Galois Cohomology

1 Motivation and Definitions

In this presentation, we will take the motivational viewpoint that group cohomology in general, and Galois cohomology in particular, is a functor designed to tell us information about a group G via the behavior of fixed-points of its action on G-modules. To the extent that we attempt to derive information from G via the way its acts on other objects, this framework fits into the larger picture of representation theory.

Our story begins with a group G and a G-module A on which it acts. The simplest question we can ask about fixed points is the following. What elements $a \in A$ are fixed by the action $a \to ga$? Well, 0_A is such an element, and the collection of these fixed points is closed under addition and taking inverses, so we get a group denoted A^G. In this special case when A is a G-module, we write $A^G = H^0(G, A)$, the 0th cohomology group of G with coefficients in A.

To motivate the next cohomology group, we concern ourselves with the problem of *lifting fixed points*. Let G act on a G-module B, and let A be a submodule. We can form a new G-module B/A, and consider the fixed points of the action of G on B/A. To what extent can we lift such fixed points to fixed points of the action of G on B? Well, take $\bar{b}$ in B/A and a representative b of this coset. For $g \in G$, form the element $gb - b$. The image of $gb - b$ is $0 \in B/A$, since $g\bar{b} = \bar{b}$. Thus $gb - b \in A$, and is zero precisely if b was a fixed point. In that sense, we might say that the map

$$G \to A$$

$$f_b : g \to gb - b$$

measures the obstruction of lifting $\bar{b}$ to a fixed point. Note that

$$f_b(gg') = gf_b(g') + f_b(g)$$

This observation motivates the following definition. If A is a G-module, a 1-cocyle of G with vaues in A is a map

$$f : G \to A$$

$$f(gg') = gf(g') + f(g)$$

This type of map is called a *crossed homomorphism* because it is similar to a homomorphism except that in one of the terms we pull out the other group element to the front. One way to obtain 1-cocycles is by starting with a fixed point $\bar{b} \in B/A$ and considering f_b associated to some lift of $\bar{b}$. Let us go ahead and also define a 1-coboundary as a map $f : G \to A$ for which there exists $a \in A$ such that

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

Note that any 1-coboundary is a 1-cocycle.

The set of 1-cocycles is denoted $Z^1(G, A)$, and the subset of 1-coboundaries is denoted $B^1(G, A)$. It is not hard to see that these are groups, where the latter is a subgroup of the former. Since everything in sight is abelian, there is nothing stopping us from defining

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

The group $H^1(G, A)$ is called the *first cohomology group of G with coefficients in A*. Recalling our earlier discussion of modules, we may start with a fixed point $\bar{b} \in B/A$ and obtain a 1-cocycle $f_b : G \to A$. This cocycle is a coboundary if and only if we can find some a for which

$$gb - b = f_b(g) = ga - a$$

That is, $b - a$ is a fixed point in G lying over $\bar{b}$. We can thus see that $H^1(G, A)$ is intimately related to our ability to lift fixed points of B/A to B, so that the vanishing of this group is tantamount to our ability to lift fixed points.

It is possible to go on and define higher cohomology groups, and a good introductory discussion of the second group cohomology can be found here[1]. However, for our purposes, we will suffice with the zeroeth and first cohomology groups.

2 The Case of Finite Cyclic Groups

Before we move on to the case of Galois cohomology, let us specialize to the situation of the cohomology of cyclic groups. Let G be finite cyclic with generator γ of exponent n. We know that a 1-cocycle $f : G \to A$ is determined by where it sends γ, since

$$f(\gamma^2) = \gamma f(\gamma) + f(\gamma)$$

and so on for higher powers, inductively. However, not every element in A is suitable to be $f(\gamma)$. We will provide a simple necessary and sufficient condition on the value of $f(\gamma)$.

Consider the homomorphism

$$\mathrm{Tr}_G : A \to A$$

$$\mathrm{Tr}_G(a) = \sum_{\sigma \in G} \sigma(a)$$

We claim that $f(\gamma)$ is in the kernel of this homomorphism.

$$\mathrm{Tr}_G(f(\gamma)) = \sum_k \gamma^k(f(\gamma))$$

If we write

$$f(\gamma^{k+1}) = f(\gamma^k\gamma) = \gamma^k f(\gamma) + f(\gamma^k)$$

then

$$\sum_k \gamma^k f(\gamma) = \sum_k f(\gamma^{k+1}) - f(\gamma^k) = 0$$

At the same time, if a is in the kernel of the trace map, we can define

$$f(\gamma) = a$$

and we want to show that

$$f(\gamma^k\gamma^m) = f(\gamma^k) + \gamma^k f(\gamma^m)$$

We know that

$$f(\gamma^2) = \gamma a + a$$

$$f(\gamma^3) = f(\gamma^2\gamma) = \gamma a + a + \gamma^2 a = \gamma^2 a + \gamma a + a$$

and so forth, with

$$f(\gamma^n) = \mathrm{Tr}_G(a) = 0$$

which lets us justify setting $k+m$ less than n, in which case the necessary equality is easy to verify. This shows that the group of 1-cocycles can be identified with the kernel of the trace map.

Next we want to identify the 1-coboundaries. These can be identified with the subgroup $(1-\gamma)A < \ker \mathrm{Tr}_G$, since if $f(\gamma^k) = \gamma^k a - a$, then $f(\gamma) = a(\gamma - 1)$, and conversely if $f(\gamma) = a(\gamma-1)$, then

$$f(\gamma^2) = f(\gamma) + \gamma f(\gamma) = \gamma a - a + \gamma^2 a - \gamma a = \gamma^2 a - a$$

and so forth, by induction. Thus we have an isomorphism

$$H^1(G/A) \cong \ker Tr_G/(1-\gamma)A$$

3 An Explicit Calculation of H^1

The field $\mathbb{C}$ comes endowed with a special field automoprhism, complex conjugation. We then have a group G of order 2 acting on $\mathbb{C}$, with the fixed points of the non-trivial group element (conjugation) being the real line. Let us compute $H^1(G, \mathbb{C})$ and $H^1(G, \mathbb{C}^\times)$.

If $f : G \to \mathbb{C}$ is a 1-cocyle, then $f(1) = f(1^2) = 1f(1) + f(1) = 2f(1)$, so $f(1) = 0$. Thus f is determined by $f(\sigma) = z_0$. We have $0 = f(1) = f(\sigma^2) = \sigma f(\sigma) + f(\sigma)$, so $\bar{z_0} = -z_0$. Hence z_0 is purely imaginary, so $z_0 = z_0/2 - (\bar{z}_0)/2 = \sigma(\bar{z}_0/2) - \bar{z}_0/2$. Hence f is a 1-coboundary, and $H^1(G, \mathbb{C}) = 0$!

Let $f : G \to \mathbb{C}^\times$ be a 1-cocyle. Then $f(1) = f(1^2) = 1f(1)f(1)$, so $f(1) = 1$. Thus f is determined by $f(\sigma) = w^0$. We have $1 = f(1) = f(\sigma^2) = \sigma f(\sigma) f(\sigma)$, hence $1 = \bar{w}^0 w^0$, so w^0 has norm 1, say $w^0 = e^{i\theta}$ for some real θ. We can thus write $w^0 = e^{i\theta/2}/e^{-i\theta/2} = v^0/\bar{v}^0$ for $v^0 = e^{-i\theta/2}$, so that f is a 1-coboundary, hence $H^1(G, \mathbb{C}^\times) = 0$.

Exercise: Let $\mathbb{Z}_2$ act on $\mathbb{Z}$ by $0 \cdot a = a$ and $1 \cdot a = -a$. Check that $H^1(\mathbb{Z}_2, \mathbb{Z}) = \mathbb{Z}_2$. Thus group cohomology is not always trivial.

4 Galois Cohomology

This first two examples above might seem like a tremendous miracle, but we will see that this is just a special case of a more general phenomenon: that is, Galois Cohomology. Recall Hilbert's Theorem 90. In its additive form, it says that an element in a cyclic extension K/k of degree n has vanishing trace iff it is of the form $\alpha - \sigma\alpha$ for $\alpha \in K$ and σ generating the Galois group. If we write $G = \text{Gal}(K/k)$ and view K as a G-module, then in light of our earlier observation regarding the trace, this is tantamount to asserting that $H^1(G, K) = 0$.

Moving now to the multiplicative version of Theorem 90, we are in the same situation of a cyclic extension K/k, and we say that an element has norm 1 iff it is of the form $\alpha/\sigma(\alpha)$ for $\alpha \in K$ and σ generating G. As before, write $G = \text{Gal}(K/k)$ and consider $K^\times$ as a G-module. The norm here amounts to the trace map as define on $K^\times$, and again Hilbert's Theorem 90 is telling us that an 1-cocyle is always a 1-coboundary, so $H^1(G, K) = 1$.

These examples explain our earlier calculation. In fact, Emmy Noether later showed that $H^1(G, K^\times)$ is trivial for any Galois extension, but we will delve into that here.

5 Rational Points on the Circle and Pythaogrean Triples

As a pleasant demonstration of the power of our results, let us parametrize rational points on the circle.

Consider the cyclic Galois extension $\mathbb{Q}(i)/\mathbb{Q}$. An element of norm 1 is one for which $\bar{z}z = |z|^2 = 1$. By Galois Cohomology, we know there is some $w \in \mathbb{Q}(i)$ for which

$$z = \frac{w}{\bar{w}} = \frac{a+bi}{a-bi}$$

where we can take a, b here to be integral. Then

$$z = \frac{a^2 - b^2}{a^2 + b^2} + \frac{2ab}{a^2 + b^2} i$$

If one writes $X = a^2 - b^2$, $Y = 2ab$ and $Z = a^2 + b^2$ then the point

$$\frac{X}{Z} + \frac{Y}{Z}i$$

has the property that $X^2 + Y^2 = Z^2$, so (X, Y, Z) is a Pythaogrean triple. Conversely, Pythagorean triples certainly correspond to rational points on the unit circle. Thus, we now have a way of parametrization pythagorean triples.

6 Connections to Non-Abelian Kummer Theory

We end with a result of Sah that has important applications to non-abelian Kummer theory.

Theorem. *Let G be a group and E a G-module. Let τ be in the center of G. Then $H^1(G, E)$ is annihilated by the map $x \to \tau_x - x$ on E. In particular, if this map is an automorphism of E, then $H^1(G, E) = 0$.*

Proof. Let f be a 1-cocyle of G in E. Then $\tau\sigma\tau^{-1} = \sigma$, so

$$f(\sigma) = f(\tau\sigma\tau^{-1}) = f(\tau) + \tau f(\sigma\tau^{-1}) = f(\tau) + \tau f(\sigma) + \tau\sigma f(\tau^{-1})$$

Therefore

$$\tau f(\sigma) - f(\sigma) = -\sigma\tau f(\tau^{-1}) - f(\tau)$$

Now, $f(1) = f(1) + f(1)$ imlpies $f(1) = 0$, hence

$$0 = f(1) = f(\tau\tau^{-1}) = f(\tau) + \tau f(\tau^{-1})$$

This proves that

$$(\tau - 1)f(\sigma) = (\sigma - 1)f(\tau)$$

Hence $(\tau - 1)f$ is a coboundary. $\square$