GALOIS MODULES AND THEIR COHOMOLOGY
A CHEAT SHEET

BRIAN OSSERMAN

ABSTRACT. This is a collection of definitions and relevant results in the theory of Galois modules and their cohomology. The proofs are omitted for the sake of having all the statements together in one relatively concise place, thus the designation of 'cheat sheet'. The material is largely 'borrowed' from the lecture notes of Mak Trifkovic, Alex Popa, Martin Weissman, and Nick Rogers.

1. GALOIS MODULES

We start with the definition of a Galois module. A lot of topology will be included, but in the most common examples most of the relevant topologies will be discrete and continuity conditions will become much simpler.

Let G be a topological group (we will be interested in G as a Galois group under the usual profinite topology), R a topological ring, and M a topological R-module.

Definition 1. *M is a G-**module** if there is a continuous R-linear action of G on M, and in the case that G is a Galois group, we call M a **Galois module**.*

For brevity's sake, we will write $G_{L/K}$ for $\mathrm{Gal}(L/K)$ and G_K for $\mathrm{Gal}(\overline{K}/K)$. We have the following simplified condition for continuity in the case we will most frequently deal with:

Proposition 1. *If M is a discrete module and a profinite group G acts on it, then M is a G-module if and only if the subgroup of G fixing any given element of M (i.e., the stabilizer of that element) has finite index in all of G.*

Note the following immediate corollary:

Corollary 1. *If further M is finite, the action of G must always be continuous.*

There are a number of functors and operators on Galois modules. The one which is in some sense the most central to the theory is the **invariant submodule** functor:

Definition 2. *If M is a G-module, we write M^G for the submodule of M fixed by the action of G.*

The theory of Galois cohomology is built up from the failure of this functor to be right exact. However, before discussing Galois cohomology, we define several important operators on Galois modules.

Definition 3. *If M and N are two G-modules over R, we can create new G-modules $M \otimes N$ and $\mathrm{Hom}(M, N)$. $M \otimes N$ is simply the module tensor product, with the G-action given by G acting independently on the left and right, i.e. $g(m \otimes n) = gm \otimes gn$. $\mathrm{Hom}_R(M, N)$ is the usual set of continuous R-module homomorphisms, with G acting via its usual action on the image, and an inverse action on the argument, i.e. $(g\phi)m = g(\phi(g^{-1}m))$.*

Note that thanks to the inverse in the definition, we can recover the set of homomorphisms from M to N which respect the their G-actions simply as $\mathrm{Hom}_R(M,N)^G$, the invariant submodule of $\mathrm{Hom}_R(M,N)$ under the action of G. We also have two dual operators on G_K-modules:

Definition 4. *If M is a G_K-module, then there is the* **Pontryagin dual** $M^\vee$, *given by* $\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})$. *There is also the* **Cartier dual** M^*, *given by* $\mathrm{Hom}_{\mathbb{Z}}(M,\mu(\overline{K}))$. *Here the G_K action on $\mathbb{Q}/\mathbb{Z}$ is the trivial action, and on $\mu(\overline{K})$ is the obvious action, under the inclusion of $\mu(\overline{K})$ in $\overline{K}$.*

2. Cohomology

We now turn our attention to Galois cohomology. Before giving the explicit definition, a note for those familiar with derived functors might not be amiss. Since this will be the cohomology theory derived from the invariant submodule functor, it would make sense to expect that it would be constructed by taking an injective resolution of the module in question, applying the invariant submodule functor, and taking the cohomology of the resulting complex. This will give the correct answer, and may provide some helpful intuition to anyone comfortable with derived functors, but it is not the standard construction given. The standard construction has the two conveniences of using projective resolutions instead of injectives, and of using a predetermined resolution which doesn't depend on the module in question.

Recall that if M,N are G-modules, then we have $\mathrm{Hom}_R(M,N)^G$ is simply the module of homomorphisms from M to N which respect the G-action. For our modules, we will work over $\mathbb{Z}$, that is, with arbitrary abelian groups. Then, observe that we can recover M^G as $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},M)^G$. It is this fact which motivates our construction of Galois cohomology:

Start with $\mathbb{Z}$, and fix a projective resolution P_i of $\mathbb{Z}$, as G modules. General abstract nonsense says that the results will be independent of which resolution we choose, but for concreteness' sake we will use a particular collection of projective modules, with P_i being the free $\mathbb{Z}$-module generated by the set of $(i+1)$-tuples of elements of G. We will make G act on the generators by translation of each coordinate, i.e. $g(g_0,\dots,g_i)=(gg_0,\dots,gg_i)$, and then extend to P_i by linearity. We then have a boundary map $d:P_i\to P_{i-1}$ defined on the generators by

$$d(g_0,\dots,g_i)=\sum_{j=0}^{i}(-1)^j(g_0,\dots,g_{j-1},g_{j+1},\dots,g_i)$$

Then these P_i together with the d maps give a projective resolution of $\mathbb{Z}$. We then bring M into the picture by applying the functor $\mathrm{Hom}_{\mathbb{Z}}(\cdot,M)^G$ to the sequence to get a complex K^i (note that we leave out the $\mathbb{Z}$ from the projective resolution, so that $K^i=\mathrm{Hom}_{\mathbb{Z}}(P^i,M)^G$, and we also require the homomorphisms to be continuous). Lastly we define $H^i(G,M)$ to be the cohomology of this complex, called the **cohomology of G with coefficients in M**. Note that all of the operations involved are operations on Galois modules, so the resulting cohomology groups are still G-modules. However, the G-action is killed when $\mathrm{Hom}_{\mathbb{Z}}(\cdot,M)^G$ is applied to the resolution, so the G-action on all cohomology groups is simply the trivial action.

The elements of K^i may be described as continuous homomorphisms from the free $\mathbb{Z}$ module generated by $(i+1)$-tuples of elements of G to M which respect the G-action. However, we will describe them somewhat differently, as arbitrary continuous functions from i-tuples of elements of G to M. These are equivalent

under the following correspondence: given $h : G^i \to M$, we get a homomorphism $f : P_i \to M$ defined on the generators by the formula

$$f(g_0, \ldots, g_i) = g_0 h(g_1 g_0^{-1}, g_2 g_1^{-1}, \ldots, g_i g_{i-1}^{-1})$$

One easily checks that multiplying through the arguments by some $g \in G$ will result in applying g to the result, so the f is in fact a $\mathbb{Z}[G]$ homomorphism as required, and the inverse correspondence is given by setting

$$h(g_1, \ldots, g_i) = f(1, g_1, g_1 g_2, \ldots, g_1 \cdots g_i)$$

This gives a more convenient description of K^i, since we no longer need to worry about respecting the G-action.

Following through the definitions gives the following formula for the coboundary map on K^i:

$$dh(g_1, \ldots, g_{i+1}) = g_1 h(g_2, \ldots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j h(g_1, \ldots, g_j g_{j+1}, \ldots g_{i+1}) + (-1)^{i+1} h(g_1, \ldots, g_i)$$

Then we can recover H^0 and H^1 quite explicitly without any difficulty. K^0 is simply the set of constant functions, so is identified with M. For $h \in K^0$, we have $dh(g) = gh - h$, which is 0 only if G acts trivially on h. Thus $H^0(G, M) = M^G$.

Similarly, we get a very concrete description of $H^1(G, M)$: the cocycles are continuous functions $h : G \to M$ satisfying $h(gg') = gh(g') + h(g)$, and the coboundaries are those of the form $h(g) = gm - m$ for some $m \in M$.

In all the examples we shall consider, the Galois modules will all have the discrete topology. In these cases, we have:

Proposition 2. *For any discrete G_K-module M, $H^1(G_K, M)$ is entirely torsion.*

Lastly, as one would hope for out of any cohomology theory, we have the property that any short exact sequence $0 \to A \to B \to C \to 0$ of G-modules gives a **long exact sequence in cohomology**:

$$\cdots \to H^{n-1}(G, C) \to H^n(G, A) \to H^n(G, B) \to H^n(G, C) \to H^{n+1}(G, A) \to \ldots$$

Before moving on, a note on a slight bizarreness of terminology: in topological cohomology theories, when one says "cohomology of X with coefficients in G", one gets a long exact sequence of cohomology out of maps between different X, holding the G fixed. In Galois cohomology the situation is reversed, with the relevant short exact sequences being those between different 'coefficient' G-modules for a fixed G.

3. Restriction and Inflation

Let M be a G-module, and suppose H is a subgroup of G. Then we get a natural **restriction** homomorphism from $H^q(G, M)$ to $H^q(H, M)$ by restricting cocyles on G to cocycles on H. If also H is normal in G, then we have that M^H is a G/H module, and we also get a natural **inflation** homomorphism from $H^q(G/H, M^H)$ to $H^q(G, M)$ induced by the quotient map from G to G/H. Then we have the following:

Proposition 3. *Inflation-Restriction is exact on H^1, i.e.*

$$0 \to H^1(G/H, M^H) \to H^1(G, M) \to H^1(H, M)$$

is exact.

Proposition 4. *If $H^1(H, M) = 0$, then Inflation-Restriction is also exact on H^2, i.e.*

$$0 \to H^2(G/H, M^H) \to H^2(G, M) \to H^2(H, M)$$

is exact.

Lastly, the cohomology arising from an Inflation-Restriction sequence is in general given by a spectral sequence:

Theorem 1. *The* **Hochschild-Serre spectral sequence** *has*

$$E_2^{p,q} = H^p(G/H, H^q(H, M))$$

and abuts to $H^n(G, M)$.

This makes sense since the $H^q(H, M)$ are still G-modules, but with trivial H-action on them. Note that both of the previous propositions, which may be proven directly without too much effort, are also immediate consequences of this spectral sequence.

4. The Cup Product and Tate Local Duality

First, we have the cross product map from $H^m(G, M) \otimes H^n(G', M')$ to $H^{m+n}(G \times G', M \otimes M')$ defined in more or less the obvious way, except with a sign depending on $m + n$. In the case where $G = G'$, we then compose with the map induced by the diagonal homomorphism to get the **cup product** map:

$$\cup : H^m(G, M) \times H^n(G, M') \to H^{m+n}(G, M \otimes M')$$

This can be given explicitly in terms of cycles as follows:

$$(u \cup v)(g_1, \dots g_{m+n}) = (-1)^{mn} u(g_1, \dots g_m) \otimes g_1 g_2 \cdots g_m v(g_{m+1}, \dots g_{m+n})$$

Observe that if M is a G_K module, $M \otimes M^*$ maps naturally to $\mu(\overline{K})$, so if $M' = M^*$, cup product induces a map to $H^{m+n}(G_K, \mu(\overline{K}))$. If also K is a local field, we have:

Proposition 5. $H^2(G_K, \mu(\overline{K})) = \mathbb{Q}/\mathbb{Z}$

This means that for M a G_K module with K a local field, the cup product induces a map

$$H^i(G_K, M) \times H^{2-i}(G_K, M^*) \to \mathbb{Q}/\mathbb{Z}$$

Then **Tate Local Duality** states:

Theorem 2. *For a finite Galois module M over a local field K, the cup product induces a perfect pairing between $H^i(G_K, M)$ and $H^{2-i}(G_K, M^*)$. Thus, it induces an isomorphism of Galois modules*

$$H^i(G_K, M)^\vee \cong H^{2-i}(G_K, M^*)$$

Note that in particular, everything beyond H^2 vanishes for such a module.

5. Selmer and Shafarevich-Tate Groups of an Abelian Variety

Let A be an abelian variety over a number field K. Then we can consider $A(\overline{K})$, the $\overline{K}$-valued points of A, to be a G_K-module. We write $A[m]$ for $A(\overline{K})[m]$, the full group of m-torsion points of A.

Then the Kummer sequence

$$0 \to A[m] \to A(\overline{K}) \to A(\overline{K}) \to 0$$

is exact, where the frist map is inclusion and the second is multiplication by m.

For every place ν of K, we define a restriction map res_ν from $H^k(G_K, A(\overline{K}))$ to $H^k(G_{K_\nu}, A(\overline{K_\nu}))$; this map is the composition of the usual restriction map from $H^k(G_K, A(\overline{K}))$ to $(H^k(G_{K_\nu}, A(\overline{K}))$ induced by the inclusion $G_{K_\nu} \hookrightarrow G_K$, composed with the map from $H^k(G_{K_\nu}, A(\overline{K}))$ to $H^k(G_{K_\nu}, A(\overline{K_\nu}))$ induced by the inclusion of $A(\overline{K}) \hookrightarrow A(\overline{K_\nu})$. Then we define the following groups:

Definition 5. *The* **Shafarevich-Tate group of** A **over** K*, written* $Ш(A/K)$*, is the kernel of the map from* $H^1(G_K, A(\overline{K}))$ *to* $\prod_\nu H^1(G_{K_\nu}, A(\overline{K_\nu}))$*, where the product is taken over all places of* K*, and each map in the product is the* res_ν *map.*

Definition 6. *The* m**-Selmer group of** A **over** K*, written* $\mathrm{Sel}_m(A/K)$*, is the subgroup of* $H^1(G_K, A[m])$ *which maps to* $Ш(A/K)$ *under the map on* H^1 *induced by the inclusion* $A[m] \hookrightarrow A(\overline{K})$*.*

Proposition 6. *The following is an exact sequence:*

$$0 \to A(K)/mA(K) \to \mathrm{Sel}_m(A/K) \to Ш(A/K)[m] \to 0$$

The Shafarevich-Tate group is motivated by an important geometric description:

Proposition 7. $H^1(G_K, E\overline{K})$ *is in bijection with the set of isomorphism classes of curves over* K *having Jacobian* E*, called the* **Weil-Chateler group of** E **over** K*, and denoted* $WC(E/K)$*.*

The trivial class is, under this correspondence, the class of curves isomorphic to E. The Shafarevich-Tate group is therefore the set of isomorphism class of curves whose Jacobian is E and which are themselves isomorphic to E everywhere locally. Since a curve of genus one is isomorphic to its Jacobian if and only it has a point over K, this is also the same thing (using slightly sloppy language which is actually fine due to the group law induced by H^1) as curves over K with Jacobian E and a rational point everywhere locally, modulo curves with a global K-ration point. Thus, it is a measure of the failure of the Hasse principle.

Definition 7. *For a* G_K *module* M*, and a place* ν *of* K*, we say that a subgroup of* $H^k(G_K, M)$ *is* **unramified at** ν *if it is contained in the kernel of the restriction map from* $H^k(G_K, M)$ *to* $H^k(I_{K_\nu}, M)$ *induced by inclusion* $I_{K_\nu} \hookrightarrow G_K$*, where* I_{K_ν} *is the inertial subgroup of* G_{K_ν}*.*

Then the Selmer groups of abelian varieties have a rather nice property:

Theorem 3. *For any abelian variety* A*,* $\mathrm{Sel}_m(A/K)$ *is unramified outside* S*, where* S *is the set of places containing those which divide* m*, those where* A *has bad reduction, and the infinite places.*

This can be shown to imply that:

Theorem 4. *For any abelian variety* A*,* $\mathrm{Sel}_m(A/K)$ *is finite.*

Conjecture 1. *For any elliptic curve E, $Ш(E/K)$ is finite.*

This conjecture is made a modicum more approachable by the fact that $H^1(G_K, E(\overline{K}))$, as the cohomology of a discrete Galois module, is entirely torsion, and therefore so is $Ш(E/K)$. This means that controlling the relationship between $E(K)/mE(K)$ and $\mathrm{Sel}_m(E/K)$ can be used to prove the finiteness of Ш. Unfortunately, while one can hope to show that the p-part of Ш is trivial almost everywhere by showing $E(K)/pE(K) \cong \mathrm{Sel}_p(E/K)$, at the places p where Ш isn't trivial, the finiteness of the Selmer group at those places doesn't suffice to prove that Ш will be finite, as the p-part isn't known to be finitely generated, and could be infinite even if all p^n torsion is finite. Thus, at the p where Ш isn't trivial, some rather delicate calculations are necessary with $E(K)/p^nE(K)$ and $\mathrm{Sel}_{p^n}(E/K)$ at all powers of p.