Galois Cohomology

John Tate

Contents

IAS/Park City Mathematics Series
Volume 00, 0000

Galois Cohomology

John Tate[1]

I thank Helena Verrill and William Stein for their help in getting this account of my talks at Park City into print. After Helena typed up her original notes of the talks, William was a great help with the editing, and put them in the canonical format for this volume.

The somewhat inefficient organization of this account is mainly a result of the fact that, after the first talk had been given with the idea that it was to be the only one, a second was later scheduled, and these are the notes of the material in the two talks in the order it was presented.

The bible for this subject is Serre [**6**], in conjunction with [**5**] or [**1**]. Haberland [**2**] is also an excellent reference.

1. Group modules

Consider a group G and an abelian group A equipped with a map

$$G \times A \to A,$$
$$(\sigma, a) \mapsto \sigma a.$$

We use notation σ, τ, $\rho, \ldots$ for elements of G, and a, b, a', $b', \ldots$ for elements of A. To say that A is a G*-set* means that

$$\tau(\sigma a) = (\tau\sigma)a \quad \text{and} \quad 1a = a,$$

for all $\sigma, \tau \in G$ and $a \in A$, where 1 is the identity in G. To say that A is a G*-module* means that, in addition, we have

$$\sigma(a+b) = \sigma a + \sigma b,$$

for all $\sigma \in G$ and $a, b \in A$. This is all equivalent to giving A the structure of $\mathbf{Z}[G]$-module.

Given a G-module A as above, the subgroup of fixed elements of A is

$$A^G := \{a \in A \mid \sigma a = a \text{ for all } \sigma \in G\}.$$

[1]Department of Mathematics; Austin, TX.
E-mail address: `tate@math.utexas.edu`.
1991 *Mathematics Subject Classification.* 11.
Key words and phrases. Galois cohomology, Elliptic curves.

We say G *acts trivially* on A if $\sigma a = a$ for all $a \in A$; thus $A^G = A$ if and only if the action is trivial. When $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Q}/\mathbf{Z}$ are considered as G-modules, this is with the trivial action, unless stated otherwise.

If we take $G = \mathrm{Gal}(K/k)$, with K a Galois extension of k of possibly infinite degree, then we have the following examples of fixed subgroups of G-modules:

A	A^G
K^+ as an additive group	k^+
K^* as a multiplicative group	k^*
$E(K)$, where E/k is an elliptic curve	$E(k)$.

The action on $E(K)$ above is given by $\sigma(x,y) = (\sigma x, \sigma y)$ for a point $P = (x,y)$, if E is given as a plane cubic. In general, if C is a commutative algebraic group over K, we can take $A = C(K)$, and then $A^G = C(k)$.

2. Cohomology

We now define the cohomology groups $H^r(G,A)$, for $r \in \mathbf{Z}$. Abstractly, these are the right derived functors of the left exact functor

$$\{G\text{-modules}\} \to \{\text{abelian groups}\}$$

that sends $A \mapsto A^G$. Since $A^G = \mathrm{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}, A)$, we have a canonical isomorphism

$$H^r(G,A) = \mathrm{Ext}^r_{\mathbf{Z}[G]}(\mathbf{Z}, A).$$

More concretely, the cohomology groups $H^r(G,A)$ can be computed using the "standard cochain complex" (see, e.g., [**1**, pg. 96]). Let

$$C^r(G,A) := \mathrm{Maps}(G^r, A);$$

an element of $C^r(G,A)$ is a function f of r variables in G,

$$f(\sigma_1, \ldots, \sigma_r) \in A,$$

and is called an *r-cochain*. (If, in addition, A and G have a topological structure, then we instead consider continuous cochains.) There is a sequence

$$\cdots \to 0 \to 0 \to C^0(G,A) \xrightarrow{\delta} C^1(G,A) \xrightarrow{\delta} C^2(G,A) \xrightarrow{\delta} \cdots$$

Here $C^0(G,A) = A$, since an element f of $C^0(G,A)$ is given by the single element $f_0(\bullet) \in A$, its value at the unique element $\bullet \in G^0$. The maps δ are defined by

$$\begin{array}{lcl} (\delta f_0)(\sigma) & = & \sigma f_0(\bullet) - f_0(\bullet), \\ (\delta f_1)(\sigma,\tau) & = & \sigma f_1(\tau) - f_1(\sigma\tau) + f_1(\sigma), \\ (\delta f_2)(\sigma,\tau,\rho) & = & \sigma f_2(\tau,\rho) - f_2(\sigma\tau,\rho) + f_2(\sigma,\tau\rho) - f_2(\sigma,\tau), \end{array}$$

and so on. Note that $\delta \circ \delta = 0$. The cohomology groups are given by

$$H^r(G,A) = \ker\delta / \operatorname{im}\delta \subset C^r(G,A)/\operatorname{im}\delta.$$

Cocycles are elements of the kernel of δ, and coboundaries are elements of the image of δ. We have

$$\begin{array}{lcl} H^0(G,A) & = & A^G, \\ H^1(G,A) & = & \frac{\text{crossed-homomorphisms}}{\text{principal crossed-homomorphisms}} \\ & = & \mathrm{Hom}(G,A), \text{ if action is trivial,} \\ H^2(G,A) & = & \text{classes of "factor sets"}. \end{array}$$

The groups $H^2(G, A)$ and $H^1(G, A)$ arise in many situations. Perhaps the simplest is their connection with group extensions and their automorphisms. Given a G-module A, suppose $\mathcal{G}$ is a group extension of G by A, that is, $\mathcal{G}$ is a group which contains A as a normal subgroup such that $\mathcal{G}/A \cong G$, where the given action of G on A is the same as the conjugation action induced by this isomorphism. Construct a 2-cocycle $a_{\sigma,\tau}$ as follows. For each element $\sigma \in G$, let $u_\sigma \in \mathcal{G}$ be a coset representative corresponding to σ. Then $\mathcal{G} = \coprod_\sigma Au_\sigma$, i.e., every element of $\mathcal{G}$ is uniquely of the form au_σ. Thus

$$u_\sigma u_\tau = a_{\sigma,\tau} u_{\sigma\tau}$$

for some $a_{\sigma,\tau} \in A$. The map $(\sigma, \tau) \mapsto a_{\sigma,\tau}$ is a 2-cocycle.

Exercise 2.1. Using the associative law, check that $a_{\sigma,\tau}$ is a 2-cocycle, and if $\mathcal{G}'$ is another extension of G by A, then there is an isomorphism $\mathcal{G}' \cong \mathcal{G}$ that induces the identity on A and G if and only if the corresponding 2-cocycles differ by a coboundary.

Exercise 2.2. Conversely, show that every 2-cocycle arises in this way. For example, in the trival case, if $a_{\sigma,\tau} = 1$ for every σ and τ, then we can take $\mathcal{G}$ to be the semidirect product $G \ltimes A$.

Therefore we may view $H^2(G, A)$ as the group of isomorphism classes of extensions of G by A with a given action of G on A.

Exercise 2.3. Show that an automorphism of $\mathcal{G}$ that induces the identity on A and on $G = \mathcal{G}/A$ is of the form $au_\sigma \mapsto ab_\sigma u_\sigma$ with $\sigma \mapsto b_\sigma$ a 1-cocycle, and it is an inner automorphism induced by an element of A if and only if $\sigma \mapsto b_\sigma$ is a coboundary.

2.1. Examples

Given a finite Galois extension K/k, and a commutative algebraic group C over k, the following notation is frequently used:

$$H^r(K/k, C) := H^r(\mathrm{Gal}(K/k), C(K)).$$

We have $H^0(K/k, C) = C(k)$ as above, and

$$\begin{aligned} H^1(K/k, \mathbf{G}_m) &= H^1(K/k, K^*) = 0, \\ H^2(K/k, \mathbf{G}_m) &= \mathrm{Br}(K/k) \subset \mathrm{Br}(k) \end{aligned}$$

The first equality is Hilbert's Theorem 90. In the second equality $\mathrm{Br}(k)$ is the Brauer group of k; this is the group of equivalence classes of central simple algebras with center k that are finite dimensional over k; two such algebras are equivalent if they are matrix algebras over k-isomorphic division algebras.

The map from $H^2(K/k, \mathbf{G}_m)$ to $\mathrm{Br}(K/k)$ is defined as follows. Given a 2-cocycle $a_{\sigma,\tau}$, define a central simple algebra over k by $\mathcal{A} = \oplus K u_\sigma$, which is a vector spaces over K with a basis $\{u_\sigma\}$ indexed by the elements $\sigma \in G$. Multiplication is defined by the same rules as for group extensions above (with $A = K^*$), extended linearly.

2.2. Characterization of $H^r(G,-)$

For fixed G and varying A the groups $H^r(G,A)$ have the following fundamental properties:

1. $H^0(G,A) = A^G$.
2. $H^r(G,-)$ is a functor
$$\{G\text{-modules}\} \to \{\text{abelian groups}\}\,.$$
3. Each short exact sequence
$$0 \to A' \to A \to A'' \to 0$$
gives rise to connecting homomorphisms (see below)
$$\delta : H^r(G,A'') \to H^{r+1}(G,A')$$
from which we get a long exact sequence of cohomology groups, functorial in short exact sequences in the natural sense.
4. If A is "induced" or "injective", then $H^r(G,A) = 0$ for all $r \neq 0$.

These properties characterize the sequence of functors H^i equipped with the δ's uniquely, up to unique isomorphism.

For $c \in H^r(G,A'')$, define $\delta(c)$ as follows. Let $c_1 : G^r \to A''$ be a cocycle representing c. Lift c_1 to any map (cochain) $c_2 : G^r \to A$. Since $\delta(c_1) = 0$, the map $\delta(c_2) : G^{r+1} \to A$ has image in A', so defines a map $\delta(c_2) : G^{r+1} \to A'$, and thus represents a class $\delta(c) \in H^{r+1}(G,A')$.

For an infinite Galois extension, one uses cocycles that come by inflation from finite Galois subextensions. This amounts to using continuous cochains, where continuous means with respect to the Krull topology on G and the discrete topology on A.

Abstracting this situation leads to the notion of the cohomology of a profinite group G (i.e., a projective limit, in the category of topological groups, of finite groups G_i) operating continuously on a discrete module A. Without loss of generality the G_i can be taken to be the quotients G/U of G by its open normal subgroups U, and then A is the union of its subgroups A^U. The cohomology groups $H^r(G,A)$ computed with continuous cochains are direct limits, relative to the inflation maps (see Section 6), of the cohomology groups $H^r(G/U,A^U)$ of the finite quotients, because the continuous cochain complex $C^*(G,A)$ is the direct limit of the complexes $C^*(G/U,A^U)$. Also, it is easy to see that the groups $\{H^r(G,-)\}_r$ are characterized by δ-functoriality on the category of *discrete* G-modules.

3. Kummer theory

Let k^{sep} be a separable closure of a field k, and put $G_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Let $m \geq 1$ be an integer, and assume that the image of m in k is nonzero. Associated to the exact sequence
$$0 \longrightarrow \mu_m \longrightarrow (k^{\mathrm{sep}})^* \xrightarrow{m} (k^{\mathrm{sep}})^* \longrightarrow 0,$$
we have a long exact sequence
$$0 \longrightarrow \mu_m \cap k \longrightarrow k^* \xrightarrow{m} k^* \longrightarrow H^1(G_k,\mu_m) \longrightarrow H^1(G_k,(k^{\mathrm{sep}})^*) = 0,$$

where the last equality is by Hilbert's Theorem 90. Thus $H^1(G_k, \mu_m) \cong k^*/(k^*)^m$.

Now assume that the group of mth roots of unity μ_m is contained in k. Then

$$H^1(G_k, \mu_m) = \mathrm{Hom}_{\mathrm{cont}}(G_k, \mu_m),$$

so

$$k^*/(k^*)^m \cong \mathrm{Hom}_{\mathrm{cont}}(G_k, \mu_m).$$

Using duality, this isomorphism describes the finite abelian extensions of k whose Galois group is killed by m. For example, consider a Galois extension K/k such that $G = \mathrm{Gal}(K/k)$ is a finite abelian group that is killed by m. Since G is a quotient of $G_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$, we have a diagram

$$\begin{tikzcd} k^*/(k^*)^m \arrow[r, "\cong"] & \mathrm{Hom}_{\mathrm{cont}}(G_k, \mu_m) \\ B \arrow[u] \arrow[r, "\cong"] & \widehat{G} := \mathrm{Hom}(G, \mu_m), \arrow[u] \end{tikzcd}$$

where B is the subgroup of $k^*/(k^*)^m$ corresponding to $\widehat{G}$ under the isomorphism.

Exercise 3.1. Show that

$$K = k(\sqrt[m]{B}) = k(\{\sqrt[m]{b} \mid b \in B\}),$$

and $[K : k] = \#B$.

The case when G cyclic is the crucial step in showing that a polynomial with solvable Galois group can be solved by radicals.

For the rest of this section, we assume that k is a number field and continue to assume that k contains μ_m. Let S be a finite set of primes of k including all divisors of m and large enough so that the ring $\mathcal{O}_S$ of S-integers of k is a principal ideal ring.

Exercise 3.2. Show that the extension $K(\sqrt[m]{B})$ above is unramified outside S if and only if $B \subset U_S k^{*m}/k^{*m} \cong U_S/U_S^m$, where $U_S = \mathcal{O}_S^*$ is the group of S-units of k.

Exercise 3.3. Let k_S be the maximal extension of k which is unramified outside S, and let $G_S = \mathrm{Gal}(k_S/k)$. Then $\mathrm{Hom}_{\mathrm{cont}}(G_S, \mu_m) = U_S/U_S^m$. It follows that $\mathrm{Hom}_{\mathrm{cont}}(G_S, \mu_m)$ is finite, because U_S is finitely generated.

Now let E be an elliptic curve over k. The m-torsion points of E over $\overline{k}$ form a group $E_m = E_m(\overline{k}) \approx (\mathbf{Z}/m\mathbf{Z})^2$. Suppose that, in addition to the conditions above, S also contain the places at which E has bad reduction. Then it is a fact that $E(k_S)$ is divisible by m, so we have an exact sequence

$$0 \to E_m \to E(k_S) \xrightarrow{m} E(k_S) \to 0.$$

Taking cohomology we obtain an exact sequence

$$0 \to E(k)/mE(k) \to H^1(k_S/k, E_m) \to H^1(k_S/k, E)_m \to 0,$$

where the subscript m means elements killed by m. Thus, to prove that $E(k)/mE(k)$ is finite (the "weak Mordell-Weil theorem"), it suffices to show that $H^1(k_S/k, E_m)$

is finite. Let $k' = k(E_m)$ be the extension of k obtained by adjoining the coordinates of the points of order m. Then k'/k is finite and unramified outside S. Hence $H^1(k'/k, E_m)$ is finite, and the exact inflation-restriction sequence (see Section 6)

$$0 \to H^1(k'/k, E_m) \to H^1(k_S/k, E_m) \to H^1(k_S/k', E_m)$$

shows that it suffices to prove $H^1(k_S/k, E_m)$ is finite when $k = k'$. But then

$$H^1(k_S/k, E_m) \cong \mathrm{Hom}_{\mathrm{cont}}(G_S, E_m) \cong \mathrm{Hom}_{\mathrm{cont}}(G_S, \mu_m)^2$$

is finite by Exercise 3.3.

Exercise 3.4. Take $k = \mathbf{Q}$ and let E be the elliptic curve $y^2 = x^3 - x$. Let $m = 2$ and $S = \{2\}$, $U_S = \langle -1, 2\rangle$, and show $(E(\mathbf{Q}) : 2E(\mathbf{Q})) \leq 16$. (In fact, $E(\mathbf{Q}) = E_2$ is of order 4, killed by 2, but to show that we need to examine what happens over $\mathbf{R}$ and over $\mathbf{Q}_2$, not just use the lack of ramification at the other places.)

Exercise 3.5. Suppose $S' = S \cup \{P_1, P_2, \ldots, P_t\}$ is obtained by adding t new primes to S. Then $U_{S'} \cong U_S \times \mathbf{Z}^t$. Hence $H^1(k_{S'}/k, E)_m \cong H^1(k_S/k, E) \times (\mathbf{Z}/m\mathbf{Z})^{2t}$. Hence $H^1(k, E)$ contains an infinite number of independent elements of order m. Hilbert Theorem 90 is far from true for E.

4. Functor of pairs (G, A)

A *morphism of pairs* $(G, A) \mapsto (G', A')$ is given by a pair of maps ϕ and f,

$$G \xleftarrow{\phi} G' \quad \text{and} \quad A_\phi \xrightarrow{f} A'\ ,$$

where ϕ is a group homomorphism, and f is a homomorphism of G'-modules, and A_ϕ means A with the G' action induced by ϕ. A morphism of pairs induces a map

$$H^r(G, A) \to H^r(G', A')$$

got by composing the map $H^r(G, A) \to H^r(G', A_\phi)$ induced by ϕ with the map $H^r(G', A_\phi) \to H^r(G', A')$ induced by f. We thus consider $H^r(G, A)$ as a functor of pairs (G, A).

If G' is a subgroup of G then there are maps

$$\begin{tikzcd} H^r(G, A) \arrow[r, bend left, "\text{restriction}"] & H^r(G', A). \arrow[l, bend left, "\text{corestriction}"] \end{tikzcd}$$

Here the corestriction map (also called the "transfer map") is defined only if the index $[G : G']$ is finite.

When $r = 0$ the corestriction map is the trace or norm:

$$\begin{tikzcd} K \arrow[dd, "G"'] \arrow[dr, dash, "G'"] & \\ & K' \arrow[dl, dash] \\ k & \end{tikzcd} \qquad \begin{tikzcd} A^G \arrow[r, bend left, "\text{res}"] & A^{G'} \arrow[l, bend left, "\text{cores}"] \end{tikzcd}$$

$$\sum_{g \in \{\text{coset reps for } G/G'\}} ga \longleftarrow\!\shortmid\ a.$$

Corollary 4.1. *If G is of finite cardinality m, then*

$$mH^r(G, A) = 0 \text{ for } r \neq 0.$$

Proof. Letting $G' = \{1\}$, we have

$$(\text{corestriction}) \circ (\text{restriction}) = [G : G'] = [G : \{1\}] = m.$$

Since $H^r(\{1\}, A) = 0$ for $r \neq 0$, this composition is 0, as claimed. □

Exercise 4.2. Restriction to a p-Sylow subgroup is injective on the p-primary component of $H^r(G, A)$.

5. The Shafarevich group

Let k be a number field, ν a place of k, and k_ν the completion of k at ν. Let $\overline{k}_\nu$ be an algebraic closure of k_ν and let $\overline{k}$ be the algebraic closure of k in $\overline{k}_\nu$. These four fields are illustrated in the following diagram.

$$\begin{tikzcd}
& \overline{k}_\nu \arrow[dl, dash] \arrow[dr, dash, "G_\nu"] & \\
\overline{k} \arrow[dr, dash, "G_k"'] & & k_\nu \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

Let E be an elliptic curve over k. We have natural morphisms of pairs

$$(G_k, E(\overline{k})) \to (G_\nu, E(\overline{k}_\nu)),$$

for each place ν, hence a homomorphism

$$H^1(k, E) \to \prod_\nu H^1(k_\nu, E),$$

where the product is taken over all places of k. The kernel of this map is the Shafarevich group Ш(k, E), which is conjectured to be finite.

If you can prove that Ш is finite, then you will be famous, and you will have shown that the descent algorithm to compute the Mordell-Weil group, which seems to work in practice, will always work. Until 1986, there was no single instance where it was known that Ш was finite! Now much is known for $k = \mathbf{Q}$ if the rank of $E(\mathbf{Q})$ is 0 or 1; see [**3**] and [**4**] for results in this direction. Almost nothing is known for higher ranks.

6. The inflation-restriction sequence

Recall that a morphism of pairs

$$(G, A) \to (G', A')$$

is a map $G' \to G$ and a G'-homomorphism $A \to A'$, where G' acts on A via $G' \to G$. In particular, we can take G' to be a subgroup H of G. Here are three special instances of the above map:

1)	restriction	$H^r(G, A) \to H^r(H, A)$
2)	inflation	$H^r(G/H, A^H) \to H^r(G, A)$
		(for $H \triangleleft G$, $G \to G/H$, $A^H \subset A$)
3)	conjugation	$H^r(H, A) \xrightarrow{\tilde{\sigma}} H^r(\sigma H \sigma^{-1}, A)$, $\sigma \in G$
		(for $\sigma h \sigma^{-1} \mapsto h$ and $a \mapsto \sigma a$)

Theorem 6.1. *If $\sigma \in H$, then the conjugation map $\tilde{\sigma}$ is the identity.*

Exercise 6.2. Given a commutative algebraic group C defined over k one sometimes uses the notation $H^r(k, C) := H^r(k^{\mathrm{sep}}/k, C)$, where k is a separable algebraic closure of k. Show that this makes sense, in the sense that if k_1^s and k_2^s are two separable closures of k, then the isomorphism $H^r(\mathrm{Gal}(k_1^s/k), C(k_1^s)) \cong H^r(\mathrm{Gal}(k_2^s/k), C(k_2^s))$ induced by a k-isomorphism $\varphi : k_1^s \to k_2^s$ is independent of the choice of φ.

Theorem 6.3. *If H is a normal subgroup of G, then there is a "Hochschild-Serre" spectral sequence*

$$E_2^{rs} = H^r(G/H, H^s(H, A)) \Rightarrow H^{r+s}(G, A)$$

By Theorem 6.1, G acts on $H^r(H, A)$ and H acts trivially, so this makes sense. (The profinite case follows immediately from the finite one by direct limit; cf. the end of Section 2.2.) The low dimensional corner of the spectral sequence can be pictured as follows.

$$\begin{tikzcd}
E^{02} \arrow[d, dash] \arrow[dr, dash] & & \\
E^{01} \arrow[r, dash] \arrow[d, dash] \arrow[dr, dash] & E^{11} \arrow[d, dash] \arrow[dr, dash] & \\
E^{00} \arrow[r, dash] & E^{10} \arrow[r, dash] & E^{20}
\end{tikzcd}$$

Inflation and restriction are "edge homomorphisms" in the spectral sequence. The lower left corner pictured above gives the obvious isomorphism $A^G \cong (A^H)^{G/H}$, and the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & H^1(G/H, A^H) \arrow[r, "\mathrm{inf}"] & H^1(G, A) \arrow[r, "\mathrm{res}"] & H^1(H, A)^{G/H} \arrow[dll, rounded corners, to path={-- ([xshift=2ex]\tikztostart.east) |- node[above, pos=0.75]{d} ([yshift=-3ex]\tikztostart.south) -| ([xshift=-4ex]\tikztotarget.west) -- (\tikztotarget)}] \\
& H^2(G/H, A^H) \arrow[r, "\mathrm{inf}"] & H^2(G, A). &
\end{tikzcd}$$

The map d is the "transgression" and is induced by $d_2 : E_2^{01} \to E_2^{20}$.

Exercise 6.4.

1. Show that this last sequence, or at least the first line, is exact by using standard 1-cocycles.
2. If $H^1(H, A) = 0$, so that $E_2^{r1} = 0$ for all r, then the sequence obtained by increasing the superscripts on the H's by 1 is exact.

Consider a subfield K of k^{sep} that is Galois over k, and let C be a commutative algebraic group over k.

$$\begin{tikzcd}
& k^{\mathrm{sep}} \arrow[d, dash] \arrow[d, dash, bend left, "G_K"] \arrow[dd, dash, bend right, "G_k"'] \\
& K \arrow[d, dash] \\
C \arrow[r, dash] & k.
\end{tikzcd}$$

The inflation-restriction sequence is

$$0 \longrightarrow H^1(K/k, C(K)) \longrightarrow H^1(k, C(k^{\mathrm{sep}})) \longrightarrow H^1(K, C(k^{\mathrm{sep}}))^{\mathrm{Gal}(K/k)} \longrightarrow H^2(K/k, C(K)) \longrightarrow H^2(k, C(k^{\mathrm{sep}})).$$

If $C = \mathbf{G}_m$, then $H^1(K, C(k^{\mathrm{sep}})) = 0$, and there is an inflation-restriction sequence with $(1,2)$ replaced by $(2,3)$:

$$0 \longrightarrow H^2(K/k, K^*) \longrightarrow H^2(k, (k^{\mathrm{sep}})^*)) \longrightarrow H^2(K, (k^{\mathrm{sep}})^*))^{\mathrm{Gal}(K/k)} \longrightarrow H^3(K/k, K^*) \longrightarrow H^3(k, (k^{\mathrm{sep}})^*).$$

An element $\alpha \in H^2(K, (k^{\mathrm{sep}})^*)^{\mathrm{Gal}(K/k)}$ represents a central simple algebra A over K which is isomorphic to all of its conjugates by $\mathrm{Gal}(K/k)$. As the diagram indicates, the image α in $H^3(K/k, K^*)$ is the "obstruction" whose vanishing is the necessary and sufficient condition for such an algebra A to come by base extension from an algebra over k.

7. Cup products

7.1. G-pairing

If A, A', and B are G-modules, then

$$A \times A' \xrightarrow{b} B$$

is a *G-pairing* if it is bi-additive, and respects the action of G:

$$b(\sigma a, \sigma a') = \sigma b(a, a').$$

Such a pairing induces a map $\tilde{b}$

$$\cup : H^r(G, A) \times H^s(G, A') \xrightarrow{\tilde{b}} H^{r+s}(G, B),$$

as follows: given cochains f and f', one defines (for a given b) a cochain $f \cup f'$ by

$$(f \cup f')(\sigma_1, \ldots, \sigma_{r+s}) = b(f(\sigma_1, \ldots, \sigma_r), \sigma_1 \ldots \sigma_r f'(\sigma_{r+1}, \ldots, \sigma_{r+s})),$$

and checks the rule

$$\delta(f \cup f') = \delta f \cup f' + (-1)^r f \cup \delta f'.$$

If $\delta f = \delta f' = 0$, then also $\delta(f \cup f') = 0$; i.e., if f and f' are cocycles, so is $f \cup f'$. Similarly one checks that the cohomology class of $f \cup f'$ depends only on the classes of f and f'. Thus we obtain the desired pairing $\tilde{b}$.

If $r = 0$ and $a \in A^G$ is fixed, then $a' \mapsto b(a, a')$ defines a G-homomorphism $\varphi_a : A' \to B$, and $\alpha' \mapsto a \cup \alpha'$ is the map $H^r(G, A') \to H^r(G, B)$ induced by φ_a.

If H is a subgroup of G, and $\alpha \in H^r(G, A)$ and $\beta \in H^s(H, A')$, then we can form

$$\mathrm{res}(\alpha) \cup \beta \in H^{r+s}(H, B).$$

Suppose that the index of H in G is finite, so that corestriction is defined; then one can show that

$$\mathrm{cores}(\mathrm{res}(\alpha) \cup \beta) = \alpha \cup \mathrm{cores}(\beta) \in H^{r+s}(G, B).$$

7.2. Duality for finite modules

If A and B are G-modules, we make the group $\mathrm{Hom}_{\mathbf{Z}}(A,B)$ into a G-module by defining $(\sigma f)(a) = \sigma(f(\sigma^{-1}a))$. Note then that $\mathrm{Hom}_G(A,B) = (\mathrm{Hom}_{\mathbf{Z}}(A,B))^G$. Also, the obvious pairing $A \times \mathrm{Hom}_{\mathbf{Z}}(A,B) \to B$ is a G-pairing. The canonical map

$$(*) \qquad A \to \mathrm{Hom}_{\mathbf{Z}}(\mathrm{Hom}_{\mathbf{Z}}(A,B))$$

is a G-homomorphism. In case A is finite, killed by m, and B has a unique cyclic subgroup of order m, the map $(*)$ is an isomorphism; one can thus recover A from its "dual" $\mathrm{Hom}_{\mathbf{Z}}(A,B)$ which has the same order as A. There are two especially important such duals for finite A.

- The *Pontrjagin Dual* of A is $\mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$; this equals $\mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Z}/m\mathbf{Z})$ if $mA = 0$.
- The *Cartier Dual* of A is $\mathrm{Hom}_{\mathbf{Z}}(A, \mu(k^{\mathrm{sep}}))$; this equals $\mathrm{Hom}_{\mathbf{Z}}(A, \mu_m(k^{\mathrm{sep}}))$ if $mA = 0$.

In the Pontrjagin case, G is an arbitrary profinite group and acts trivially on $\mathbf{Q}/\mathbf{Z}$. Taking limits, this duality extends to a perfect duality (i.e., an anti-equivalence of categories) between discrete abelian torsion groups and profinite abelian groups.

In the Cartier case, $G = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ or some quotient thereof, and $m \neq 0$ in k. (The Cartier dual of a p-group in characteristic p is a *group scheme*, not just a Galois module.) If E is an elliptic curve over k and the image of m in k is nonzero, the *Weil pairing* $E_m(k^{\mathrm{sep}}) \times E_m(k^{\mathrm{sep}}) \to \mu_m$ identifies E_m with its Cartier dual.

8. Local fields

Let k be a local field, i.e., the field of fractions of a complete discrete valuation ring with finite residue field F. Let K be a finite extension of k.

Fundamental facts:

$$\begin{aligned} H^1(K/k, K^*) &= 0 \qquad \text{(Hilbert's Theorem 90)} \\ H^2(K/k, K^*) &= \mathbf{Z}/[K:k]\mathbf{Z} \\ H^2(k, \mathbf{G}_m) &= \mathrm{Br}(k) = \mathbf{Q}/\mathbf{Z} \end{aligned}$$

The equality $\mathrm{Br}(k) = \mathbf{Q}/\mathbf{Z}$ is given canonically, by the Hasse invariant, as follows: The group $\mathrm{Br}(k)$ is the Brauer group, defined in §2.1. Consider the inflation-restriction sequence for $H^2(-, \mathbf{G}_m)$ in the tower of fields

$$\begin{array}{c} \overline{k} \\ | \\ k^{\mathrm{ur}} \\ | \\ k \end{array}$$

where k^{ur} is the maximal unramified extension of k. Since every central division algebra over a local field has an unramified splitting field, we have $\mathrm{Br}(k^{\mathrm{ur}}) = 0$, and hence an isomorphism

$$\mathrm{Br}(k) \cong H^2(k^{\mathrm{ur}}/k, \mathbf{G}_m) = H^2(\mathrm{Frob}^{\widehat{\mathbf{Z}}}, (k^{\mathrm{ur}})^*).$$

Using the exact sequence

$$0 \longrightarrow U(k^{\mathrm{ur}}) \longrightarrow (k^{\mathrm{ur}})^* \xrightarrow{\text{valuation}} \mathbf{Z} \longrightarrow 0$$

and the fact that the unit group of an unramified extension has trivial cohomology in dimension $\neq 0$, we find that we can replace $(k^{\mathrm{ur}})^*$ by $\mathbf{Z}$, and hence

$$\mathrm{Br}(k) \cong H^2(\hat{\mathbf{Z}}, \mathbf{Z}) = H^1(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z};$$

the middle equality comes from the short exact sequence

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

and the fact that $\mathbf{Q}$, being uniquely divisible, has trivial cohomology in nonzero dimensions. The resulting map

$$\mathrm{Br}(k) \to \mathbf{Q}/\mathbf{Z}$$

is the called the Hasse invariant.

Theorem 8.1. *Let A be a finite G_k-module of order prime to the characteristic of k. Let*

$$A^* = \mathrm{Hom}(A, \mathbf{G}_m) = \mathrm{Hom}(A, \mu(\overline{k}))$$

be the Cartier dual of A. Then the G-pairing

$$A \times A^* \to \overline{k}^*$$

induces a pairing

$$H^r(k, A) \times H^{2-r}(k, A^*) \to H^2(G_k, (k^{\mathrm{sep}})^*) = \mathrm{Br}(k) = \mathbf{Q}/\mathbf{Z}.$$

This is a perfect pairing of finite groups, for all $r \in \mathbf{Z}$. It is nontrivial only if $r = 0, 1, 2$, since for $r \geq 3$,

$$H^r(k, A) = 0 \quad \textit{for all } A,$$

i.e., "the cohomological dimension of a non-archimedean local field is 2."

Example. By Kummer theory, we have

$$k^*/(k^*)^m = H^1(k, \mu_m(\overline{k})).$$

Thus there is a perfect pairing

$$\begin{array}{ccccc} H^1(k, \mathbf{Z}/m\mathbf{Z}) & \times & H^1(k, \mu_m(\overline{k})) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \\ \| & & \| & & \\ \mathrm{Hom}(G_k, \mathbf{Z}/m\mathbf{Z}) & \times & k^*/(k^*)^m & & \end{array}$$

The left hand equality is because the action is trivial. Conclusion:

$$G_k^{\mathrm{ab}}/(G_k^{\mathrm{ab}})^m \cong k^*/(k^*)^m.$$

Taking the limit gives *Artin reciprocity*:

$$k^* \hookrightarrow G_k^{ab}\ ;$$

the image is dense.

Let E/k be an elliptic curve. In some sense,

$$E = \mathrm{Ext}^1(E, \mathbf{G}_m)$$

in the category of algebraic groups. There is a pairing

$$H^r(k,E) \times H^s(k,E) \to H^{r+s+1}(k,\mathbf{G}_m).$$

For example, taking $r=0$ and $s=1$, we have the following theorem.

Theorem 8.2. *Let E be an elliptic curve over a non-archimedean local field k, then we have the following perfect pairing between Pontrjagin duals.*

$$\begin{array}{ccccc} H^0(k,E) & \times & H^1(k,E) & \longrightarrow & H^2(k,\mathbf{G}_m) = \mathbf{Q}/\mathbf{Z} \\ \| & & \| & & \\ E(k) & & H^1(k,E) & & \\ \textit{profinite} & \times & \textit{discrete, torsion} & & \end{array}$$

Sketch of Proof. We use the Weil pairing. Letting D denote "Pontrjagin dual", we have a diagram

$$\begin{tikzcd} 0 \arrow[r] & E(k)/mE(k) \arrow[r] \arrow[d] & H^1(k,E_m) \arrow[r] \arrow[d] & H^1(k,E)_m \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & H^1(k,E)_m^D \arrow[r] & H^1(k,E_m)^D \arrow[r] & (E(k)/mE(k))^D \arrow[r] & 0 \end{tikzcd}$$

The rows are exact. The top one from the Kummer sequence, and the bottom is the dual of the top one. The middle vertical arrow is an isomorphism by Theorem 8.1. The outside vertical arrows are induced by the pairing of Theorem 8.2. The diagram commutes, so they are also isomorphisms, and Theorem 8.2 follows by passage to the limit with more and more divisible m. $\square$

It was in trying to prove Theorem 8.2 that I was led to Theorem 8.1 in the late 1950's. Of course the "fundamental facts" and the Artin isomorphism are a much older story.

BIBLIOGRAPHY

1. J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.
2. K. Haberland, *Galois cohomology of algebraic number fields*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978, With two appendices by Helmut Koch and Thomas Zink.
3. V. A. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990) (Tokyo), Math. Soc. Japan, 1991, pp. 429–436.
4. K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.
5. J-P. Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.
6. ———, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.