Lecture 17: Brauer Groups of Central Simple Algebras, Reduced Norm and Trace

17.1 Reduced norm and trace

We can generalize the determinant and trace to central simple algebras. Suppose A is a central simple algebra of degree d over k.

Proposition 17.1: *There exist unique polynomial maps $\tau, \delta \colon A \to k$ so that for any field extension K/k such that A splits over K,*

$$\tau_k \colon A \otimes_k K \cong \mathrm{Mat}_n(K) \to K$$

is the trace and

$$\delta_K \colon A \otimes_k K \cong \mathrm{Mat}_{n(K)} \to K$$

*is the determinant. τ is called the **reduced trace** and δ is called the **reduced norm**.*

Example 17.2: Let's take $A = \mathbb{H}$ and $k = \mathbb{R}$. Then $\tau \colon a+bi+cj+dk \mapsto 2a$ and $\delta \colon a+bi+cj+dk \mapsto a^2+b^2+c^2+d^2$.

Proof. By the Artin-Wedderburn theorem, WLOG we can assume $|k| = \infty$ so that we can say that polynomials are determined by their values on k^n. Now the proof follows from Galois descent and the fact that Tr, det are invariant under all automorphisms of the matrix ring. For a fixed extension K/k, τ, δ satisfying the compatibility with Tr, det are unique; moreover, they will satisfy the same compatibility for any extension $K' \supset K$, and also for $K'' \subset K$ if K splits A. So we only have to construct τ, δ satisfying the compatibility for a fixed extension splitting A.
Choose a finite Galois extension K/k which splits A and choose an isomorphism $A \otimes K \cong \mathrm{Mat}_n(K)$. Let $G = \mathrm{Gal}(K/k)$, it acts on $A \otimes K$ by acting on K. It suffices for us to show that det, Tr commute with the G-action, which will imply that they come from polynomial maps defined over k.
To see this, consider the action of G on $\mathrm{Mat}_n(K)$, which is different from the action above; say it sends $a \mapsto {}^{\gamma}a$. Then the map $a \mapsto \gamma^{-1}({}^{\gamma}a)$ is a K-linear automorphism on $\mathrm{Mat}_n(K)$, hence given by conjugation by some element $g_\gamma \in \mathrm{GL}_n(K)$. Since det is conjugation-invariant, we have

$$\det(a) = \det(\gamma^{-1}({}^{\gamma}a)) \Rightarrow \det(\gamma(a)) = \det({}^{\gamma}a) = \gamma(\det a).$$

The same argument works for trace. So we are done. □

From these, we see that $\tau(ab) = \tau(ba)$, $\delta(ab) = \delta(a)\delta(b)$, and $\delta(1) = 1$.

17.2 C_1 fields

Definition 17.3: *We say a field is a **quasi-closed** or C_1 if any homogeneous polynomial of degree d in $n > d$ variables has a nontrivial zero. More generally, we say a field is C_k if any homogeneous polynomial of degree d in $n > d^k$ variables has a nontrivial zero.*

Proposition 17.4: *If F is C_1, $\mathrm{Br}(F) = 0$.*

Proof. Suppose not. Then let D be a skew field finite over F with $Z(D) = F$. Then δ (the reduced norm) is a degree d polynomial but $\dim_F(D) = d^2$, so δ has a nontrivial zero. But δ is invertible, a contradiction. □

Lemma 17.5: *Finite extensions of C_1 fields are also C_1.*

Proof. Suppose F is C_1 and E/F is a degree m extension. Let P be a polynomial of degree d in n variables over E. By choosing a basis for E over F, we can identify $E^n = F^{nm}$. Then consider the polynomial

$$\tilde{P}(x) := \mathrm{Nm}_{E/F}(P(x));$$

this is a degree md polynomial in mn variables over F, and it has a nontrivial zero iff P does. □

Theorem 17.6 (Chevalley-Warning): *Finite fields are C_1 fields.*

Proof. The previous lemma shows that it's enough to consider $\mathbb{F}_p$. Then the result follows from the following fact: if P is a homogeneous polynomial in n variables of degree $n > d$ over $\mathbb{F}_p$, the number of zeroes is 0 mod p. Since there is at least one zero (the trivial one), there are at least p zeroes. So it remains to prove this fact.
We know that for $a \in \mathbb{F}_p$, a^{p-1} is either 0 or 1 (if $a \neq 0$). So

$$\sum_{a_1,\ldots,a_n \in \mathbb{F}_p} (1 - P(a_1, \ldots, a_n)^{p-1}) \equiv \#\,\text{zeroes of } P \pmod{p}.$$

Every monomial in this sum (considered as a polynomial in a_i) will have at least one variable that has exponent less than $p-1$ because the polynomial has degree $d(p-1)$ and has n variables (we use that $d(p-1) < n(p-1)$ because $d < n$). Summing over that variable and using that $\sum_a a^m = 0$ when $0 \leqslant m < p-1$, we see that the whole sum is 0. □

Remark 17.7: This gives another proof of Theorem 14.15.

Theorem 17.8 (Tsen's Theorem): *Suppose k is algebraically closed. Then the field $F = k(t)$ is C_1.*

Proof (Sketch). Clear denominators so that WLOG $P \in k[t][x_1, \ldots, x_n]$. Then use that a system of m homogeneous polynomial equations over k in n variables has a nontrivial solution if $n > m$ (this is true because k is algebraically closed). If K is the maximum degree (in t) of a coefficient of P, look at a solution of degree r. Then you get $dr+K+1$ equations in $(r+1)n$ variables and $d < n$ implies $dr + K + 1 < (r+1)n$ when $r \gg 0$. □

17.3 Second approach to the cohomological description of Brauer group

Let A be a central simple algebra over F and E/F a finite Galois extension. As described in the proof of Proposition 17.1, when you fix an isomorphism $A \otimes_F E \cong \mathrm{Mat}_n(E)$, you get two G-actions, $\gamma(a)$ and ${}^{\gamma}a$, that differ by conjugation by $g_\gamma \in \mathrm{GL}_n(E)$. This g_γ is determined up to multiplication by a scalar matrix, so $g_{\gamma_1} g_{\gamma_2}$ and $g_{\gamma_1\gamma_2}$ have the same image in $\mathrm{PGL}_n(E) = \mathrm{Aut}(\mathrm{Mat}_n(E))$ (but lifting to GL_n requires a choice). So we can define

$$c(\gamma_1, \gamma_2) = g_{\gamma_1} g_{\gamma_2} g_{\gamma_1\gamma_2}^{-1} \in E^\times.$$

In fact, c is a 2-cocycle, and its class in H^2 is independent of choice. Therefore, we get a map $\mathrm{Br}(E/F) \to H^2(G, E^\times)$, and it's an isomorphism.

Remark 17.9: We can interpret the definition of c as follows. The set of isomorphisms $A \otimes_F E \cong \mathrm{Mat}_n(E)$ form a $\mathrm{PGL}_n(E)$-torsor over G. As discussed earlier, the isomorphism class of this torsor corresponds to an element $\tilde{c} \in H^1(G, \mathrm{PGL}_n(E))$, the nonabelian cohomology group. A short exact sequence of abelian groups with a G-action will produce a long exact sequence in cohomology. For

$$1 \to E^\times \to \mathrm{GL}_n(E) \to \mathrm{PGL}_n(E) \to 1$$

the first few terms of the sequence are still well-defined, even though the sequence involves two nonabelian groups. The class c is the image of $\tilde{c}$ under the connecting homomorphism.
The injectivity of the map can be deduced from Hilbert's Theorem 90, which says that $H^1(G, \mathrm{GL}_n(E)) = 1$. (Hilbert originally considered the case $n = 1$ only.) An equivalent form of this statement is as follows: given an n-dimensional E-vector space V_E with a compatible G-action, there is an F-vector space V_F and a G-equivariant isomorphism $V_E = V_F \otimes_F E$.

17.4 Brauer groups of local fields

Theorem 17.10: *Let F be a non-Archimedean local field, i.e. it's a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ (in which case $F \cong \mathbb{F}_q((t))$). Then $\mathrm{Br}(F) \cong \mathbb{Q}/\mathbb{Z}$.*

First, let us recall without proof some facts about non-Archimedean local fields. If F is such a field, we have a valuation $F^\times \to \mathbb{Z}$ satisfying $v(ab) = v(a) + v(b)$ and $v(a+b) \geqslant \min(v(a), v(b))$; we can extend this to F by setting $v(0) = \infty$. WLOG we can assume that v is onto. Then there exists an element π with $v(\pi) = 1$, called a uniformizer. The elements x with $v(x) \geqslant 0$ form the ring of integers $\mathcal{O} \subset F$, the elements x with $v(x) \geqslant 1$ form the unique maximal ideal $\mathfrak{m} = \pi\mathcal{O} \subset \mathcal{O}$, and the residue field $k = \mathcal{O}/\pi\mathcal{O}$ is finite. For all $x \in F^\times$, $x\pi^{-v(x)} \in \mathcal{O}^\times$.

Definition 17.11: *If E/F is a finite extension, then k_E/k_F is an extension of finite fields. Its degree $i_{E/F} = [k_E : k_F]$ is the **inertia degree** of the extension. The **ramification index** of the extension, $r = r_{E/F}$, is the integer such that $\pi_E^r \pi_F^{-1} \in \mathcal{O}^\times$ where π_E, π_F are uniformizers of their respective valuations. Then*

$$[E : F] = i_{E/F} r_{E/F}$$

since you can see these are both $\dim_{k_F}(\mathcal{O}_E/\mathfrak{m}_E)$.

Remark 17.12: This also works if E is a skew field.

Definition 17.13: *If $r = 1$, we say that E/F is **unramified**. In this case, E/F is Galois and $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(k_E/k_F)$ (in particular, it is cyclic).*

Proposition 17.14: *Every central simple algebra over a local field F splits over an unramified extension.*

Proof (Sketch). Let D be a central simple algebra over F. Then we can extend the valuation to $D^\times$, choose a uniformizer π_D where $v_D(\pi_D) = 1$, $\mathcal{O}_D = \{x \in D \mid v_D(x) \geqslant 0\}$. We get a finite extension $k_D := \mathcal{O}_D/\pi_D\mathcal{O}_D$ over k_F (note that by Artin-Wedderburn theorem, k_D is a field), and

$$\dim_F D = d^2 = [k_D : k_F] r_{D/F}$$

where d is the degree of D. We also claim that $i_{D/F}, r_{D/F} \leqslant d$ (recall that $i_{D/F} := [k_D : k_F]$). To see this, it's enough to show the existence of commutative subfields E_1, E_2 in D with $i_{D/F} \leqslant [E_1 : F]$ and $r_{D/F} \leqslant [E_2 : F]$ (use Corollary 14.13). Let $E_1 = F(\alpha)$ where $\alpha \in \mathcal{O}_D$ is such that $\alpha \bmod \pi_D\mathcal{O}_D$ generates k_D over k_F and $E_2 = F(\pi_D)$.
Therefore, $i_{D/F} = r_{D/F} = d = [E_1 : F]$. This shows that E_1/F is unramified and that it is a maximal commutative subfield in D. Thus it splits D (see Lemma 16.3) and is our desired extension. □

Proposition 17.15: *If E/F is an unramified degree n extension of a non-Archimedean local field, then* $\mathrm{Br}(E/F) = \mathbb{Z}/n\mathbb{Z}$.

Proof. We saw last time that for a cyclic extension, $\mathrm{Br}(E/F) \cong F^\times/\mathrm{Nm}(E^\times)$. Since E/F is unramified, $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(k_E/k_F)$ and every extension of finite fields is cyclic (the Galois group is generated by the Frobenius). For an unramified extension, $O_E^\times \twoheadrightarrow O_F^\times$; this follows from surjectivity of the associated graded maps $k_E^\times \twoheadrightarrow k_F^\times$ and $(1+\pi^n O_E)/(1+\pi^{n+1}O_E) \twoheadrightarrow (1+\pi^n O_F)/(1+\pi^{n+1}O_F)$, where $\pi = \pi_F$. The first map is identified with the norm and the second with the trace $k_E \longrightarrow k_F$. Since $\mathrm{Nm}(\pi) = \pi^n$, we get that $\mathrm{Br}(E/F) = \mathbb{Z}/n\mathbb{Z}$. □

Proof (of Theorem 17.10). Let F^{unr} be a maximal unramified extension of F. Then it contains a unique degree n subextension F_n/F for every $n > 1$ and

$$\mathrm{Br}(F) = \mathrm{Br}(F^{\mathrm{unr}}/F) = \varinjlim \mathrm{Br}(F_n/F) = \varinjlim \mathbb{Z}/n\mathbb{Z} = \mathbb{Q}/\mathbb{Z}.$$

□

Remark 17.16: The theorem allows us to formulate a version of the reciprocity law of Class Field Theory. Let k be a global field, i.e. a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$. For every valuation v, we get a corresponding local field k_v by completing k at v. Then we get a map

$$\mathrm{Br}(k) \longrightarrow \prod_v \mathrm{Br}(k_v)$$

and we claim that in fact

$$\mathrm{Br}(k) \hookrightarrow \bigoplus_v \mathrm{Br}(k_v)$$

and this induces an isomorphism of $\mathrm{Br}(k)$ with the kernel of the sum map, i.e.

$$\mathrm{Br}(k) \cong \left\{ (b_v) \in \bigoplus_v \mathrm{Br}(k_v) \,\middle|\, \sum b_v = 0 \right\} = \ker\left(\bigoplus_v \mathrm{Br}(k_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \right).$$

This is one of several equivalent forms of the reciprocity law of class field theory. For example, the corresponding identity for degree 2 central simple algebras over $\mathbb{Q}$, $\mathbb{H}_{a,b} = \mathbb{Q}\langle i, j\rangle/(i^2 = a, j^2 = b, ij = -ji)$ is essentially equivalent to quadratic reciprocity.

18.706 Noncommutative Algebra
Spring 2023