1(G,A)$ can be identified with the group of homomorphisms from G to A. In particular the group $H^1(G)$ is the dual of the abelization of G.

1.2 The meaning of H^1

Let us see what group-theoretic information does $H^1(G,A)$ encode.

First let A be just an abelian group. By a **principle homogenious** (PH for short) A-space we mean a set X with a a transitive and free action of A on it. Since A is abelian we shall usually write this action of the element $a \in A$ on a point $x \in X$ by $x \mapsto x + a$. Note that A acts on itself by translations, and this action is both transitive and free, so A itself has a natural structure of a PH A-space. Let us denote it by $\widehat{A}$.

Now if X is any PH A-space, then X is **non-naturally** isomorphic to $\widehat{A}$ by choosing any point $x \in X$ and considering the mapping $a \mapsto x + a$ as an isomorphism of PH A-spaces from $\widehat{A}$ to X.

Now suppose that A is not just an abelian group, but also a G-module. We say that X is a G-PH A-space if it is a PH A-space together with an action of G on it, such that

$$g(x + a) = g(x) + g(a)$$

for each $x \in X, a \in A$ and $g \in G$. Now the situation is more complicated, and not every two G-PH A-spaces are isomorphic (as G-PH A-spaces). Their isomorphism types are classified exactly by the group $H^1(G,A)$.

First of all, why is it natural that the isomorphism types will be classified by a group? The answer is that we have a natural operation of **tensor product** (over A) between two G-PH A-spaces which induces a group operation on the isomorphism classes. In order to describe it we first consider PH A-spaces without G-action.

Let X, Y be two PH A-spaces. Define the set Z to be $X \times Y$ modolu the relations

$$(x, y) \sim (x + a, y - a)$$

for each $a \in A$. Now the action of the element $a \in A$ on an equivalence class $[(x, y)]$ is defined by

$$[(x, y)] \mapsto [(x + a, y)]$$

Note that this is indeed well defined on equivalence classes. This action is easily checked to be transitive and free, so Z is indeed an A-space. We denote it by $Z = X \otimes_A Y$ and call it the tensor product of PH A-spaces. Tensor product is a commutative operation with an inverse which can be described by $X^* = Hom_{PH}(X, \widehat{A})$. By considering homomorphism classes we obtain a group, which we saw is trivial.

But what happens if we consider G-PH A-spaces? The tensor product operation is still defined in the same way and we have a natural action of G on $X \otimes_A Y$ by setting

$$g([(x, y)]) = [(g(x), g(y))]$$

Now the tensor product induces a commutative group structure on the isomorphism classes of G-PH A-spaces, so it makes sense that we can classify it by an abelian group.

Let us describe now the correspondence between elements in $H^1(G, A)$ and isomorphism classes of G-PH A-spaces. First given an element in $H^1(G, A)$, describe it by a 1-cycle $\varphi : G \to A$. Define $X_\varphi = \widehat{A}$ with the action of $g \in G$ given by

$$x \mapsto g(x) + \varphi(g)$$

The cycle condition will now make this into a G-action. If we would choose a different φ' which describes the same cohomology class, then there would be an $a \in A$ such that $\varphi(g) - \varphi'(g) = ga - a$ and then the map $x \mapsto x + a$ would induce an idomorphism of G-PH A-spaces from X_φ to $X_{\varphi'}$.

In the other direction, given a G-PH A-space X, choose a some point $x \in X$ and define $\varphi_x(g)$ to be the unique element $a \in A$ whihc satisfies $x + a = g(x)$. This defines a map $\varphi_x : G \to A$ which can easily be checked to be a cocycle. If we would choose a different $x' \in X$ then the element $a \in A$ which satisfies $x + a = x'$ would satisfy also

$$\varphi_x(g) - \varphi_{x'}(g) = ga - a$$

and thus φ_x and $\varphi_{x'}$ reduce to the same cohomology class in $H^1(G, A)$.

Exercises:

1. Show that the maps given above define a bijective correspondence between $H^1(G, A)$ and isomorphism classes of G-PH A-spaces.

2. Show that addition of cocycles corresponds to tensor product over A.

3. Show that a G-PH A-space X corresponds to the trivial element if and only if there exists an $x \in X$ such that $g(x) = x$ for every $g \in G$.

Remark: The definition of $H^1(G, A)$ can be generalized to the case where A is not abelian (with the same construction using 1-cocycles). In that case $H^1(G, A)$ will no longer be a group but only a pointed set. The notion of a G-PH A-space can still be defined and the elements of $H^1(G, A)$ will still correspond to isomorphism classes of G-PH A-space. As for $H^n(G, A)$ for $n \geq 2$ the right way to generalize them to non-commutative groups A (if there is one) is still an open question.

1.3 The meaning of H^2

We will not go into this in any detail, but just to name names, the second cohomology group $H^2(G, A)$ classifies group extensions of the form

$$1 \to A \xrightarrow{i} H \xrightarrow{p} G \to 1$$

For which the action of G on A coincides with the one induced by conjugation inside H.

2 Galois Cohomology

We now wish to apply this general theory to the case where G is the galois group of a field extension $\overline{K}/K$ where $\overline{K}$ is the algebraic closure of K. Note that in this situation G is a profinite group and carries naturally the profinite topology. Thus in order to apply the theory in a meaningful manner we need to modify it a bit so it would suit the category of **topological groups**.

This modification is quite simple. An A-module is now a topological abelian group together with a continuous action of G on it. When constructing the cohomology groups we inforce that all the cochains will be continous functions.

Now the situation here is not the most general one. Most galois modules (G-modules when G is a galois group) we will encounter will carry the **discrete topology**. This simplifies matters a bit as one can show that an action of a profinite group G on a discrete group A is continuous if and only if the orbit of each $a \in A$ is finite. This will be the standard case for us, as we will always derive our galois action from the galois action on algebraic field extensions which clearly poseses this property.

2.1 K-forms and H^1

Fix a field K and set $G = Gal(\overline{K}/K)$. Let X be an algebraic variety defined over K. Let

$$A_{X,X} = Iso_{\overline{K}}(X, X)$$

be the group of automorphisms of X over $\overline{K}$. Similarily for each variety Y which is isomorphic to X over $\overline{K}$ consider

$$A_{X,Y} = Iso_{\overline{K}}(X, Y)$$

which is the set of isomorphisms from X to Y defined over $\overline{K}$. Then $A_{X,Y}$ is PH $A_{X,X}$-space where the action of $A_{X,X}$ is given by composition.

We claim that both $A_{X,X}$ and $A_{X,Y}$ admit an action of the galois group G which is given by conjugation, i.e.

$$\sigma(\psi) \mapsto \sigma^{-1} \circ \psi \circ \sigma$$

This makes $A_{X,X}$ into a (not necessarily commutative) G-module and $A_{X,Y}$ into a G-PH A-space.

When is Y isomorphic to X over the base field K? This is equivalent to the existence of an isomorphism $\psi \in A_{X,Y}$ which is galois invariant. From exercise 3 in the previous section we see that this is equivalent to the fact that $A_{X,Y}$ is the trivial G-PH $A_{X,X}$-space. In fact, one can show that $H^1(G, A)$ is in a bijective correspondence with the set of K-isomorphism classes of varieties which are isomorphic to X over $\overline{K}$. The K-isomorphism types of varieties $\overline{K}$-isomorphic to X are called K-forms of X, or sometimes K-twists of X.

Example:

Let $X \subseteq \mathbb{A}^2$ be defined over $\mathbb{C}$ by the equation

$$xy = 1$$

X is actually isomorphic to the algebraic group $\mathbb{G}_m$.

Now consider the subfield $\mathbb{R} \subseteq \mathbb{C}$. Since the equation above has coefficients in $\mathbb{R}$ this gives us a specific $\mathbb{R}$-structure ($\mathbb{R}$-form) on X. The automorphisms of X are all of the form

$$\psi_{a,\epsilon}(x, y) = (a \cdot x^{\epsilon}, a^{-1}y^{-\epsilon})$$

for $a \in \mathbb{C}^*, \epsilon \in \{-1, 1\}$. The galois group is

$$G = Gal(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2$$

and the non-trivial element is complex conjugate. This element σ acts on $A_{X,X}$ as follows:

$$\sigma(\psi_{a,\epsilon}) = \psi_{\overline{a},\epsilon}$$

Thus $A_{X,X}$ fits in the following exact sequence of galois modules:

$$0 \to \mathbb{C}^* \to A_{X,X} \to \mathbb{Z}/2 \to 0$$

It is a well known theorem that $H^1(G, \mathbb{C}^*) = 0$ so we get that $H^1(G, A_{X,X})$ is embedded in $H^1(G, \mathbb{Z}/2) \cong \mathbb{Z}/2$. In order to show that it is actually equal to $\mathbb{Z}/2$ we shall denostrate a non-trivial $\mathbb{R}$-twist of X.

Define $Y \subseteq \mathbb{A}^2$ over $\mathbb{C}$ by the equation

$$x^2 + y^2 = 1$$

Y is isomorphic to X over $\mathbb{C}$ by the map $\phi : Y \to X$ given by

$$\phi(x, y) = (x + iy, x - iy)$$

This isomorphism is not defined over $\mathbb{R}$ as it uses the element i which is not in $\mathbb{R}$. Indeed X and Y are not isomorphic over $\mathbb{R}$ since the set of $\mathbb{R}$ points in Y is compact while the set of $\mathbb{R}$ points in X isn't. Not surprisingly, Y is called the compact $\mathbb{R}$-form of $\mathbb{G}_m$ and X is called the non-compact form.

2.2 The Meaning of H^2

Again we will not go into this in any detail, but just to name names, the second cohomology group $H^2(G, \overline{K}^*)$ classifies isomorphism classes of division algebras over K, and is called the **brauer group** of K. This group is very important in number theory and espcially in class field theory.

3 Applications to Elliptic Curves

We now arrive finally to our main interest of elliptic curves. Let E be an elliptic curve defined over $\mathbb{Q}$ and $G = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. In particular we mean that the unit element $e \in E$ is a rational point. We shall use the notation $H^n(K, E)$ to denote $H^n(Gal(\overline{K}/K), E(K))$ where K is some field containing $\mathbb{Q}$.

As we saw above, the group $H^1(\mathbb{Q}, E)$ classifies G-PH E-spaces. In fact, if we have a cohomology class represented by a 1-cocycle $\varphi : G \to E$ then the corresponding G-PH A-space will be an algebraic curve C defined over over $\mathbb{Q}$ which admits a $\overline{\mathbb{Q}}$-isomorphism

$$\psi : E \to C$$

satisfying the property

$$\sigma^{-1}(\psi^{-1}(\sigma(\psi(P)))) = P + \varphi(\sigma)$$

for all $P \in E$, when by $+$ we mean the group operation of E. The action of E on C can then be defined via the addition in E conjugated by ψ. Given such a curve C, we see that C has a rational point if and only if it corresponds to the trivial element in $H^1(\mathbb{Q}, E)$.

3.1 The Tate-Shafarevich Group

For each prime p let $\mathbb{Q}_p$ be the field of p-adic numbers and $\mathbb{Q}_\infty = \mathbb{R}$ the archimedian completion. Note that for each $2 \leq p \leq \infty$ we have the natural inclusions $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ which induce maps from the galois groups

$$Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to Gal(\overline{\mathbb{Q}}/\mathbb{Q})$$

These maps are in fact inclusions for each p. In the other direction we get maps

$$E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}_p})$$

The maps in both direction together induce maps on the cohomology groups

$$H^n(\mathbb{Q}, E) \to H^n(\mathbb{Q}_p, E)$$

We define the **Tate-Shafarevich** group to be

$$ker(H^1(\mathbb{Q}, E) \to \prod_{p \leq \infty} H^1(\mathbb{Q}_p, E))$$

and is denoted by $sha^1(\mathbb{Q}, E)$. In the language of the previous section we see that $sha^1(\mathbb{Q}, E)$ classifies the PH E-spaces which have a point in every $\mathbb{Q}_p$. It is a big conjecture (and one can say that it is part of the BSD conjecture as well) that $sha^1(\mathbb{Q}, E)$ is finite.

Now one can say that the **obstruction** to the existence of a rational point on a PH E-space X is divided into two parts - first of all X has to have a point over every $\mathbb{Q}_p$ and second of all we get an obstruction element in the (conjecturally finite) group $sha^1(\mathbb{Q}), E)$ which must vanish.

Although it hasn't been proved that the Tate-Shafarevich group is finite, it is quite easy to show that for each n, its n-torsion part is finite. Let us try to illustrate how this is done. For simplicitely let us work with $n = 2$ and with an elliptic curves E given by a Weierstrass equation of the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3) = x^3 + Ax + B$$

where $e_1, e_2, e_3 \in \mathbb{Z}$.

Consider the short exact sequence

$$0 \to E[2] \to E \overset{\cdot 2}{\to} E \to 0$$

We get a long exact sequence in the galois cohomology groups. Since assumed that e_1, e_2, e_3 are rational we get that $E[2]$ is rational, so we can write

$$0 \to E[2] \to E(\mathbb{Q}) \overset{\cdot 2}{\to} E(\mathbb{Q}) \to$$

$$H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}, E) \overset{\cdot 2}{\to} H^1(\mathbb{Q}, E) \to ...$$

From this sequence we get the short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}, E)[2] \to 0$$

Let us try to understand how do elements in $H^1(\mathbb{Q}, E[2])$ look like. Since $E[2] \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ and since $E[2]$ has only rational points we see that $H^1(\mathbb{Q}, E[2])$ is the group of homomorphisms from the galois group G to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. It is not hard to show that such homomorphisms are in one to one correspondense the group

$$\mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}$$

where if we represent an element in this group by a pair $(a_1, a_2) \in \mathbb{Q}^* \times \mathbb{Q}^*$ then the homomorphism $\varphi : G \to \{-1, 1\} \times \{-1, 1\}$ is given by

$$\varphi(\sigma) = \left(\frac{\sigma(a_1)}{a_1}, \frac{\sigma(a_2)}{a_2} \right)$$

It will be more covinient for us to describe this group as

$$\{(a_1, a_2, a_3) \in \left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right)^3 | a_1 a_2 a_3 = 1\}$$

What is the element in $H^1(\mathbb{Q}, E)$ which is the image of the element $(a_1, a_2, a_3) \in H^1(\mathbb{Q}, E[2])$? This can be given a nice geometric description (see the book of Washington).

Represent this element by a triplet $a_1, a_2, a_3 \in \mathbb{Q}^*$ such that $a_1 a_2 a_3$ is a square in $\mathbb{Q}$. Define the curve $C_{a_1,a_2,a_3} \subseteq \mathbb{P}^3$ via the homogenization of the following affine model:

$$a_1 u_1^2 - a_2 u_2^2 = e_2 - e_1$$

$$a_1u_1^2 - a_3u_3^2 = e_3 - e_1$$

We have a $\overline{\mathbb{Q}}$-map $\psi : E \to C$ defined by

$$\psi(x, y) = (f_1(x, y), f_2(x, y), f_3(x, y))$$

where

$$f_i(x, y) = \frac{x^2 - 2e_ix + \left(A + \frac{2B}{e_i}\right)}{2\sqrt{a_i}y}$$

It is a bit tidious, but one can check that

$$a_if_i^2 = F_2 - e_i$$

where

$$F_2(x, y) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2}$$

is the rational function $P \mapsto x(2P)$ obtained by taking the x-coordinate of $2P$. In particular we see that

$$a_1f_1^2 - a_2f_2^2 = e_2 - e_1$$

$$a_1f_1^2 - a_3f_3^2 = e_3 - e_1$$

so these polynomials induce a map from E to C. Of course we need to homogenize this map and show that everything works but we won't do this here.

We also have a map in the other direction, which is not hard to see as the f_i's are linearly independent and so we can take linear combinations of them (over $\overline{\mathbb{Q}}$) to obtain $\frac{x}{y}$ and $\frac{1}{y}$ (from which we obtain can obtain the functions x and y).

This ψ induces a structure of a PH E-space on C. In particular, it is easy to show that if we would change a_1, a_2, a_3 by multiplying them with squares then the resulting PH E-space would be isomorphic. This construction is a geometric realization of the map $H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}, E)$.

Let us try to explain what is going on here and where did these maps come from. Let

$$D = [0] + [(e_1, 0)] + [(e_2, 0)] + [(e_3, 0)]$$

be the divisor which is the sum of the two torsion points. Let $L(D)$ be the vector apce of all rational functions f which satisfy

$$div(f) + D \geq 0$$

i.e. the functions that are allowed to have poles of degree at most 1 in the two torsion points. $L(D)$ is 4 dimensional and is spanned over $\overline{\mathbb{Q}}$ by $1, f_1, f_2, f_3$. The galois group acts on these functions by conjugation (which more concretely means acting on the coefficients) by

$$\sigma(f_i) = \frac{\sigma(\sqrt{a_i})}{a_i} f_i = \pm f_i$$

Note that $L(D)$ is closed under the action of $E[2]$ (the 2-torsion points pf E) by translation. Let us denote this action by $P^* f_i$ for $P \in E[2]$. In particular, since $af_i^2 = P_2 - e_i$ and the rational function P_2 is invariant under translation by an element of $E[2]$, we get that

$$P^* f_i = \pm f_i$$

and this sign does not depend on the choice of the a_i's. Our 1-cocycle will be a map $\varphi : G \to E[2] \subseteq E$ such that

$$\sigma(f_i) = \varphi(\sigma)^* f_i$$

for $i = 1, 2, 3$.

Nose the important fact that since the map $H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}, E)[2]$ is surjective, it follows that this geometric description describes **all possible** PH E-spaces which are 2-torsion. This is a geometric fact for which I can't see any direct geoemtric proof not using galois cohomology.

Exercises:

1. Show that the map boundary map $E(\mathbb{Q}) \to H^1(\mathbb{Q}, E[2])$ associates with the element (x, y) the element (a_1, a_2, a_3) (mod squares) given by

$$a_1 = x - e_1$$

$$a_2 = x - e_2$$

$$a_3 = x - e_3$$

   Hint: apply the functions f_1, f_2, f_3 to the set $\{P | 2P = (x, y)\}$ in order to calculate how the galois group acts on them versus how $E[2]$ acts on them (use the property $a_i f_i^2 = F_2 - e_i$ satisfied by the f_i's).

2. Our PH E-space corresponds to a 2-torsion element in $H^1(\mathbb{Q}, E)$. Show that this means that there exists a $\mathbb{Q}$-map $\pi : C \to E$ such that $\pi \circ \psi$ is multiplication by 2. Construct this map.

3. Show that if C has a point in $\mathbb{Q}_p$ and if p appears in an odd degree in at least one of a_1, a_2, a_3, then p divides the discriminant

$$\Delta = (e_2 - e_1)(e_3 - e_1)(e_3 - e_2)$$

   Conclude that there are only finitely many 2-torsion elements in $sha^1(\mathbb{Q}, E)$.

4. Conclude that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.