Galois cohomology seminar
Week 9 -

Joshua Ruiter

March 19, 2019

Contents

1 Computation of $\mathrm{Br}(\mathbb{R})$

Proposition 1.1. *The only nontrivial finite dimensional central division algebra over* $\mathbb{R}$ *is the Hamilton quaternions.*

Proof. Let D be a nontrivial finite dimensional central division algebra over $\mathbb{R}$. By a result that Nick proved, $\dim_{\mathbb{R}} D = d^2$ is a perfect square, and by anothe result of Nick, D has a maximal subfield P so that $P/\mathbb{R}$ is separable, and $\dim_{\mathbb{R}} P = d$. Since the only nontrivial extension of $\mathbb{R}$ is $\mathbb{C}$, $P = \mathbb{C} = \mathbb{R}(i)$ and $d = 2$, so $\dim_{\mathbb{R}} D = 4$. Now consider the two homomorphisms

$$\begin{aligned} f : \mathbb{C} \to D \qquad & z \mapsto z \\ g : \mathbb{C} \to D \qquad & z \mapsto \overline{z} \end{aligned}$$

where $\overline{z}$ denotes the complex conjugate. By the Skolem-Noether theorem, there exists $j \in D^\times$ so that

$$\overline{z} = jzj^{-1} \qquad \forall z \in \mathbb{C}$$

In particular, $jij^{-1} = -i$. Note that since j does not commute with i, j does not lie in $\mathbb{C}$.

We claim $j^2 \in \mathbb{R}$. Note that since D is central, j (hence j^2) commutes with $\mathbb{R}$. Since $j^2 i j^{-2} = i$, j^2 commutes with $\mathbb{C}$. Since j^2 is a unit, $\mathbb{C}(j^2)$ is a field, but since $\mathbb{C}$ is a maximal subfield of D, $\mathbb{C}(j^2) = \mathbb{C}$, hence $j^2 \in \mathbb{C}$. Since j^2 commutes with j, $jj^2j^{-1} = j^2$. Since $j^2 \in \mathbb{C}$ and conjugation by j is complex conjugation, $jj^2j^{-1} = \overline{j^2}$, hence $j^2 = \overline{j^2}$, so $j^2 \in \mathbb{R}$.

Now we claim $j^2 < 0$. Since $j \notin \mathbb{R}$, its minimal polynomial over $\mathbb{R}$ is $t^2 - j^2$. But if $j^2 > 0$, this would be reducible into $(t - j)(t + j)$, which is a contradiction, so we must have

$j^2 < 0$. Replacing j by $\frac{j}{\sqrt{|j^2|}}$, we may assume $j^2 = -1$. We claim that $1, i, j, ij$ are linearly independent over $\mathbb{R}$. Suppose there are $a, b, c, d \in \mathbb{R}$ so that

$$a + bi + cj + dij = 0$$

Then if $c + di \neq 0$, we get

$$(a + bi) + (c + di)j = 0 \implies j = \frac{a + bi}{c + di} \implies j \in \mathbb{C}$$

which is impossible since we know $j \notin \mathbb{C}$, so $c = d = 0$. Then $a + bi = 0 \implies a = b = 0$, hence $1, i, j, ij$ are linearly independent. Thus D is four dimensional $\mathbb{R}$-algebra with basis $1, i, j, ij$ satisfying relations $i^2 = j^2 = -1$ and $ij = -ij$, so $D \cong \mathbb{H}$. □

Corollary 1.2. *$\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.*

2 Computation of $\mathrm{Br}(\mathbb{F}_q)$ again

We already showed that $\mathrm{Br}(\mathbb{F}_q) = 0$ using the cohomological version of the Brauer group. We can also prove this in a different way using the language of algebras.

Lemma 2.1 (Finite group not equal to conjugates of proper subgroup)**.** *Let G be a finite group and $H \subset G$ a proper subgroup. The union of all conjugates of H is not equal to G. That is,*

$$\bigcup_{g \in G} gHg^{-1}$$

is a proper subset of G.

Proof. Let $K_H = \{gHg \in : g \in G\}$ be the set of conjugate subgroups to H. Then G acts on K_H by conjugation. The stabilizer of this action is exactly the normalizer of H in G, which we denote $N_G(H)$. Note that $H \subset N_G(H)$, thus

$$[G : N_G(H)] \leq [G : H]$$

By the orbit-stabilizer theorem,

$$|K_H| = [G : N_G(H)]$$

Each conjugate subgroup of H has the same order as H, and also contains the identity, so the maximum number of non-overlapping elements in each subgroup is $|H| - 1$, and there are $|K_H|$ such conjugate subgroups. Thus

$$\left| \bigcup_{g \in G} gHg^{-1} \right| \leq \Big(|H| - 1 \Big) |K_H| + 1$$

Now we do some trivial manipulations to this using facts established above.

$$\begin{aligned}\Big(|H|-1\Big)|K_H|+1 &= \Big(|H|-1\Big)[G:N_G(H)]+1 \\ &\le \Big(|H|-1\Big)[G:H]+1 \\ &= |H|[G:H]-[G:H]+1 \\ &= |G|-[G:H]+1\end{aligned}$$

Since H is a proper subgroup, $[G:H] \geq 2$, thus, the expression above is at most $|G|-1$. Thus the union of all conjugates of G has size strictly less than G, so it is not the whole group. □

Proposition 2.2 (Every finite division algebra is a field)**.** *Let D be a finite dimensional central division algebra over a finite field. Then D is commutative, hence a field.*

Proof. Suppose D is a noncommutative finite central division algebra over a finite field F. Let $\dim_F D = n^2$. If $n = 1$ then $D = F$ and we are done, so assume $n > 1$. By a result of Nick, there is a maximal intermediate subfield $F \subset P \subset D$ with $\dim_F P = n$. Since F has a unique (up to isomorphism) extension of degree n, all maximal subfields of D are isomorphic.

By the Skolem-Noether theorem, any two maximal subfields of D are conjugate. More precisely, if P, P' two maximal subfields with embeddings $\iota : P \hookrightarrow D, \iota' : P \hookrightarrow D$, and we fix an isomorphism $\phi : P \xrightarrow{\cong} P'$ (isomorphism as K-algebras), then by the Skolem-Noether theorem applied to the homomorphisms ι and $\iota' \circ \phi$, there exists $d \in D$ such that for all $x \in P$,

$$\iota' \circ \phi(x) = d\big(\iota(x)\big)d^{-1}$$

Since ι, ι' are inclusions, we can write this instead as

$$\phi(x) = dxd^{-1}$$

That is to say,

$$P \to P' \qquad x \mapsto dxd^{-1}$$

is an isomorphism, which is what we mean when we say that P, P' are conjugate in D. Thus if P is any one maximal subfield, then all other maximal subfields arise as conjugates dPd^{-1}. Now, every element of D is contained in some maximal subfield, so we obtain

$$D^\times = \bigcup_{\substack{P \text{ maximal} \\ \text{subfield}}} P^\times = \bigcup_{d \in D^\times} dP^\times d^{-1}$$

Since $D^\times$ is a finite group and $P^\times \subset D^\times$ is a proper subgroup, by our group theory lemma 2.1, this is a contradiction, so no such D exists. □

Corollary 2.3. *Let F be a finite field. Then* $\mathrm{Br}(F) = 0$*.*

Proof. Nonzero elements of $\mathrm{Br}(F)$ correspond to equivalence classes of (noncommutative) finite dimensional central division algebras, but by Proposition 2.2, there are no such division algebras. □

3 First approximation 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 (or much desire) to go into all the details, since it involves a lot of them, and the details don't do much to illustrate the ideas. 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 #1, and none of the parts involved is easy. Each of the following steps takes about a page of detailed work: construction of the map $\beta_{L/K}$, showing that what you've constructed is a cocycle, showing $\beta_{L/K}$ is injective, showing $\beta_{L/K}$ is surjective, showing that $\beta_{L/K}$ is a group homomorphism. This is where we'll omit a lot of details later.

In contrast, #2 is not so bad, so we can talk about some of it now. Consider an infinite Galois extension L/K, and let $\mathcal{E}$ be the collection of finite Galois intermediate extensions $K \subset E \subset L$. For $E_1, E_2 \in \mathcal{E}$, we have the inflation map

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

which makes the groups $H^2(\mathrm{Gal}(E_i/K), E_i^\times)$ into a directed system with

$$H^2(\mathrm{Gal}(L/K), L^\times) = \varinjlim_{E \in \mathcal{E}} H^2(\mathrm{Gal}(E/K), E^\times)$$

By a slight generalization of something Nick proved,

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

with the maps of this directed system just being inclusions

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

Thus we have maps in the following square.

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

If this diagram commutes, 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.

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