LECTURE 25, MONDAY 10.05.04

FRANZ LEMMERMEYER

Galois cohomology studies the action of Galois groups on certain abelian groups (fields, rings, ideals, units, class groups, ...). A typical example is the following: let $K/\mathbb{Q}$ be a normal extension and consider the exact sequence

$$1 \longrightarrow E_K \longrightarrow K^\times \longrightarrow P_K \longrightarrow 1, \tag{1}$$

where $E_K = \mathcal{O}_K^\times$ is the group of units of $\mathcal{O}_K$, $K^\times = K \setminus \{0\}$ is the unit group of K, and P_K is the group of nonzero principal ideals (α).

Now let A be an abelian group on which $G = \mathrm{Gal}\,(K/\mathbb{Q})$ acts; we say that A is a Galois module. In such a situation, we define the fixed module of A by $A^G = \{a \in A : a^\sigma = a \text{ for all } \sigma \in G\}$. It is the largest submodule of A on which G acts trivially.

In the above example, we have $E_K^G = \mathbb{Z}^\times = \{\pm 1\}$ and $(K^\times)^G = \mathbb{Q}^\times$. If we had $P_K^G = P_\mathbb{Q}$, taking the fixed modules would transform (refE1) into the exact sequence

$$1 \longrightarrow \mathbb{Z}^\times \longrightarrow \mathbb{Q}^\times \longrightarrow P_\mathbb{Q} \longrightarrow 1.$$

But things are not that simple. Take e.g. the quadratic field $K = \mathbb{Q}(\sqrt{2}\,)$. Then $(\sqrt{2}\,)$ is a principal ideal, and it is fixed by $G = \mathrm{Gal}\,(K/\mathbb{Q})$ since $(\sqrt{2}\,) = (-\sqrt{2}\,)$. Thus P_K^G contains $(\sqrt{2}\,)$, but $P_\mathbb{Q}$ does not.

This shows that taking fixed modules does not transform exact sequences into exact sequences (in more fancy words: it is not an exact functor from the category of G-modules to the category of abelian groups).

1. The First Cohomology Group

Proposition 1. *Let G be a group and*

$$0 \longrightarrow A \xrightarrow{\ \iota\ } B \xrightarrow{\ \pi\ } C \longrightarrow 0$$

and exact sequence of G-modules. Then

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G$$

is exact. In other words, taking fixed modules is a left exact functor from the category of G-modules to the category of abelian groups.

Proof. Since we can view A as a subgroup of B, it is clear that A^G is a subgroup of B^G, hence the first map is injective. Now let π^G denote the restriction of $\pi : B \longrightarrow C$ to B^G. Clearly elements from A^G get killed by π^G, so take an element $b \in \ker \pi^G$. Then $\pi(b) = 0$, hence $b = \iota(a)$ for some $a \in A$. Moreover, $\iota(ga) = g\iota(a) = gb = b = \iota(a)$, so $\iota(ga - a) = 0$, and since ι is injective, we have $ga = a$. Thus $a \in A^G$, and the claim follows. □

Our example shows that we cannot paste some $\longrightarrow 0$ to the end of the exact sequence of fixed modules. Of course we could make it into an exact sequence by adding $\longrightarrow C^G/B^G \longrightarrow 0$, but that would not be of much help in practice. What

we will do instead is try to prove that $B^G \longrightarrow C^G$ is surjective (of course we will not succeed) and use the information gained by doing this to get a clear picture of the obstruction to surjectivity.

We take an element $c \in C^G$. Since π is surjective, there is a $b \in B$ such that $\pi(b) = c$. We would like to show that $b \in B^G$; now $\pi(gb) = g\pi(b) = gc = c = \pi(b)$, hence $\pi(gb - b) = 0$, and therefore $gb - b \in \ker \pi = \operatorname{im} \iota$. Thus there is an $a_1 \in A$ such that $gb - b = a_1$ (we now identify A with a subgroup of B). If we could choose b in such a way that $a_1 = 0$ for all $g \in G$, then we would have $b \in B^G$ and we would be done.

The problem is that we cannot see how we should achieve this. What he have achieved so far is this: given $c \in C^G$, we have constructed a map $x : G \longrightarrow A$ with $x(g) = gb - b$. This map x is not a homomorphism: we have $x(gh) = gh(b) - b = g(h(b) - b) + g(b) - b = gx(h) + x(g)$. Maps $x : G \longrightarrow A$ with the property that $x(gh) = gx(h) + x(g)$ are called *crossed homomorphisms*. They clearly form a group with respect to addition that will be denoted by $C^1(G, A)$.

Thus it seems we have constructed a map $C^G \longrightarrow C^1(G, A)$; actually, we haven't, because the map sending $c \in C^G$ to the crossed homomorphism $x(g) = gb - b$ is not well defined: it depends on the choice of b. In fact, assume that $\pi(b') = c$ and $x'(g) = gb' - b'$; then $\pi(b - b') = 0$, so $b - b' = a$ for some $a \in A$, hence $x(g) - x'(g) = ga - a$. Thus the maps x and x' differ by a very special map sending g to $ga - a$; these maps are called split crossed homomorphism, and we will denote them by the elements a themselves: thus $a : G \longrightarrow A$ is defined by $a(g) = ga - a$. The set of all split crossed homomorphisms is denoted by $B^1(G, A)$ and forms a subgroup of $C^1(G, A)$. The quotient $H^1(G, A) = C^1(G, A)/B^1(G, A)$ is called the first cohomology group of G with values in A.

What we have so far is this: to every element $c \in C^G$ we have assigned a crossed homomorphism in $C^1(G, A)$ that is defined up to a split crossed homomorphism in $B^1(G, A)$. In other words: we have a map $C^G \longrightarrow H^1(G, A)$. It is now straightforward to check that this map is a homomorphism, and that we have a long exact sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C).$$

This suggests defining $H^0(G, A) = A^G$; then the above sequence is a sequence of cohomology groups of dimension 0 and 1.

Instead of verifying this directly, we now go back, start from scratch, and let the snake lemma do the work.

2. Second Construction

Let X be a G-module; we define

$$C^1(G, X) = C^1(X) = \{x : G \longrightarrow X : x(gh) = gx(h) + x(g)\}.$$

We add these 1-cocycles via $(x + y)(g) = x(g) + y(g)$; this makes $C^1(G, X)$ into an abelian group. If G acts trivially on X, then clearly $C^1(G, X) = \operatorname{Hom}(G, X)$ is just the group of homomorphisms from G to A.

Next we address functoriality: a G-homomorphism $f : X \longrightarrow Y$ between G-modules induces a homomorphism $f^1 : C^1(G, X) \longrightarrow C^1(Y)$ via $f^1 : C^1(X) \longrightarrow C^1(Y) : x \longmapsto f^1 \circ x$. A simple calculation shows

Lemma 2. *If* $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ *is an exact sequence of* G*-modules, then*

$$0 \longrightarrow C^1(G,A) \longrightarrow C^1(G,B) \longrightarrow C^1(G,C)$$

is an exact sequence of abelian groups.

Thus C^1 is a left exact functor from the category of G-modules to abelian groups. Next we define homomorphisms $\lambda : X \longrightarrow C^1(G,X)$; actually we already did that: for each $x \in X$ we have the element $x \in C^1(G,X)$ sending $g \in G$ to $gx - x$. The kernel of λ consists of all elements $x \in X$ for which $gx - x = 0$ for all $g \in G$: this is exactly the fixed module X^G. Moreover, the image of λ is the set of all split crossed homomorphisms, hence $\operatorname{im} \lambda = B^1(G,X)$ and $\operatorname{coker} \lambda = H^1(G,X)$. Thus we have an exact sequence

$$0 \longrightarrow X^G \longrightarrow X \longrightarrow C^1(G,X) \longrightarrow H^1(G,X) \longrightarrow 0.$$

Collecting everything into one big diagram we end up with

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & A^G & & B^G & & C^G & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C^1(A) & \longrightarrow & C^1(B) & \longrightarrow & C^1(C) & &
\end{array}$$

The snake lemma then implies

Proposition 3. *For every exact sequence of* G*-modules*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

there is an exact sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C).$$

In general, the homomorphism $H^1(G,B) \longrightarrow H^1(G,C)$ will not be surjective. Attempting to prove that it is leads to a definition of groups $H^2(G,A)$, and this process can be continued indefinitely, giving us an infinite exact sequence of cohomology groups.

3. Basic Properties

Proposition 4. *Any* G*-homomorphism* $f : A \longrightarrow B$ *of* G*-modules induces a homomorphism* $f^1 : H^1(G,A) \longrightarrow H^1(G,B)$ *of abelian groups.*

Proof. Exercise. □

Proposition 5. *Let* G *be a finite group of order* n*; then* $H^1(G,A)$ *is a torsion group killed by* n*.*

Proof. Let $x \in C^1(G,A)$; we have to show that $nx \in B^1(G,A)$. Now $x(g) = x(h^{-1}hg) = h^{-1}x(hg) + x(h^{-1})$; adding these equations for all $h \in G$ and putting $a = \sum_{h\in G} x(h^{-1})$ we find

$$nx(g) = a + \sum_{h\in G} h^{-1}x(hg) = a + g\Big(\sum_{h\in G}(hg)^{-1}x(hg)\Big).$$

As h runs through G, so does hg; moreover $0 = x(1) = x(h^{-1}h) = h^{-1}x(h)+x(h^{-1})$, hence $h^{-1}x(h) = -x(h^{-1})$ and $\sum_{h\in G} h^{-1}x(h) = -a$. Thus $nx(g) = a - ga$ for all $g \in G$, and this shows that $nx \in B^1(G,A)$. □

Corollary 6. *If G is a finite group of order n and if A is uniquely divisible by n (i.e., every equation $ny = a$ has a unique solution for all $a \in A$ and $n \in \mathbb{N}$), then $H^1(G,A) = 0$.*

Proof. The short exact sequence

$$0 \longrightarrow A \xrightarrow{\ n\ } A \longrightarrow 0 \longrightarrow 0$$

yields

$$0 \longrightarrow H^1(G,A) \xrightarrow{\ n\ } H^1(G,A) \longrightarrow H^1(G,0) = 0,$$

i.e., multiplication by n induces an automorphism of $H^1(G,A)$; since $H^1(G,A)$ is killed by n, we conclude that $H^1(G,A) = 0$. □

The group $\mathbb{Q}$ is uniquely divisible by any $n \ge 1$. A finite group of order m is uniquely divisible by any n coprime to m. This implies in particular that $H^1(G,A) = 0$ if G and A are finite groups with coprime order.