Cyclic Matters

David Saltman
Center for Communications Research

June 2022

I. Prime Degree p - p always odd

1. Characteristic p

F field characteristic p, L/F cycle Galois degree $p \Rightarrow L = F(x)$, $x^p - x = a \in F$ AND $\sigma(x) = x+1$

FACT: Still true for commutative rings R with $pR = (0)$.

Also, G a $p-$group ,S/R -G Galois $\Rightarrow S \simeq R[G]$ (Normal basis).

2. Mixed Characteristic:

Commutative rings R will be (for a while)

$\mathbb{Z}[p]$ algebra, $\rho^p = 1$ primitive, $\eta = \rho - 1$.

Define $x^p + g(x) \in \mathbb{Z}[\rho]$ by

$$(1 + x\eta)^p = 1 + (x^p + g(x))\eta^p$$

Theorem:

1. Modulo η, $x^p + g(x) \equiv x^p - x$.

2. If $S = R[T]/(T^p + g(T) - a)R[T]$, $a \in R$

   AND $1 + a\eta^p \in R^*$ THEN

   S/R is $G = \langle\sigma\rangle$ Galois,

   $$\boxed{\sigma(x) = \rho x + 1}$$

   (and converse - Galois $\Rightarrow 1 + a\eta^p \in R^*$)

3. If $R \to \bar{R}$, $\eta\bar{R} = 0$, $(p\bar{R} = 0)$ and $\bar{S}/\bar{R}$ is C_p Galois $\Rightarrow \bar{S}$ lifts to S/R which is C_p Galois

   IF $1 + \eta R \subseteq R^*$

   (e.g., R local but in many more cases)

"Corollary:" Can remove $\rho \in R$ assumption via corestriction (not super easy).

3. Degree p Azumaya algebras

In my thesis (1976!)

I showed that if $pR = 0$

Br$(R)[p]$ generated by "differential crossed products" which are algebras generated by x, y subject to $xy - yx = 1$, x^p, y^p central.

Call this algebra $[a, b]$ if $x^p = a$, $x^p = b$.

Note: Azumaya even if $ab = 0$! (i.e., All a, b).

Surprising observation (+ many years)

In $[a, b]$, xy satisfies $(xy)^p - (xy)$ central and is Galois!

ALMOST CYCLIC Algebras

Split Case:

$$\begin{pmatrix} \star & \diamond & & & & & & b \\ \bullet & \star & \diamond & & & & & \\ & \bullet & & & & & & \\ & & \ddots & \ddots & \ddots & & & \\ & & & & & & \diamond & \\ & & & & & \bullet & \star & \diamond \\ a & & & & & & \bullet & \star \end{pmatrix}$$

Diagonal $= R[xy]$. Super diagonal element + "a" is x. Subdiagonal element plus b is y.

Note: xy might be singular but rank $\geq p-1$ since xy separable $\Rightarrow$ 0 at most 1 eigenvalue $\Rightarrow x, y$ rank $\geq p-1$. So mod any maximal ideal can assume all super diagonal entries of x and subdiagonal entries y are $\neq 0$ though $a = 0$, $b = 0$ possible

$\Rightarrow R[xy]$, x, y generates full matrix ring.

WHAT IS NOT IMPORTANT: "differential" "crossed product" "characteristic p"

WHAT IS IMPORTANT: $R[xy]/R$ cyclic Galois, rank $xy \geq p-1$

Characteristic 0 example:

R a $\mathbb{Z}[\rho]$ algebra

A/R generated by x, y such that $x^p = a \in R$, $y^p = b \in R$ AND

$$xy - \rho yx = 1.$$

Call $A = [a, b]_\rho$.

This Azumaya $\Leftrightarrow 1 + ab\eta^p \in R^*$

because $R[xy]/R$ Galois

$$\sigma(xy) = \rho(xy) + 1 \quad (xy)^p + g(xy) = ab$$

Theorem: $R \to \bar{R}$, $\eta\bar{R} = 0, (1 + \eta R) \subseteq R^* \Rightarrow$ $\mathrm{Br}(R) \to \mathrm{Br}(\bar{R})$ subjective on elements of order p.

By the way, what does "almost cyclic" mean?

Look at $[a,b]\rho$. Let $S = R[xy]$, $1 + ab\eta \in R^*$

$$(xy)x = x(yx) = x(\rho^{-1}xy - p^{-1}) = x\sigma^{-1}(xy).$$

SO if $P_\sigma = \{z \in A \mid z\theta = \sigma(\theta)z \text{ all } \theta \in S\}$ then $x \in P_\sigma$.

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

SO $y^{p-1} \in P_\sigma$

Matrix argument from above shows

$P_\sigma P_{\sigma^{-1}} = R$ and $(P_\sigma)^p = R$

$\Rightarrow P_\sigma$ is in Pic(S).

Definition: Almost cyclic algebra of degree p.

S/R degree p, $G = \langle \sigma \rangle$ Galois

$I \in \mathrm{Pic}(S)$ with $\varphi : I^p \cong S$.

$A = \Delta(S/R, \sigma, I, \varphi) =$

$S \oplus I \oplus \cdots \oplus I^{p-1}$. Use φ to multiply.

I hard to work with but $[a, b]$ and $[a, b]_\rho$ are special.

Hidden in all above:

S/R is $G = \langle \sigma \rangle$ Galois, $|G| = p$

then $R[G] = R[T]/(T^p - 1)R[T]$

and $(T^p - 1) = (T - \rho^{p-1}) \dots (T - \rho)(T - 1)$

$R[G]$ is iterated fiber product but only care about

$$R[G](1) = R[T]/(T - \rho)(T - 1)R[T].$$

Theorem: TFAE

1. $S \cong R[G]$ (normal basis)

2. $S(1) \cong R[G](1)$

3. $S = R[T]/(T^P + g(T) - a)R[T]$ some a.

In general,

if $P(1)$ is a rank one $R[G](1)$ projective, $P(1)/(T-1)P(1) \cong R$ and $P_1 = P(1)/(T-\rho)P(1)$ satisfies $P_1^p \cong R$

<u>AND</u> $P(\rho)^G \cong R *_p R$

$\Rightarrow$ build S/R G-Galois from $P(1)$ so $P(1) = S(1)$

Description of $R *_p R$ as fiber diagram.

$$\begin{array}{ccc} R *_p R & \longrightarrow & R \\ \downarrow & & \downarrow \\ R & \longrightarrow & R/\eta^p R \end{array} \qquad \text{pull back}$$

$P(p)^G$ always rank one projective over $R *_p R$ and $P(p)^G \cong R *_p R \Rightarrow P_1^p \cong R$

II. Degree p^n Cyclic Extensions

Basically if $R = \mathbb{Z}[\rho][x]\left(\frac{1}{1+\eta^p x}\right)$ and $S = R[T]/(T^p + g(T) - x)$ then S/R "generic" or "versal" mixed characteristic

Now for generalization $R = \mathbb{Z}[\rho][x_1, \ldots, x_n]\left(\frac{1}{s}\right)$

where $s \in 1 + \eta M$, $M = (x_1, \ldots, x_n)$.

<u>Note</u>:

$$\begin{aligned} R/\eta R &= F_p[x_1, \ldots, x_n] \\ R/MR &= \mathbb{Z}[\rho]. \end{aligned}$$

Suppose S/R is C_{p^r} "versal" or "generic" in some sense.

<u>Vital</u>: in characteristic p gives all.

Next steps:

1. Build $T/S/R$ $C_{p^{r+1}}$ Galois

2. Make generic

1 is hard, 2 is easy:

$R \subset R' = R[x_{n+1}](1/1 + \eta x_{n+1})$

form $S' = R'[T]/(T^p + g(T) - x_{n+1})$

form $T \otimes S'$ over R'

is $C_{p^r} \oplus C_p$ Galois

$C'_p \hookrightarrow$ diagonal $C_{p^r} \oplus C_p$ Form $(T \otimes S')^{C'_p}$.

Moral: "Generic" T = special T times generic degree p.

To accomplish 1 need an Albert criterion for rings: When does S/R extend? Recall L/K C_{p^r} extends $\Leftrightarrow \Delta(L/K, \rho) = 1 \in \mathrm{Br}(K)$

Think of S/R as G/C Galois

$$|G| = p^{r+1}$$
$$|C| = p$$
$$C = \langle \tau \rangle$$

cyclic. Form

$$A = \Delta(S[C]/R[C], \sigma, \tau)$$

Remember $\tau \in C$! A is actually

$S * [G]-$ twisted group ring where G acts on S

$$
\begin{aligned}
A(1) &= \frac{A}{(\tau-\rho)(\tau-1)A} \text{ is really important piece} \\
&= \Delta(S[C](1)/R[C](1), \rho) \\
\rho &= \text{image } \tau.
\end{aligned}
$$

Theorem: S/R extends to $C_{p^{r+1}}$ Galois $T/S/R \Leftrightarrow A(1) \simeq \mathrm{End}_{R[C](1)}(P(1))$ where $P_0 = P(1)/(\tau - 1) \cong S$ (over G/C) (easy to arrange) **and** $P(\rho)^G \cong R *_p R$.

Note $\to$ One Brauer group condition (like Albert). One Picard group condition.

Ideas in proof:

When $R = \mathbb{Z}[\rho][x_1, \ldots x_n](1/s)$ as above R is regular so $\mathrm{Br}(R) \hookrightarrow \mathrm{Br}(q(R))$ and deal with Brauer condition at field level (old Albert condition).

Also $\mathrm{Pic}(R) = \mathrm{Pic}(\mathbb{Z}[\rho])$ **and** $R^* \to (R/\eta)^*$ surjective **and** $\mathrm{Pic}(R/\eta) = (0)$

The above ideas allow one to lift cyclic extensions of degree p and p^2. We conjecture:

If $1 + \eta R \subset R^*$, $\eta \in P$, $\bar{R} = R/P$ then every degree p^r cyclic $\bar{S}/\bar{R}$ lifts to a cyclic S/R of the same degree.

III. Degree p^r Almost Cyclic Azumaya Algebras

Let S/R be G-Galois, G cyclic order n. Let $J \in$ Pic(S) have $N(J) \simeq R$. Then $\Delta(S/R, \sigma, \tau, \varphi) = T/I$ as follows

$S[t, \sigma] \supseteq S \oplus Jt \oplus (Jt)^2 \cdots = T$

$(Jt)^m = J\sigma(J) \ldots \sigma^m(J)t^m$

so $(Jt)^n \cong N(J)St^n$

$\varphi : (Jt)^n \cong S$ G-preserving. Set $I = \langle x - \varphi(x) \rangle$.

Then $[a, b]$ and $[a, b]_\rho$ are almost cyclic.

The very general definition above too hard to work with. So let R be a domain, S/R cyclic Galois group G with $|G| = n$ $F = q(R)$ $K = S \otimes_R F$ Set:

$B = \Delta(K/F, \sigma, a)$.

Assume $x, y \in B$, $x^n = a$, $y^n = b$

$$xs = \sigma(s)x \quad sy = y\sigma(s).$$

Assume

$$\alpha = xy \in S$$

and

$$Sa + S\alpha + S\mathrm{adj}(\alpha) + Sb = S$$

where

$$\mathrm{adj}(\alpha) = N(\alpha)/\alpha.$$

Let $A = \Delta(S/R, a, \alpha, b)$ be the subalgebra of B generated by S, x, y.

Theorem: $A = \Delta(S/R, a, \alpha, b)$ is Azumaya if and only if $Sa + S\alpha + S\text{adj}(\alpha) + Sb = S$.

Set

$$J_\sigma = Sx + Sy^{n-1} \subseteq \{z \in A | zs = \sigma(s)z\}$$

and

$$J_{\sigma^{-1}} = Sx^{n-1} + Sy \subseteq \{z \in A | sz = z\sigma(s)\}.$$

Then

$$J_\sigma J_{\sigma^{-1}} = Sa + Sb + S\alpha + S \text{ adj}(\alpha)(!)$$

This shows $J_\sigma \in \text{Pic}(S)$ when $Sa + S\alpha + S\text{adj}(\alpha) + Sb = S$.

How construct?

S/R is "a-split" $\Leftrightarrow S/aS$ split over R/aR.

Lemma: Suppose S/R is $G = \langle\sigma\rangle$ Galois and a-split. Then $\exists\alpha \in S$ and an almost cyclic $A = \Delta(S/R, a, \alpha, b)$. If R is regular the Brauer class of A only depends on S/R and a.

What we actually use:

If $a \in R$ and $\alpha \in S$ is such that $a \mid n(\alpha)$ **and** $Sa + S\alpha + S\text{adj}(\alpha) = S$ we say a, α are **suitable** in S.

Note that $Sa + S\alpha + S\text{adj}(\alpha) = S$ means α has rank $\geq n - 1$ modulo aS.

We use suitable a, α to solve 2 problems. First is to make concrete the p-divisiblilty of Br(R) when $pR = (0)$.

Theorem: Suppose $pR = 0$, R/aR domain and S/R cyclic Galois degree p^r. Let $A = \Delta(S/R, a, \alpha, b)$ be such at a, α are suitable in S. Then $\exists$ degree p^{r+1} T/R and $\alpha' \in T$ with a, α' suitable in T and a $B = \Delta(T/R, a, \alpha', b')$ with $p[B] = [A]$ in $\mathrm{Br}(R)$.

Corollary: Apply this to $[a, b]$ over $F_p[a, b]$ to get general result!

Let R be a $\mathbb{Z}[\rho]$ algebra (commutative) and $\bar{R} = R/\eta R$.

Let $\bar{A} = \Delta(\bar{S}/\bar{R}, a, \alpha, b)$ with a, α suitable in S so $(\bar{S}/a\bar{S})/(\bar{R}/a\bar{R}) = \tilde{S}/\tilde{R}$ split.

Take pullback:

$$
\begin{tikzcd}
 & \hat{S}/\hat{R} \arrow[dl] \arrow[dr] & \\
\bar{S}/\bar{R} \arrow[dr] & & \text{split}/\bar{R} \arrow[dl] \\
 & \tilde{S}/\tilde{R} &
\end{tikzcd}
$$

$\hat{R} = R/(\eta R \cap aR)$ and $\widehat{S}$ defined by pullback. Lift $\widehat{S}$ to S/R to get a-split S.

Assume $\bar{R}$ regular so Brauer class only depends on a. Apply to $F_p[a, b]$.

The following is a currently a conjecture, but the above ideas yield the result for Brauer classes of order p and p^2.

Theorem: Let R be a $\mathbb{Z}[\rho]$ algebra. and $\bar{R} = R/\eta R$. Assume $(1 + \eta R) \subseteq R^*$. Then $\mathrm{Br}(R) \to \mathrm{Br}(R/\eta)$ surjective on p-primary parts.