MATH808K - Brauer Groups

Haoran Li

2022/03/17

Contents

1 Overview

The goals of the this course:

1. Define central simple k-algebras(CSA/k)
2. Classify CSA's
3. Define the Brauer group(motivate Galois cohomology)
4. Blackbox Galois cohomology
5. Computing Brauer gorups of some special fields

Example 1.1 (CSA/k(Central simple k-algebras))**.** 1. $\mathcal{C}$ is a category, $\mathrm{Hom}_{\mathcal{C}}(A, B)$ are finite dim vector spaces, $\mathrm{End}_{\mathcal{C}}(A)$ are finite dim k-algebras

2. $\mathcal{C}'$ is the category of finite dim vector spaces, $\mathrm{End}_{\mathcal{C}'}(k^{\oplus n}) = M_n(k)$
3. $\mathcal{C}$ is the cat of local Artinian k-algebras, $\mathrm{Hom}_{\mathcal{C}}(A, B) \subseteq \mathrm{Hom}_{\mathcal{C}'}(A, B)$
4. X proj k-var and V, W vector bundles over X

$$\mathrm{Hom}(V, W) = \Gamma(X, \mathrm{Hom}(V, W)) = \Gamma(X, V^\vee \otimes W) = H^0(X, V^\vee \otimes W)$$

Example 1.2 (Examples of finite k-algebras)**.** F/k finite field extension, $k[x]/(x^2)$, $k[x, y]/(x^2, y^2, xy)$, $M_n(k)$, $M_n(F)$

2 Quaternion Algebras

First let's assume $\mathrm{Char}\, k \neq 2$

Definition 2.1. $a, b \in k^\times$, the *generalized quaternion algebra* is denoted as $(a, b) = k[i, j]/(i^2 = a, j^2 = b, ij = -ji)$, for $q = x + yi + zj + wij$, write $\bar{q} = x - yi - zj - wij$, and $\|q\|^2 = q\bar{q} = \bar{q}q = x^2 + ay^2 + bz^2 + abw^2$

Definition 2.2. We say a k-algebra A has *division* if A is a division ring. We say A *split* if $A \cong M_n(k)$ for some n. We call $f : A \xrightarrow{\cong} M_n(k)$ a splitting of A

Example 2.3. $(-1, -1)/\mathbb{R}$ has divsion: $q^{-1} = \frac{\bar{q}}{\|q\|^2} = \frac{x-yi-zj-wij}{x^2+y^2+z^2+w^2}$ for $q = x + yi + zj + wij$. $(-1, -1)/\mathbb{C}$ splits with splitting $f : Q \to M_2(\mathbb{C})$, $f(i) = \begin{bmatrix} -i & \\ & i \end{bmatrix}$, $f(j) = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}$

Proposition 2.4. Suppose $Q = (a, b)/k$, then the following are equivalent

1. Q split
2. Q doesn't have division
3. There is a nontrivial solution over k to $x^2 - ay^2 - bz^2 + abw^2 = 0$
4. There is a solution over k to either $a = x^2 - by^2$ or $b = z^2 - aw^2$

Remark. $(-1, -1)/\bar{k}$ always split

Proof.

- (1)⇒(2): E_{ij} has no inverse
- (2)⇒(3): Assume not, then $q^{-1} = \frac{\bar{q}}{\|q\|^2}$ is defined
- (3)⇒(4):
- (4)⇒(1):

$\square$

Lemma 2.5.

1. $(a, b) \cong (b, a)$
2. $(a, b) \cong (au^2, b)$ for all $u \in k^\times$
3. $(1, b) \cong M_2(k)$

Proof.

1. Switch i, j
2. Consider $i \mapsto ui$
3. $i \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $j \mapsto \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}$

$\square$

Proposition 2.6 (Classification of finite division k-algebra of dimension 1,2,3,4)**.**

1. $\dim_k A = 1$: $A = k$
2. $\dim_k A = 2$: $A = k1 \oplus ki$, hence A is commutative, therefore A/k is a quadratic field extension
3. $\dim_k A = 3$: Consider $Z(A)$, we have the following cases
   (a) $\dim_k Z(A) = 3$: A is commutative, hence A/k is a cubic field extension
   (b) $\dim_k Z(A) = 2$: we may assume $A = k1 \oplus ki \oplus kj$ and $Z(A) = k1 \oplus ki$, but then $ij = ji$ and $\dim_k Z(A) = 3$
   (c) $\dim_k Z(A) = 1$: we may assume $A = k1 \oplus ki \oplus kj$, $Z(A) = k$ and $ij \neq ji$. Let's write $i^2 = a + bi + cj$, then $ai + bi^2 + cij = ii^2 = i^2 i = ai + bi^2 + cji \Rightarrow c(ij - ji) = 0 \Rightarrow c = 0$, hence $i^2 = a + bi$. Then multiply by i as a matrix would look like $\begin{bmatrix} 0 & a & x \\ 1 & b & y \\ 0 & 0 & z \end{bmatrix} =: M$ for some $x, y, z \in k$, so $\exists v \neq 0$ such that $iv = zv$, but then $(i - z)v = 0$ which is impossible
4. $\dim_k A = 4$: $A \cong (a, b)$ for some $a, b \in k^\times$

Lemma 2.7. Let D be a 4 dimensional, k-central division algebra, and assume there exists a k-subalgebra $E \subseteq A$ so that $E \cong k(\sqrt{a})$, $a \notin {k^\times}^2$, then $A \cong (a, b)$ for some $b \in k^\times$

If $\operatorname{Char} k = 2$(note that $-1 = 1$), things are more complicated

Definition 2.8. $a \in k, b \in k^\times$, define $[a, b) = k[i, j]/(i^2 + i = a, j^2 = b, ij = ji + j)$, suppose $q = x + yi + zj + wij$, then $\bar{q} = x + y(1 + i) + zj + wij = (x + y) + yi + zj + wij$, since the minimal polynomials of i, j, ij are $x^2 + x + a$, $x^2 + b$ and $x^2 + ab$ [since $(ij)^2 = ijij = i(ij + j)j = i^2 j^2 + ij^2 = (i + a)b + ib = ab$]

Exercise 2.9. Suppose $\operatorname{Char} k = 2$, the following are equivalent

1. $[a, b)$ split
2. $[a, b)$ doesn't have division
3. b is a norm from $k(\alpha)/k$ where α is a root of $x^2 + x + a = 0$
4. The conic $ax^2 + by^2 = z^2 + zw$ has a k point

3 Projective Conics

For $a, b \in k^\times$, consider

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 0 & b & 0 \\ a & 0 & 0 \\ 0 & 0 & ab \end{bmatrix} = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} bx_1 \\ ax_0 \\ abx_2 \end{bmatrix}$$

Then conics $V(ay_0^2 + by_1^2 - y_2^2) = V(a(bx_1)^2 + b(ax_0)^2 - (abx_2)^2) = V(ax_0^2 + bx_1^2 - abx_2^2)$

Proposition 3.1. $(a, b), (c, d)$ are two quaternion algebras over k, then $(a, b) \cong (c, d)$ iff $C_{a,b} = V(ax_0^2 + bx_1^2 - x_2^2)$ and $C_{c,d} = V(cx_0^2 + dx_1^2 - x_2^2)$ define the same conics up to $PGL_2(k)$

Proposition 3.2. $(a, b)/k$ split iff $C_{a,b}(k) \neq \varnothing$

Let's briefly recall Hensel's lemma

Hensel's lemma

Lemma 3.3 (Hensel's lemma)**.** $f(x) \in \mathbb{Z}_p[x]$, $a \in \mathbb{Z}_p$, $f(a) \equiv 0 \bmod p$, $f'(a) \not\equiv 0 \bmod p$, then there exists $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ in $\mathbb{Z}_p$ and $\alpha \equiv a \bmod p$

Example 3.4 (Non-isomorphic quaternion algebras with divisions)**.** $Q_1 = (-1, 7)/\mathbb{Q} \not\cong Q_2 = (-1, 3)/\mathbb{Q}$.

- Check Q_1 has division, suppose not, then $7 = z^2 + w^2$ has a solution, but since $0 = z^2 + w^2$ has no non-trivial solution in $\mathbb{F}_7$, hence we have $7 = (7\alpha)^2 + (7\gamma)^2 = 49(\alpha^2 + \gamma^2)$ which is impossible
- Check Q_2 has division, suppose not, then $3 = z^2 + w^2$ has a solution, but since $0 = z^2 + w^2$ has no non-trivial solution in $\mathbb{F}_3$, hence we have $3 = (3\alpha)^2 + (3\gamma)^2 = 9(\alpha^2 + \gamma^2)$ which is impossible
- $(-1, 3)/\mathbb{Q}_7$ split, consider $x^2 + y^2 - 3z^2 - 3w^2 = 0$, let $y = z = 1$, $w = 0$ and $f(x) = x^2 - 2$, then $f(3) \equiv 0 \bmod 7$ and $f'(3) \equiv 1 \bmod 7$, by Hensel's lemma 3.3 we know there exists $\mathbb{Q}_7 \ni \alpha \equiv 3$ such that $f(\alpha) = 0$

Example 3.5. Quaternion algebras over $\mathbb{F}_q (q = p^n, p \neq 2)$ split, just consider $1^2 - ax^2 - by^2 + 0^2 = 0 \Rightarrow ax^2 = 1 - by^2$, write $S_a = \{ax^2\}$, $S_b = \{1 - by^2\}$, then $|S_a| = |S_b| = |\{x^2\}| = \frac{q-1}{2} + 1 = \frac{q+1}{2}$, so S_a and S_b cannot be disjoint

4 Central Simple Algebras

Definition 4.1. A k-algebra A is a *simple* if the only two-sided ideals of A is 0 and A. A k*central algebra* is a finite k-algebra with $Z(A) = k$

Example 4.2. $M_n(k)$ as a left module is not simple, for example, consider left ideal generated by $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$

Example 4.3.

1. $M_n(k)$
2. Quaternion algebra A/k, F/k is a quadratic field extension such that A splits over F, i.e. $A \otimes_k F \cong M_2(F)$, thus $Z(A) \otimes_k F \subseteq Z(A \otimes_k F) = Z(M_2(F)) = F$, which implies that $Z(A) = k$. (Similarly, if $I \subseteq A$ is a two-sided ideal, then $I \otimes_k F$ is either $M_2(F)$ or 0, which implies that $I = A$ or $I = 0$ respectively)

Proposition 4.4. A, B are finite k-algebras, then $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$

Proposition 4.5. A is CSA/k, B finite k-alg, then two-sided ideals of $A \otimes_k B$ are of the form $A \otimes_k J$ where $J = I \cap (1 \otimes_k B)$ is a two-sided ideal in B

Example 4.6. If $D = (a, b)/k$, $D' = (a, b')/k$, then $D \otimes_k D' \cong (a, bb') \otimes_k M_2(k)$

Example 4.7. D is a k-central division algebra, then $M_n(k) \otimes_k D \to M_n(D)$ $(a_{ij}) \otimes d \mapsto (a_{ij}d)$ is an iso, in particular $M_n(k) \otimes M_m(k) \to M_{nm}(k)$ is the Kronecker product

Theorem 4.8 (Wedderburn's theorem)**.** *A is a finite simple k-alg, then $A \cong M_n(D)$ for some division k-alg and some n, D is unique up to iso, n is unique. Moreover, if A is k-central, so is D*

As a corollary of a Theorem 4.8, $\dim_k(A) = n^2$, so we can define

Definition 4.9. The the *degree* of a simple k-algebra is the square root of its dimension

The notion of a CSA is really irrelevant with respect to base change, as the following proposition asserts

Proposition 4.10. *A is a finite k-algebra, F/k field extension. Then A is a CSA/k iff $A \otimes_k F$ is a CSA/F for all F(for some F)*

Lemma 4.11. *If D is a finite division $\bar{k}$ algebra, then $D \cong \bar{k}$*

Theorem 4.12. *A finite k-algebra A is CSA/k iff $A \otimes_k \bar{k} \cong M_n(\bar{k})$*

Proof. □

5 Galois Splitting Fields

6 Brauer Groups

Theorem 6.1 (Relative Skolem-Noether theorem)**.** *S is a CSA/k, $R \hookrightarrow S$ is a simple k-algebra, suppose $f, g : R \to S$ are are homomorphisms, there there exists automorphism $\alpha : S \to S$ such that $\alpha \circ f = g$*

Consider A is a CSA/k with E being a maximal subfield where E/k is finite Galois with Galois group G, then for each $\sigma \in G$, we can find $x_\sigma \in A^\times$ such that $x_\sigma a x_\sigma^{-1} = \sigma(a)$, $\forall a \in E$. If y_σ is another choice, then x_σ, y_σ differ by $E^\times$, hence this defines $x_\sigma x_\tau = \alpha_{\sigma,\tau} x_{\sigma\tau}$
$\alpha : G \times G \to E^\times$ is actually a 2-cocycle

Definition 6.2. Suppose H is an abelian group with a G action, $Z^2(G, H)$ consists of $\alpha : G \times G \to H$ such that $\alpha_{\rho\sigma,\tau} \cdot \alpha_{\rho,\sigma} = \rho(\alpha_{\sigma,\tau}) \cdot \alpha_{\rho,\sigma\tau}$. $B^2(G, H)$ consists of $\gamma_{\sigma,\tau} = \frac{\sigma(f_\tau)\cdot f_\sigma}{f_{\sigma\tau}}$

Lemma 6.3. *Suppose A is a finite dimensional k-algebra, $E/k \subseteq A$ is a finite Galois extension with Galois group G, and if $\{x_\sigma\}_{\sigma \in G} \subseteq A^\times$ such that $x_\sigma a x_\sigma^{-1} = \sigma(a)$, $\forall a \in E$. Then x_σ are E-linear independent in A*

Proof. □

Proposition 6.4. *Suppose $\alpha : G \times G \to E^\times$ is a 2-cocycle, There is a k-algebra $(E/k, \alpha) := \oplus E x_\sigma$ with $x_\sigma x_\tau = \alpha_{\sigma,\tau} x_{\sigma\tau}$, $x_\sigma a x_\sigma^{-1} = \sigma(a)$, $\forall a \in E$. This is a CSA/k. Moreover, $(E/k, \alpha) \cong (E/k, \beta)$ if $\alpha \sim \beta$*

Proof. □

Theorem 6.5. *Consider $\phi : \mathrm{Br}(E/k) \to H^2(G, E^\times)$*

Proof. Consider the inverse $\phi^{-1} : H^2(G, E^\times) \to \mathrm{Br}(E/k)$, $[\alpha] \mapsto (E/k, \alpha)$ □

Definition 6.6. Suppose H is a group with a G-action, then

$$H^0(G, H) = Z^0(G, H) = H^G = \{h \in H | \sigma(h) = h, \forall \sigma \in G\}$$

If H is not abelian, this is a pointed set

Remark. A sequence of pointed set is $L \xrightarrow{\pi} M \xrightarrow{\rho} N$, and every element in $\ker \rho$ has an preimage in L. If $N = \{*\}$, then π is surjective, but even if $L = \{*\}$, ρ might be non-injective

Proposition 6.7. Suppose $1 \to A \to B \to C \to 1$ is an exact sequence of groups with G-action, then there is the long exact sequence

$$1 \to H^0(G, A) \xrightarrow{(1)} H^0(G, B) \xrightarrow{(2)} H^0(G, C) \xrightarrow{\delta^1} H^1(G, A) \xrightarrow{(3)} H^1(G, B) \xrightarrow{(4)} H^1(G, C)$$

Moreover, if A is central in B, then δ^2 exists and we can extend this with $\xrightarrow{\delta^2} H^2(G, A) \to H^2(G, B) \to H^2(G, C)$

Proof.

□

Example 6.8.

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

Then we get $H^1(G, E^\times) \to H^1(G, \mathrm{PGL}_n(E))(\cong CSA/k) \xrightarrow{\delta^2} H^2(G, \times E)(\cong \mathrm{Br}(E/k))$

Proposition 6.9.

1. For CSA/k A, B with $\deg A = n$, $\deg B = m$, $\delta^2_{nm}([A \otimes_k B]) = \delta^2_n([A])\delta^2_m([B])$
2. For CSA/k A with $\deg A = n$, $\delta^2_n([A]) = 0 \iff A \cong M_n(k)$
3. If $[E : k] = n$, then δ^2_n is surjective, and $\phi^{-1} \circ \delta^2_n([(E/k, \alpha)]) = [(E/k, \alpha)^{\mathrm{op}}]$

Proposition 6.10. Suppose A is a CSA/k with $\operatorname{ind} A = d$, then $\operatorname{ind} A^{\otimes r} \mid \binom{d}{r}$, $r \leq d$. In particular, $A^{\otimes r}$ split, and $\mathrm{Br}(E/k)$ are torsion

Proof. Let E/k be finite Galois extension that splits A, $G = \mathrm{Gal}(E/k)$, $V = E^{\oplus d}$, we get the following commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & E^\times \arrow[r] \arrow[d, "\lambda \mapsto \lambda^r"'] & \mathrm{GL}(V) \arrow[r] \arrow[d, "\pi"'] & \mathrm{GL}(V) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & E^\times \arrow[r] & \mathrm{GL}(\bigwedge^r V) \arrow[r] & \mathrm{PGL}(\bigwedge^r V) \arrow[r] & 1
\end{tikzcd}$$

Here $\pi(\phi) = \bigwedge^r \phi$, so we get exact squares

□

References