Cyclic Algebras

What is a Cyclic Algebra?

It's a generalization of quaternion algebra to an arbitrary degree

k: field that contains primitive mth root of unity ω.

A degree m cyclic algebra can be described as:

$$\langle x, y \mid x^m = a,\ y^m = b,\ xy = \omega yx \rangle.$$

Problem: It's not clearly why this defines a CSA.

Construction of Cyclic algebras:

K/k be a cyclic Galois Extension. $G := Gal(K/k) \cong \mathbb{Z}/m\mathbb{Z}$.

$\chi: G \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z}$.

$b \in k^\times$.

then we want to associate a CSA/k w/ these datas.

$$\deg m \text{ CSA}/k \longleftrightarrow (K/k)\text{-twisted forms of matrix algebra } M_m(k).$$

$$\tilde{F}(b) = \begin{bmatrix} 0 & \cdots & b \\ 1 & \ddots & \vdots \\ \vdots & \ddots & 0 \\ 0 & \cdots & 0 \end{bmatrix} \in GL_m(k) \qquad \Rightarrow \tilde{F}(b)^m = b \cdot I_m.$$

$F(b)$: image of $\tilde{F}(b)$ in $PGL_m(k)$, $\Rightarrow F(b)^m = I_m$.

$\Rightarrow F(b)$ has order m in $PGL_m(k)$.

$$z(b): G \xrightarrow{\chi}_{\sim} \mathbb{Z}/m\mathbb{Z} \longrightarrow PGL_m(k) \xhookrightarrow{i} PGL_m(K).$$

$$1 \longmapsto F(b)$$

Get a 1-cocycle $z(b): G \longrightarrow PGL_m(K)$.

$G \curvearrowright PGL_m(K)$. acting on each entry.

$\sigma \in G \curvearrowright M \in PGL_m(K)$.

$a_{\sigma\tau} = a_\sigma \cdot \sigma(a_\tau)$

Construction 2.3.6 :

A : a group equipped w/ a left action by another grp G.

X : A set that G & A act in a compatible way.

i.e. $\sigma(a(x)) = \sigma(a)\cdot(\sigma(x))$, $\forall\ x \in X,\ a \in A,\ \sigma \in G$.

Assume we're given a 1-cocycle $\sigma \longmapsto a_\sigma$ of G w/ values in A.

$\Rightarrow$ Define the twisted action of G on X by the cocycle a_σ via

$$(\sigma, x) \longmapsto a_\sigma(\sigma(x)).$$

What we've done in 2.3 & 2.4.

a_σ repesents some cohomology class in $H^1(G, \mathrm{Aut}_{\bar{k}}(\bar{k}))$.

Take $G := \mathrm{Gal}(K/k)$, $A = \mathrm{Aut}_K(\bar{k})$, $X = V_K$

We proved that the invariant subspace $({}_aV_K)^G$ under the twisted action of G gives a twisted form of $(V, \bar{k})$.

$G \cong \mathbb{Z}/m\mathbb{Z}$. $A = PGL_m(K)$. $V_K = M_m(K)$.

$\Rightarrow \left(_{Z(b)} M_m(K)\right)^G$ gives us a CSA / k splits by K.

Denote (χ, b). Cyclic algebra.

Prop 2.5.2 : The algebra (χ, b), can be described as:

$\exists\ y \in (\chi, b)$. s.t. (χ, b) is generated as a k-algebra by K and y.

Subject to :

$$\star : \boxed{y^m = b, \quad \lambda y = y\sigma(\lambda), \quad \forall\ \lambda \in K, \quad \langle\sigma\rangle = G, \quad \chi : G \longrightarrow \mathbb{Z}/m\mathbb{Z},\ \sigma \longmapsto 1.}$$

Rk : K is a commutative k-algebra in (χ, b). but it's not contained in the center

$\lambda y \lambda^{-1} = y\sigma(\lambda)\lambda^{-1} = y$ only $\sigma(\lambda) = \lambda$. not possible.

Pf: Let A be the k-algebra defined by ★.

Define a k-algebra homo $\bar{j}: A \longrightarrow M_m(K)$.

$$y \longmapsto \tilde{F}(b)$$

$$\lambda \longmapsto \begin{bmatrix} \lambda & & & 0 \\ & \sigma(\lambda) & & \\ & & \sigma^2(\lambda) & \\ 0 & & & \ddots \\ & & & & \sigma^{m-1}(\lambda) \end{bmatrix}, \quad \lambda \in K.$$

To check $\bar{j}$ is a homomorphism:

$$\bar{j}(\lambda y) = \bar{j}(y\sigma(\lambda)) = \tilde{F}(b) \cdot \begin{bmatrix} \sigma(\lambda) & & & \\ & \sigma^2(\lambda) & & \\ & & \ddots & \\ & & & \sigma^{m-1}(\lambda) \\ & & & & \lambda \end{bmatrix} = b\lambda$$

$$\| \qquad\qquad \tilde{F}(b) = \begin{bmatrix} 0 & \cdots & \cdots & b \\ 1 & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{bmatrix}$$

$$\bar{j}(\lambda)\,\bar{j}(y) = \begin{bmatrix} \lambda & & & \\ & \sigma(\lambda) & & \\ & & \ddots & \\ & & & \sigma^{m-1}(\lambda) \end{bmatrix} \cdot \tilde{F}(b) = \lambda b.$$

First, show: $\mathrm{im}(\bar{j}) = \bar{j}(A) \subseteq (\chi, b)$.

$$Z(b)^{M_m(K)^G} = \left\{ M \in M_m(K) \;\middle|\; \tilde{F}(b)\,\sigma(M)\,\tilde{F}(b)^{-1} = M \right\}.$$

Image of generators of A: $\bar{j}(y) = \tilde{F}(b)$, $\bar{j}(\lambda) = y\sigma(\lambda)$. also satisfy

$\Rightarrow \mathrm{im}(\bar{j}) \subseteq (\chi, b)$.

$\bar{j}: A \longrightarrow M_m(K)$

$(\bar{j} \otimes \mathrm{id}_K)(A \otimes_k K)$ in $M_m(K)$ is the K-subalgebra generated by

$\tilde{F}(b)$ & diagonal algebra $\underbrace{K \oplus K \oplus \cdots \oplus K}_{m \text{ copies of } K}$.

$\{E_{ij}\}$ for $M_m(K)$. It suffices to show $\forall E_{ij} \in (\bar{j} \otimes \mathrm{id}_K)(A \otimes_k K)$.

$E_{ij} = \tilde{F}(b)^{i-j} E_{jj}$ for $i \neq j$. ($\tilde{F}(b) \nearrow \bar{j}(y)$; E_{jj}: diagonal.)

∎

"Converse".

Prop 2.5.3: Assume A is a CSA / k of deg m, containing a k-subalgebra K, which is a cyclic Galois field extension of deg m, then A is isomorphic to a cyclic algebra given by a presentation in prop 2.5.2:

$\exists\, y \in (\chi, b)$, s.t. (χ, b) is generated as a k-algebra by K and y,

subject to $y^m = b$, $\lambda y = y\sigma(\lambda)$, $\forall \lambda \in K$, $\langle\sigma\rangle = G$, $\chi: G \to \mathbb{Z}/n\mathbb{Z}$, $\sigma \mapsto 1$.

Lemma: $\exists\, y \in A^\times$, s.t. $y^{-1}xy = \sigma(x)$, $\forall x \in K$, where $\langle\sigma\rangle = G = Gal(K/k)$.

Pf: To avoid confusing notation,

take $\tilde{K}/k$, $\tilde{K} \cong K$, $\tilde{G} := Gal(\tilde{K}/k) \cong G$

Then $A \otimes_k \tilde{K}$ is split by Prop 2.29 (If a CSA of deg $n \geq K$. K/k deg n ext. then CSA Splits / K).

$K \otimes_k \tilde{K} \longrightarrow A \otimes_k \tilde{K}$ is $\tilde{G}$-equivariant, $\tilde{G} \curvearrowright$ 2nd factor.

Let $G \curvearrowright K \otimes_k \tilde{K}$ on the first factor. These two actions commute.

In proof of 2.3.8,

$K \otimes_k \tilde{K} \cong \tilde{K}^m$, the action of G permutes the components on RHS.

Under the diagonal embedding,

$K \otimes_k \tilde{K} \longrightarrow A \otimes_k \tilde{K} \cong M_m(\tilde{K})$.

we may identify the permutation of the components of the diagonal w/ conjugation by a permutation matrix. So can find an element

$y \in GL_m(\tilde{K}) \cong (A \otimes_k \tilde{K})^\times$ s.t. $\sigma(x) = y^{-1} x y$, $\forall\, x \in K \otimes_k \tilde{K}$.

Then it remains to show that we may choose $y \in A^\times \subset (A \otimes_k \tilde{K})^\times$.

For all $\tilde{\tau} \in \tilde{G}$, $x \in K$ (View $K \hookrightarrow K \otimes_k \tilde{K}$ via first factor).

$\sigma(x) = \sigma(\tilde{\tau}(x)) = \tilde{\tau}(\sigma(x)) = \tilde{\tau}(y^{-1} x y) = \tilde{\tau}(y^{-1})\tilde{\tau}(x)\tilde{\tau}(y) = \tilde{\tau}(y)^{-1} x \tilde{\tau}(y)$

($\tilde{G}$ acts trivially on K; $\hookrightarrow$ $\tilde{G}$, G-actions commute)

Then define $z_{\tilde{\tau}} := y\tilde{\tau}(y)^{-1}$ satisfies $z_{\tilde{\tau}}^{-1} x z_{\tilde{\tau}} = x$, $\forall\, x \in K$.

$\Rightarrow z_{\tilde{\tau}} \in Z_A(K) \otimes_k \tilde{K}$

↳ Centralizer of K in A.

Also $K \xrightarrow{\sim} Z_A(K)$. (pass to the split case, then $A \otimes_k \tilde{K} \cong M_m(\tilde{K})$, so $Z_A(K)$ only contains diagonal matrices. so dim $= m$. $K \otimes_k \tilde{K} \cong \tilde{K}^m$, also dim m).

$\Rightarrow \tilde{\tau} \longmapsto z_{\tilde{\tau}}$ has values in $(K \otimes_k \tilde{K})^\times$, and it's a 1-cocycle for $\tilde{G}$ by construction.

What is $H^1(\tilde{G}, (K \otimes_k \tilde{K})^\times)$?

$$(K \otimes_k \tilde{K})^\times = \mathrm{Aut}_{K \otimes_k \tilde{K}}(K \otimes_k \tilde{K}).$$

So $H^1(\tilde{G}, (K \otimes_k \tilde{K})^\times)$ classifies K-algebras B, s.t. $B \otimes_k \tilde{K} \cong K \otimes_k \tilde{K}$, as $K \otimes_k \tilde{K}$-algebras.

For dimension reasons, these algebras are already isomorphic /k.

So $H^1(\tilde{G}, (K \otimes_k \tilde{K})^\times) = 1$.

$\Rightarrow \exists\, y_0 \in (K \otimes_k \tilde{K})^\times$, s.t. $z_{\tilde{\tau}}(y)^{-1} = y_0 \tilde{\tau}(y_0)^{-1}$, $\forall\, \tilde{\tau} \in \tilde{G}$.

Then replace y by $y_0^{-1} y$ in $\sigma(x) = y^{-1} x y$. $\Rightarrow \tilde{\tau}(y) = y$, $\forall\, \tilde{\tau} \Rightarrow y \in A^\times$ (fixed by Gal).

Proof to 2.5.3 :

Claim : y in the previous Lemma satisfies $y^m \in k$.

$\sigma(x) = y^{-1}xy$

Replace x by $\sigma(x)$ $\Rightarrow$ $\sigma^2(x) = y^{-1}\sigma(x)y = y^{-1}(y^{-1}xy)y = y^{-2}xy^2$.

Iterate $(m-1)$ times, get $x = \sigma^m(x) = y^{-m}xy^m$

$\hookrightarrow \sigma \in Gal(K/k) \cong \mathbb{Z}/m\mathbb{Z}$.

$\Rightarrow y^m$ commutes w/ $\forall x \in K$, $\Rightarrow y^m \in Z_A(K) = K$.

Apply again, $\sigma(y^m) = y^{-1}y^m y = y^m$. $\Rightarrow y^m \in k$.

Set $b := y^m$. Then it remains to show that K & y generate A.

i.e. Check $\{1, y, \cdots, y^{m-1}\}$ are K-linearly independent in A.

See the book. Pretty much linear algebra.

□

Ex :

(1). k, m is invertible in k, and k contains a primitive m-th root of unity ω.

for $a, b \in k^\times$,

$$(a,b)_\omega = \langle x, y \mid x^m = a,\ y^m = b,\ xy = \omega yx \rangle.$$

In the case $m=2$, $\omega = -1$. $\Rightarrow$ generalized quaternion algebras.

$K = k(\sqrt[m]{a})$, $\chi : Gal(K/k) \longrightarrow \mathbb{Z}/m\mathbb{Z}$

$(\sigma : \sqrt[m]{a} \longmapsto \omega\sqrt[m]{a}) \longmapsto 1$.

Take $x = \sqrt[n]{a}$, y constructed in 2.5.3.

(3) $m = p$, $\operatorname{char} k = p$.

for $a \in k$, $b \in k^\times$,

$$[a, b) = \langle x, y \mid x^p - x = a,\ y^p = b,\ xy = y(x+1) \rangle.$$

Rk: $x^p - x = a$ defines a cyclic Galois extension.
Gal given by $\alpha \longmapsto \alpha + i$, $0 \le i \le p+i$.

$x = \alpha$, y constructed in 2.5.3.

In chapter 4, by Kummer (Artin-Shreier) theory,

One may write an arbitary cyclic extension of deg m (deg p),

as $K = k(\sqrt[m]{a})$. ($K = k(\alpha)$, $\alpha^p - \alpha - a = 0$).

The class of non-split quaternion algebra has order 2 in the Brauer group.

More generally, one can show that the class of a cyclic division algebra $(a, b)_w$ defined above has order m. So the class of a tensor product of deg m cyclic algebras has order dividing m in the Brauer group.

Then the converse:

(Merkurjev-Suslin): Assume k contains primitive mth root of unity w.

Then a CSA $/k$ whose class has order dividing m in $Br(k)$ is Brauer equivalent to a tensor product

$$(a_1, b_1)_w \otimes_k \cdots \otimes_k (a_i, b_i)_w \quad \text{of cyclic algebras.}$$