Galois cohomology seminar
Week 10 - Cohomology and central simple algebras

Joshua Ruiter

March 31, 2019

Contents

1 Two-step outline of $\mathrm{Br}(K) \cong H^2(G_K, (K^{\mathrm{sep}})^\times)$

Our next goal is to describe the isomorphism

$$\mathrm{Br}(K) \cong H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times)$$

More generally, for any Galois extension L/K,

$$\mathrm{Br}(L/K) \cong H^2(\mathrm{Gal}(L/K), L^\times)$$

and the first isomorphism is the case $L = K^{\mathrm{sep}}$. We won't have time to go into all the details, since it involves a lot of them, and the details don't do much to illustrate the ideas, at least for me. We will try to outline the construction of the isomorphism, at least. Here is a first approximation outline.

1. For a **finite** Galois extension L/K, construct a group isomorphism
$$\beta_{L/K} : \mathrm{Br}(L/K) \to H^2(\mathrm{Gal}(L/K), L^\times) \qquad [A] \mapsto [\{a_{\sigma,\tau}\}]$$
2. Extend the isomorphism to infinite Galois extensions via an isomorphism of directed systems.

The hard part is step 1. Each of the following 5 steps takes about a page of detailed work:

(1a) Definition of $\beta_{L/K}$

(1b) Showing that construction gives a cocycle

(1c) Injectivity of $\beta_{L/K}$

(1d) Surjectivity of $\beta_{L/K}$

(1e) Homomorphism property of $\beta_{L/K}$

In order to see the benefits of going through step 1, first we'll go through how it gets used in step 2. Then we'll describe some of (1a) and (1d), and mostly skip the rest of these details.

2 Details of step 2

In contrast to step 1, step 2 is not so bad. Since it mostly involves the tools that Nick talked about last time, let's talk about it first. We will end up with two directed systems, on one side a system of cohomology groups of Galois groups acting on the nonzero elements of fields, and on the other side a system of relative Brauer groups.

2.1 Directed system of cohomology groups

We've already described the cohomology side, but let's remember the details. Recall a result from profinite group cohomology that Stan proved.

Proposition 2.1. *Let G be a profinite group, and let $\mathcal{U}$ be the set of open normal subgroups of G. Let A be a discrete G-module. Then*
$$H^i(G, A) \cong \varinjlim_{N \in \mathcal{U}} H^i(G/N, A^N)$$
where the maps of the directed system are inflation maps.

The case we care most about here is when L/K is an infinite Galois extension, since this says that the profinite group cohomology of $\mathrm{Gal}(L/K)$ is determined by the group cohomology of Galois groups of finite Galois subextensions. If L/K is infinite Galois, the set of open normal subgroups of G is the set of subgroups $\mathrm{Gal}(L/E)$ where E/K is finite Galois, so the isomorphism becomes

$$H^i(\mathrm{Gal}(L/K), L^\times) \cong \varinjlim_{E\in\mathcal{E}} H^i\left(\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/E)}, (L^\times)^{\mathrm{Gal}(L/E)}\right) \cong \varinjlim_{E\in\mathcal{E}} H^i(\mathrm{Gal}(E/K), E^\times)$$

For $E_1, E_2 \in \mathcal{E}$ with $E_1 \subset E_2$, the maps of the directed system are the inflation maps

$$\theta_2^1 = \mathrm{Inf} : H^2(\mathrm{Gal}(E_1/K), E_1^\times) \to H^2(\mathrm{Gal}(E_2, K), E_2^\times)$$

As an aside, this map is induced by restriction maps

$$\mathrm{Gal}(E_2/K) \to \mathrm{Gal}(E_1/K) \qquad \sigma \mapsto \sigma|_{E_1}$$

in the following way. If $\phi : \mathrm{Gal}(E_1/K)^2 \to E_1^\times$ is a 2-cocycle, then for $\sigma, \tau \in \mathrm{Gal}(E_2/K)$,

$$\Big(\theta_2^1(\phi)\Big)(\sigma, \tau) = \phi(\sigma|_{E_1}, \tau|_{E_1})$$

Ok, the previous equation isn't technically right, because it involves cocycles instead of homology classes in H^2, but practically speaking it is what's going on.

2.2 Directed system of relative Brauer groups

Recall that for an extension L/K, the relative Brauer group L/K is the kernel fitting into the exact sequence

$$0 \to \mathrm{Br}(L/K) \to \mathrm{Br}(K) \xrightarrow{[A]\mapsto[A\otimes_K L]} \mathrm{Br}(L)$$

Last time, Nick proved that

$$\mathrm{Br}(K) = \bigcup \mathrm{Br}(E/K)$$

with the union taken over finite Galois extensions E/K. Let L/K be (infinite) Galois, and $\mathcal{E}$ the set of finite Galois subextensions $K \subset E \subset L$. We will need the following slight generalization of this.

Lemma 2.2. *Let L/K be a Galois extension, and $\mathcal{E}$ the set of finite Galois subextensions $K \subset E \subset L$. Then*

$$\mathrm{Br}(L/K) = \bigcup_{E\in\mathcal{E}} \mathrm{Br}(E/K)$$

Proof. The inclusion $\supset$ is obvious from the fact that if a K-algebra A splits over E (that is $A \otimes_K E \cong M_n(K)$) then tensoring further up to L still makes it a matrix algebra. So we just need to prove $\subset$.

Let $[A] \in \mathrm{Br}(L/K)$ with representative A of degree n, so $\dim_K A = n^2$. By definition of $\mathrm{Br}(L/K)$, there is an isomorphism

$$A \otimes_K L \xrightarrow[\cong]{\alpha} M_n(L)$$

Let $e_1, \dots, e_{n^2}$ be a K-basis of A, and consider the elements $\alpha(e_j \otimes 1) \in M_n(L)$. There are only finitely many entries (from L) in the matrices $\alpha(e_j \otimes 1)$, so let $E \subset L$ be a finite extension of K containing all entries of all matrices $\alpha(e_j \otimes 1)$ for $j = 1, \dots, n^2$. We can further enlarge E to make E/K Galois if necessary.

Then the image of α lies in $M_n(E)$, so restricting α gives an isomorphism

$$A \otimes_K E \xrightarrow{\cong} M_n(E) \qquad a \otimes x \mapsto \alpha(a \otimes x)$$

Hence $[A] \in \operatorname{Br}(E/K)$. This proves the inclusion $\subset$ we needed. □

Remark 2.1. It is immediate from the previous equality and the fact that the direct limit of groups is the disjoint union modulo equivalence that

$$\operatorname{Br}(L/K) = \varinjlim_{E \in \mathcal{E}} \operatorname{Br}(E/K)$$

with the maps of this directed system just being inclusions

$$\iota_2^1 : \operatorname{Br}(E_1/K) \hookrightarrow \operatorname{Br}(E_2/K) \qquad [A] \mapsto [A]$$

Remark 2.2. A useful special case of the previous lemma is $L = K^{\text{sep}}$. In this case, $\mathcal{E}$ is the set of all[1] finite Galois extensions E/K, so the lemma gives

$$\operatorname{Br}(K^{\text{sep}}/K) = \bigcup_{E \in \mathcal{E}} \operatorname{Br}(E/K) = \operatorname{Br}(K)$$

2.3 Finalizing step 2

Up till now in step 2, we haven't made use of step 1, and now is the moment. Using step 1, we have isomorphisms $\beta_{E_i/K} : \operatorname{Br}(E_i/K) \to H^2(\operatorname{Gal}(E_i/K), E_i^\times)$ fitting into the following square.

$$\begin{array}{ccc} \operatorname{Br}(E_1/K) & \xrightarrow{\iota_2^1} & \operatorname{Br}(E_2/K) \\ \cong \downarrow \beta_{E_1/K} & & \cong \downarrow \beta_{E_2/K} \\ H^2(\operatorname{Gal}(E_1/K), E_1^\times) & \xrightarrow{\theta_2^1} & H^2(\operatorname{Gal}(E_2/K), E_2^\times) \end{array}$$

If this diagram commutes (this is not obvious, it requires going into details of β maps), then the isomorphisms $\beta_{E/K}$ are not merely group isomorphisms, but the collection of them is an isomorphism of directed systems, which induces an isomorphism on the direct limit, which is exactly the isomorphism we wanted.

$$\operatorname{Br}(L/K) \cong H^2(\operatorname{Gal}(L/K), L^\times)$$

[1] Technicall speaking $\mathcal{E}$ is the set of all finite Galois extensions contained in K^{sep} but this is this only reasonable meaning of "all" in this context.

3 Details of step 1 - the isomorphism $\beta_{L/K}$ for finite Galois extensions

3.1 Steps (1a), (1b) - construction of $\beta_{L/K}$, the 2-cocycle (factor set) associated to a central simple algebra

Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. In this section, we associate an element of $H^2(G, L^\times)$ to an element $[A] \in \mathrm{Br}(L/K)$, to construct our map

$$\beta_{L/K} : \mathrm{Br}(L/K) \to H^2(G, L^\times)$$

Definition 3.1. Let L/K be a finite Galois extension, and recall that

$$\mathrm{Br}(L/K) = \left\{[A] \in \mathrm{Br}(K) : \dim_K A = n^2, L \subset A\right\}$$

Let $[A] \in \mathrm{Br}(L/K)$ with representative A so that $\dim_K A = n^2$ and $L \subset A$. Let $\sigma \in G = \mathrm{Gal}(L/K)$. Since A is central simple over K and L is simple over K, we can apply the Skolem-Noether theorem to the two homomorphisms

$$\begin{aligned} L &\hookrightarrow A \qquad a \mapsto a \\ L &\hookrightarrow A \qquad a \mapsto \sigma(a) \end{aligned}$$

By Skolem-Noether, these are conjugate, which is to say, there exists $x_\sigma \in A^\times$ so that

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \qquad \forall a \in L$$

Then for $\sigma, \tau \in G$, define

$$a_{\sigma,\tau} = x_\sigma x_\tau x_{\sigma\tau}^{-1}$$

The collection $\{a_{\sigma,\tau}\}$ is the **factor set of A relative to L.**

Remark 3.1. Here are some facts (without proof) which explain various aspects of the previous definition. Recall $G = \mathrm{Gal}(L/K)$.

1. (Lemma 6 of Rapinchuk [2]) The elements x_σ (for $\sigma \in G$) give a basis of A over L, that is,

$$A = \bigoplus_{\sigma \in G} L x_\sigma$$

2. The elements $a_{\sigma,\tau}$ lie in $L^\times$, so they may be viewed as functions

$$G \times G \to L^\times \qquad (\sigma, \tau) \mapsto a_{\sigma,\tau}$$

3. The products $x_\sigma x_\tau$ for $\sigma, \tau \in G$ determine all the multiplication in A, and

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

hence the collection $\{a_{\sigma,\tau}\}$ captures all information about multiplication in A.

4. The functions $a_{\sigma,\tau}$ are in fact 2-cocycles (elements of $Z^2(G, L^\times)$), since they satisfy the relations
$$\rho(a_{\sigma,\tau})a_{\rho,\sigma\tau} = a_{\rho,\sigma}a_{\rho\sigma,\tau}$$
for $\rho, \sigma, \tau \in G$. This adresses (1b). Thus we have a map
$$\mathrm{CSA}(L/K) \to H^2(G, L^\times) \qquad A \mapsto [\{a_{\sigma,\tau}\}]$$
By $\mathrm{CSA}(L/K)$ I mean central simple K-algebras that split over L.

5. If we replace the central simple algebra A with another Brauer-equivalent central simple algebra A' (that is, $[A] = [A']$), and repeat the construction to obtain a factor set $\{a'_{\sigma,\tau}\}$ for A', then there are elements $b_\sigma \in L^\times$ such that
$$a'_{\sigma,\tau} = \left(\frac{b_\sigma \sigma(b_\tau)}{b_{\sigma\tau}}\right) a_{\sigma,\tau}$$
Since $\left(\frac{b_\sigma \sigma(b_\tau)}{b_{\sigma\tau}}\right)$ is a 2-coboundary, this says that
$$[a'_{\sigma,\tau}] = [a_{\sigma,\tau}] \qquad \text{in } H^2(G, L^\times)$$
Thus we have a well-defined map
$$\beta_{L/K} : \mathrm{Br}(L/K) \to H^2(G, L^\times) \qquad [A] \mapsto [\{a_{\sigma,\tau}\}]$$
This addresses (1a).

For more details behind all of these facts, see pages 13-14 of Rapinchuk [2].

3.2 Step (1c) - injectivity of $\beta_{L/K}$

For (1c), I'm just going to cite Igor's notes [2].

Lemma 3.1. *$\beta_{L/K}$ is injective.*

Proof. Lemma 7 of Rapinchuk [2]. □

3.3 Step (1d) - surjectivity of $\beta_{L/K}$, the algebra (crossed product) associated to a 2-cocycle (factor set)

To show that $\beta_{L/K}$ is surjective, we construct an algebra from a cocycle/factor set $\{a_{\sigma,\tau}\}$.

Definition 3.2. Continuing the notation of above, we have a finite Galois extension L/K with $G = \mathrm{Gal}(L/K)$. Let $\{a_{\sigma,\tau}\}$ be a factor set, thought of as an element of $Z^2(G, L^\times)$. Define the L-vector space
$$A = \bigoplus_{\sigma \in G} L x_\sigma$$

Then define multiplication in A as follows. For $a, b \in L$, define

$$(ax_\sigma)(bx_\tau) = a\sigma(b)a_{\sigma,\tau}x_{\sigma\tau}$$

(recall that $a_{\sigma,\tau} \in L$). Then extend this by L-linearity. The most general way to write this multiplication is

$$\left(\sum_\sigma a_\sigma x_\sigma\right)\left(\sum_\tau b_\tau x_\tau\right) = \sum_{\sigma,\tau} a_\sigma \sigma(b_\tau) a_{\sigma,\tau} x_{\sigma\tau}$$

We then view A as a K-algebra. The K-action is just given by multiplication on the left (since $K \subset L$, we already know how to multiply elements of K by elements of L). The algebra A is called the **crossed product of L and G relative to the factor set $\{a_{\sigma,\tau}\}$**, and is denoted $(L, G, \{a_{\sigma,\tau}\})$.

Lemma 3.2. *Let L/K be a finite Galois extension and $G = \mathrm{Gal}(L/K)$, $n = [L : K] = |G|$. Let $\{a_{\sigma,\tau}\}$ be a factor set. The K-algebra $A = (L, G, \{a_{\sigma,\tau}\})$ is an associative, unital, central simple K-algebra containing (an isomorphic copy of) L, and with $\dim_K A = n^2$, and*

$$\beta_{L/K}[A] = [\{a_{\sigma,\tau}\}]$$

Hence $\beta_{L/K}$ is surjective.

Proof. Note that the identity element is $a_{1,1}^{-1}x_1$. Lemma 8 of Rapinchuk [2]. □

3.4 Step (1e) - homomorphism property of $\beta_{L/K}$

Theorem 3.3. *Let L/K be a finite Galois extension. The map*

$$\beta_{L/K} : \mathrm{Br}(L/K) \to H^2(\mathrm{Gal}(L/K), L^\times) \qquad [A] \mapsto [\{a_{\sigma,\tau}\}]$$

is a group homomorphism. Since we already showed it to be injective and surjective, it is an isomorphism.

Proof. Theorem 7 of Rapinchuk [2]. □

4 Return to step 2, conclusions

Theorem 4.1. *Let L/K be an infinite Galois extension and let $\mathcal{E}$ be the set of intermediate finite Galois extension $K \subset E \subset L$. The isomorphism $\beta_{E/K}$ give an isomorphism of directed systems $\left(H^2(\mathrm{Gal}(E/K), E^\times), \theta_j^i\right) \cong \left(\mathrm{Br}(E/K), \iota_j^i\right)$. That is, for all $E_1, E_2 \in \mathcal{E}, E_1 \subset E_2$, the following diagram commutes.*

$$\begin{array}{ccc}
\mathrm{Br}(E_1/K) & \xrightarrow{\iota_2^1} & \mathrm{Br}(E_2/K) \\
\downarrow{\scriptstyle \beta_{E_1/K}} & & \downarrow{\scriptstyle \beta_{E_2/K}} \\
H^2(\mathrm{Gal}(E_1/K), E_1^\times) & \xrightarrow{\theta_2^1} & H^2(\mathrm{Gal}(E_2/K), E_2^\times)
\end{array}$$

Thus the direct limit of maps $\beta_{E/K}$ gives an isomorphism on the direct limits.

$$\mathrm{Br}(L/K) \xrightarrow[\cong]{\beta_{L/K} = \varinjlim \beta_{E/K}} H^2(\mathrm{Gal}(L/K), L^\times)$$

In particular, for $L = K^{\mathrm{sep}}$,

$$\mathrm{Br}(K) = \mathrm{Br}(K^{\mathrm{sep}}/K) \cong H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times)$$

Proof. Proposition 6 and Theorem 8 of Rapinchuk [2]. □

4.1 Descrption in terms of cup products

The isomorphism $\mathrm{Br}(K) \cong H^2(G_K, (K^{\mathrm{sep}})^\times)$ can also be described in terms of cup products, although this requires some langauge which we don't know.

Proposition 4.2. *Let K be a field, let $m \in \mathbb{Z}_{>0}$, fix a separable closure K^{sep}, and let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Let L/K be a cyclic Galois extension of degree m contained in K^{sep}, and fix an isomorphism*

$$\chi : \mathrm{Gal}(L/K) \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}$$

Then define

$$\widetilde{\chi} : G_K \to \mathbb{Z}/m\mathbb{Z} \qquad \sigma \mapsto \chi(\sigma|_L)$$

so that $\widetilde{\chi} \in H^1(G_K, \mathbb{Z}/m\mathbb{Z})$. Let $\delta : H^1(G_K, \mathbb{Z}/m\mathbb{Z}) \to H^2(G_K, \mathbb{Z})$ be the coboundary map of the LES associated to

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$$

[2] *Then consider the cup product map*

$$H^2(G_K, \mathbb{Z}) \times H^0(G_K, (K^{\mathrm{sep}})^\times) \xrightarrow{\cup} H^2(G_K, (K^{\mathrm{sep}})^\times)$$

Under the isomorphism

$$H^2(G_K, (K^{\mathrm{sep}})^\times) \cong Br(K)$$

the element $\delta(\widetilde{\chi}) \cup b$ corresponds to the Brauer class of the cyclic algebra (χ, b).

Proof. Proposition 4.7.3 of Gille & Szamuely [1]. □

4.2 Compatibility with restriction maps

Finally, we have a result which says that the isomorphisms $\beta_{L/K}$ are "compatible" with restriction maps on cohomology and the relative Brauer group maps

$$\mathrm{Br}(K) \to \mathrm{Br}(L) \qquad [A] \mapsto [A \otimes_K L]$$

In particular it is "the same" as the Res map on cohomology. This statement is made more precise by the next proposition.

[2] Note that we are viewing $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ as trivial G_K-modules, and $H^1(G_K, \mathbb{Z}/m\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G_K, \mathbb{Z}/m\mathbb{Z})$, so $\widetilde{\chi} \in H^2(G_K, \mathbb{Z}/m\mathbb{Z})$.

Proposition 4.3. *Let $K \subset L \subset M$ be a tower of fields with M/K finite Galois. Consider the homomorphism*

$$\epsilon : \mathrm{Br}(M/K) \to \mathrm{Br}(M/L) \qquad [A] \mapsto [A \otimes_K M]$$

Note that $\mathrm{Gal}(M/L)$ *is a subgroup of* $\mathrm{Gal}(M/K)$*, so there is the (profinite) cohomology map*

$$\mathrm{Res} : H^2(\mathrm{Gal}(M/K), M^\times) \to H^2(\mathrm{Gal}(M/L), M^\times)$$

Then the following diagram commutes.

$$\begin{array}{ccc}
\mathrm{Br}(M/K) & \xrightarrow{\quad\epsilon\quad} & \mathrm{Br}(M/L) \\
\cong\big\downarrow \beta_{M/K} & & \cong\big\downarrow \beta_{M/L} \\
H^2(\mathrm{Gal}(M/K), M^\times) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}(M/L), M^\times)
\end{array}$$

In particular, in the case $M = K^{\mathrm{sep}}$, we note that $L^{\mathrm{sep}} = K^{\mathrm{sep}}, \mathrm{Br}(K) = \mathrm{Br}(K^{\mathrm{sep}}/K), \mathrm{Br}(L) = \mathrm{Br}(L^{\mathrm{sep}}/L)$, so the above commutative square becomes

$$\begin{array}{ccc}
\mathrm{Br}(K) & \xrightarrow{[A]\mapsto[A\otimes_K L]} & \mathrm{Br}(L) \\
\big\downarrow\cong & & \big\downarrow\cong \\
H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}(L^{\mathrm{sep}})/L), (L^{\mathrm{sep}})^\times)
\end{array}$$

Proof. Proposition 7 of Rapinchuk [2]. □

References

[1] Philippe Gille and Tamás Szamuely. Central simple algebras and group cohomology, 2006.

[2] Igor Rapinchuk. The brauer group of a field. Available at https://drive.google.com/file/d/0B0CCc00SqXL4dTBIbU8xa0Vjb2c/edit.