# Galois action on Fermat curves: non-vanishing of obstruction map

Dr. Rachel Pries

Colorado State University
rachelpries@gmail.com

$KR^2V$: joint work with R. Davis, V. Stojanoska, K.Wickelgren

Thanks for invitation!

16th Arithmetic, Geometry, Cryptography, and Coding Theory
Luminy, June 2017

# Outline

We compute (maps between) Galois cohomology groups of Fermat curves which arise in connection with obstructions to rational points.

1. The Fermat curve $X$ with affine equation $U : x^p + y^p = 1$.
2. The splitting field $L$ of $1 - (1 - x^p)^p$ and $Q = \mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$.
3. Explicit formula for Galois action on $H_1(U)$.
4. The Kummer maps $X(K) \to H^1(G_K, H_1(U))$, with $K = \mathbb{Q}(\zeta_p)$.
5. Computing the differential map $\delta_2$ on $H^1(Q, H_1(U))$.
6. Using Heisenberg extensions to bound $H^1(G_K, H_1(U))$.

$KR^2V$: joint work with R. Davis, V. Stojanoska, K.Wickelgren

# 1. The Fermat curve

Fix $p$ odd prime. Let $\zeta$ be a $p$th root of unity.

Let $X$ be the (smooth projective) curve $x^p + y^p = z^p$.

$X$ is the **Fermat curve**, with affine equation $x^p + y^p = 1$.

The genus of $X$ is $g = \frac{(p-1)(p-2)}{2}$.

(this is not a talk about) **Fermat's Last Theorem:**
If $[x : y : z] \in X(\mathbb{Q})$ then $xyz = 0$.

Let $Z$ be the closed subscheme of $p$ points where $z = 0$.

Let $U = X - Z$.

Let $Y \subset X$ be closed subscheme of $2p$ points where $xy = 0$.
$Y = \{(\zeta^i, 0), (0, \zeta^j) \mid i, j \in \mathbb{Z}/p\}$.

# Survey: points on Fermat curve over number fields

The points of $Z$ and $Y$ are defined over the cyclotomic field $K = \mathbb{Q}(\zeta)$.

**Debarre/Klassen:** all but finitely many points of $X$ of degree $p-1$ arise by intersecting $X$ with $\mathbb{Q}$-rational line through a point of $X(\mathbb{Q})$.

**Klassen/Tzermias, Tzermias, Sall:** for Fermat curve of degree $p = 5, 7$, have complete description of degree $\leq p-1$ points.

Also: Cusps yield all torsion points on $\mathrm{Jac}(X)$.
Cusps: $C = Y \cup Z = \{[x : y : z] \in X \mid xyz = 0\}$.

Fix one cusp $b = [0 : 1 : 1]$. Embed $\iota : X \to \mathrm{Jac}(X)$ by $\iota(P) = [P - b]$.

## Theorem - Anderson

For $p$ an odd prime, let $L$ be the splitting field of $1-(1-x^p)^p$.

Let $J_Z(X)$ be the generalized Jacobian of $X$ with conductor $Z$.

Let $b =$ "$(1,0)-(0,1)$", a $\mathbb{Q}$-rational point of $S$.

The number field generated by the $p$th roots of $b$ in $J_Z(X)(\overline{\mathbb{Q}})$ is $L$.

(It contains $L$ if $n$ is not prime).

Similar results: Greenberg, Ihara, Coleman,

# 2. Facts about the splitting field $L$ of $1-(1-x^p)^p$

i) $L = K(\sqrt[p]{1-\zeta^i} : 1 \leq i \leq p-1)$, where $K = \mathbb{Q}(\zeta_p)$.

ii) $K/\mathbb{Q}$ ramified only over $p$ and $L/K$ ramified only over $\langle 1-\zeta_p \rangle$.

iii) $L = K(\zeta_{p^2}, \sqrt[p]{1-\zeta^i} : 1 \leq i \leq r)$ with $r = (p-1)/2$.
(because $(1-\zeta^i)/(1-\zeta^{-i}) = -\zeta^i$).

iv) $Q := \mathrm{Gal}(L/K) \simeq (\mathbb{Z}/p)^\rho$ is an elementary abelian $p$-group.

v) The rank $\rho = r+1$ if and only if Vandiver's Conjecture is true for $p$.

**Vandiver's Conjecture (first conjectured by Kummer in 1849)**

The prime $p$ does not divide the class number $h^+$ of $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

True for all $p <$ 163 million (Buhler/Harvey) and for all regular primes.

# Relative homology

Recall that $U = X - Z$.

Consider étale homology groups with coefficients in $\mathbb{Z}/p$.

The homology group $H_1(U)$ has dimension $(p-1)^2$.

Its quotient $H_1(X)$ has dimension $2g = (p-1)(p-2)$.

The relative homology group $M = H_1(U, Y)$ has dimension $p^2$.

Let $\beta \in M = H_1(U, Y)$ be the path (singular 1-simplex)
$\beta : [0,1] \to U(\mathbb{C})$ given by $t \mapsto (\sqrt[p]{t}, \sqrt[p]{1-t})$ (real $p$th roots).

Why is the relative homology easier to work with?

# 3. Action of automorphisms on homology

The group $\mu_p \times \mu_p$ acts on $X : x^p + y^p = z^p$ (stabilizing $U$ and $Y$).

Consider the group ring $\Lambda_1 = (\mathbb{Z}/p)[\mu_p \times \mu_p] = \mathbb{F}_p[\varepsilon_0, \varepsilon_1]/\langle \varepsilon_i^p - 1 \rangle$.

Nilpotent generators: $y_i = \varepsilon_i - 1$, then $\Lambda_1 = \mathbb{F}_p[y_0, y_1]/\langle y_i^p \rangle$.

The Jacobian (and other (co)homology groups) are $\Lambda_1$-modules

Note that $\dim(H_1(U, Y)) = p^2 = \dim(\Lambda_1)$.

Let $\beta \in M = H_1(U, Y)$ be the chosen path (singular 1-simplex)

**Theorem - Anderson**

$M = H_1(U, Y)$ is a free $\Lambda_1$-module of rank 1 with generator $\beta$.

# Galois action on homology

Let $K = \mathbb{Q}(\zeta)$ and let $G_K$ be its absolute Galois group.

The Jacobian (and other (co)homology groups) are modules for $G_K$.

Since $M = H_1(U, Y)$ is a free $\Lambda_1$-module of rank 1 with generator $\beta$,

the action of $\sigma \in G_K$ on $M$ is determined by its action on $\beta$.

For $p$ an odd prime, let $L$ be the splitting field of $1 - (1 - x^p)^p$.

**Theorem - Anderson**

Then $\sigma \in G_K$ acts trivially on $M = H_1(U, Y)$ if and only if $\sigma$ fixes $L$.

The action of $G_K$ on $M = H_1(U, Y)$ factors through $Q = \mathrm{Gal}(L/K)$.
If $q \in Q$, then action determined by $q \cdot \beta = B_q \beta$ for some $B_q \in \Lambda_1$.

# 3. Explicit formula for $B_q$

The action of $G_K$ on $M = H_1(U, Y)$ factors through $Q = \mathrm{Gal}(L/K)$.
If $q \in Q$, then action determined by $q \cdot \beta = B_q \beta$ for some $B_q \in \Lambda_1$.

Anderson gave a theoretical characterization of $B_q$.
Corollary (A): $(B_q - 1)\beta \in H_1(U)$ so $B_q - 1 \in \langle y_0 y_1 \rangle$.

**Theorem $KR^2V$ - For $p$ satisfying Vandiver's conjecture:**

The action of $q \in Q$ on $H_1(U, Y)$ is determined explicitly by:

$$B_q = \frac{E(\gamma_q(\varepsilon_0))E(\gamma_q(\varepsilon_1))}{E(\gamma_q(\varepsilon_0\varepsilon_1))}.$$

Corollary ($KR^2V$): $B_q$ has norm 0 for all $q \in Q$ if $p \geq 5$.

Corollary ($KR^2V$): $\mathrm{codim}(H_1(U)^Q, M^Q) = 2$ for all $p$.

# Explicit formula: example when $p = 3$

If $p = 3$, then $L = K(\zeta_9, \sqrt[3]{1-\zeta^{-1}})$
and $Q = \langle \sigma, \tau \rangle$ (commuting elements of order 3)

$\sigma$ acts by multiplication by $\zeta$ on $\zeta_9$ and
$\tau$ acts by multiplication by $\zeta$ on $\sqrt[3]{1-\zeta^{-1}}$.

$\Lambda_1 = \mathbb{Z}/3[\mu_3 \times \mu_3]$ generated by $\varepsilon_0$ and $\varepsilon_1$, and $y_i = \varepsilon_i - 1$.

When $p = 3$, then

$$B_\sigma - 1 = -(1-\varepsilon_0)(1-\varepsilon_1)(\varepsilon_0 + \varepsilon_1) = y_0 y_1 (1 - y_0 - y_1)$$

$$B_\tau - 1 = (1-\varepsilon_0)(1-\varepsilon_1)(-1 + \varepsilon_0\varepsilon_1) = y_0 y_1 (-y_0 - y_1 + y_0 y_1).$$

$N(B_\tau) := 1 + B_\tau + B_\tau^2 = 0$ and $H_1(U)^Q = \langle y_0^2 y_1, y_0 y_1^2, y_0^2 y_1^2 \rangle$.

# 4. The Kummer map on rational points

Classical Kummer map: if $\theta \in K^*$, let $\kappa(\theta) : G_K \to \mu_p$ by $\kappa(\theta)(\sigma) = \frac{\sigma \sqrt[p]{\theta}}{\sqrt[p]{\theta}}$.

Generalized Kummer map: pick $b = (0,1) \in X(K)$ and let $\pi = \pi_1(X_{\bar{K}}, b)$.

**Kummer map**

Define $\kappa : X(K) \to \mathbf{H^1}(\mathbf{G_K}, \pi)$, by $\kappa(x) = [\sigma \mapsto \gamma^{-1}\sigma\gamma]$ ($\gamma$ is path $b \mapsto x$).

The map $\kappa^{\mathrm{ab,p}} : X(K) \to \mathbf{H^1}(\mathbf{G_K}, \pi^{\mathrm{ab}} \otimes \mathbb{Z}_\mathbf{p})$ is injective.

Since $X$ has good reduction away from $p$,
it factors through $\kappa^{\mathrm{ab,p}} : X(K) \to \mathbf{H^1}(\mathbf{G}, \pi^{\mathrm{ab}} \otimes \mathbb{Z}_\mathbf{p})$, where

$G = G_{K,S}$ is Galois group of max. extension of $K$ ramified only over $\langle 1 - \zeta \rangle$ and the infinite places, and $\pi^{\mathrm{ab}}$ is max. abelian quotient of $\pi$.

Change to $\mathbb{Z}/p$ coefficients.

# 5. The $\delta_2$ map viewed as an obstruction

Let $G = G_{K,S}$ (Galois group of max. ext. of $K$ ram. only over $p$ and $\infty$)

Given $\xi \in H^1(G, H_1(U))$, does there exist $\eta \in X(K)$ s.t. $\kappa(\eta) = \xi$?

Let $W = H_1(U) \wedge H_1(U) \simeq [\pi]_2/[\pi]_3$.

There is a map $\delta_2 : H^1(G, H_1(U)) \to H^2(G, W)$.
If $\eta \in X(K)$, then $\delta_2(\kappa^{\mathrm{ab}}(\eta)) = 0$.

**Observation (Ellenberg):** the non-vanishing of $\delta_2$ yields an obstruction to lifting a point $\eta' \in \mathrm{Jac}(X)(K)$ to a point $\eta$ of $X(K)$.

$\delta_2(\eta) = [-,-]_*(\eta \cup \eta) + L(\eta)$ for some linear map $L(\eta)$.
$[-,-]_*$ is anti-commutative.
$[-,-]_*(\xi_1 \cup \xi_2) : G \times G \to W$ is $(g_1, g_2) \mapsto \xi_1(g_1) \wedge_{\mathbb{Z}/p\mathbb{Z}} g_1 \circ \xi_2(g_2)$.
Schmidt/Wingberg: $\delta_2$ factors through $G$.

# Strategy

Recall $\kappa : U(K) \to H^1(G, H_1(U))$ and $\delta_2 : H^1(G, H_1(U)) \to H^2(G, W)$.

If $\eta \in U(K)$, then $\delta_2(\kappa(\eta)) = 0$.

(1) Compute $\kappa$ on well-known points, e.g., $\eta \in Y$.

(2) Use relation $\delta_2(\eta_1 + \eta_2) = \delta_2(\eta_1) + \delta_2(\eta_2) + [-,-]_*(\eta_1 \cup \eta_2)$ to compute $\delta_2$ on span of these in $H^1(G, H_1(U))$.

(3) Show non-zero except at well-known points.

Current status: for $\eta \in Y$, finished (1) and (2) for all $p$ and (3) for $p = 3$.
for $\eta$ a tangential base point at $z \in Z$, finished (1) up to shift.

# 4. The Kummer map on points of $Y$

We determine the Kummer map $\kappa^{\mathrm{ab}} : U(K) \to H^1(Q, H_1(U))$ on the points of $Y(K) = \{(\zeta^i, 0), (0, \zeta^j) : i, j \in \mathbb{Z}/p\}$.

**Prop: $KR^2V$**

The cocycle $q \mapsto (1 - \varepsilon_1^j)(B_q - 1)$ is a cocycle representing $\kappa^{\mathrm{ab}}((0, \zeta^j))$.
The cocycle $q \mapsto \varepsilon_0^i(B_q - 1)$ is a cocycle representing $\kappa^{\mathrm{ab}}((\zeta^i, 0))$.

**Proof:** Let $\beta \in H_1(U, Y)$ be path $(\sqrt[p]{t}, \sqrt[p]{1-t})$ in $U$ from $(0,1)$ to $(1,0)$.

Then $\varepsilon_0^i \beta$ is a path from $(0,1)$ to $(\zeta^i, 0)$.

Then $\kappa^{\mathrm{ab}}((\zeta^i, 0))$ is represented by the cocycle that takes

$q \in Q$ to $q(\varepsilon_0^i \beta) - \varepsilon_0^i \beta = q(\varepsilon_0^i \beta) - \varepsilon_0^i \beta = \varepsilon_0^i (B_q - 1)\beta$.

# 4. Dimension of image of Kummer map on $Y$

Let $S_Y = \mathrm{Span}\{\kappa(\eta) \mid \eta \in Y\}$, in $H^1(Q, H_1(U))$.

**Prop: $KR^2V$**

The dimension of $S_Y$ is $2p-3$.
The relations are: $\kappa^{ab}((0,1)) = 0$, $\sum_{y_\eta=0} \kappa^{ab}(\eta) = 0$, $\sum_{x_\eta=0} \kappa^{ab}(\eta) = 0$.

Proof: uses long exact sequence, for $M = H_1(U, Y)$,

$$H_1(U)^Q \to M^Q \stackrel{g}{\to} JY^Q \stackrel{\kappa}{\to} H^1(Q, H_1(U)) \to H^1(Q, M) \to H^1(Q, JY) \ldots$$

Note that $JY^Q = JY$ since the points $\eta \in Y$ are fixed by $Q$.
Now $\dim(S_Y) = \dim(\mathrm{Coker}(g))$.
So $\dim(\mathrm{Coker}(g)) = \dim(JY^Q) - \mathrm{codim}(H_1(U)^Q, M^Q) = 2p-3$.

The cocycle $\sum_{y_\eta=0} \kappa^{ab}(\eta)$ is: $q \mapsto \sum_{j=0}^{p-1} \varepsilon_0^i (B_q - 1) = y_0^{p-1}(B_q - 1)$.
This equals 0 since $B_q - 1 \in \langle y_0 y_1 \rangle$.

# 5. Non-vanishing of obstruction when $p = 3$

Let $S_Y = \mathrm{Span}(\kappa(\eta) \mid \eta \in Y) \subset H^1(Q, H_1(U))$.

Let $\delta_2 : H^1(Q, H_1(U)) \to H^2(Q, W)$.

When $p = 3$: $\dim(H_1(U)) = 4$, $\dim(H^1(Q, H_1(U))) = 6$, and $\dim(S) = 3$;

$\dim(W) = 6$ and ** $H^2(Q, W) \simeq W^3$ since all $q \in Q$ act trivially on $W$.

**Application:** when $p = 3$, if $s \in S_Y$ has the property that $\delta_2(s) = 0$, then $s = \kappa(\eta)$ for one of the 6 points $\eta \in Y$.

Note: this calculation can be done for any $p$ but ** more complicated.

Current work:
let $S_Z = \mathrm{Span}\{\kappa(t_z) \mid z \in Z\}$ where $t_z$ tangential base point at $z$.
Expectation: $\dim(S_Z) = p - 1$ and $S_Z \cap S_Y = \{0\}$.

# 6. Bounding $H^1(G, H_1(U))$

Determine info about target for Kummer map $\kappa : X(K) \to H^1(G, M)$.

Recall $Q = \mathrm{Gal}(L/K)$ and $L/K$ ramified only above $p$ and $\infty$.
Let $N = \mathrm{Gal}(\tilde{L}/L)$ where $\tilde{L}$ is maximal elementary abelian $p$-group extension of $L$ ramified only above $p$ and $\infty$.
Note $\tilde{L}/K$ Galois and $0 \to N \to G \to Q \to 0$.

Spectral sequence argument yields
$0 \to H^1(Q, M) \to \mathbf{H^1(G, M)} \to \mathrm{Ker}(d_2) \to 0$,

(B) Differential $d_2 : H^1(N, M)^Q \to H^2(Q, M)$

**Theorem:** Complete analysis of $\mathrm{Ker}(d_2)$ for all odd primes $p$.

**Application:** If $p = 3$, then $\dim(H^1(G_K, M)) = 13$, explicit description.

(C) lower bound on $\mathrm{Ker}(d_2)$ from Heisenberg extensions of $K$.

# Exact sequence for target of Kummer map

Kummer map $\kappa^{\mathrm{ab}} : X(K) \to \mathbf{H^1}(\mathbf{G}, \pi^{\mathrm{ab}})$.

Let $G$ (resp. $N$) be Galois group of maximal extension of $K$ (resp. $L$) ramified only over $p$ and infinite places.

Write short exact sequence $1 \to N \to G \to Q \to 1$.

Goal: calculate $\mathbf{H^1}(\mathbf{G}, \mathbf{M})$ where $M$ trivial $N$-module, $M = H_1(U, Y)$.

Spectral sequence yields:

## Exact sequence

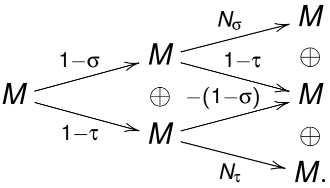
$$0 \to H^1(Q, M) \to \mathbf{H^1}(\mathbf{G}, \mathbf{M}) \to \mathrm{Ker}(d_2) \to 0,$$

where $d_2 : H^1(N, M)^Q \to H^2(Q, M)$.

# Understanding $H^1(Q,M)$

$$0 \to H^1(Q,M) \to \mathbf{H^1(G,M)} \to \mathrm{Ker}(d_2) \to 0,$$

**Example:** When $p=3$, then $\dim(H^1(Q,M))=9$.
Can compute $H^1(Q,M)$ using cohomology $(\mathrm{Ker}/\mathrm{Im})$ of complex:




**Example:** when $p=5$, then $\dim(H^1(Q,M))=33$.

# (B) Kernel of $d_2$, set-up

Suppose $1 \to N \to G \to Q \to 1$ is an exact sequence

Fix a set-theoretic section $s : Q \to G$
This yields 2-cycle $w : Q \times Q \to N$ via $w(q_1, q_2) = s(q_1)s(q_2)s(q_1 q_2)^{-1}$.
Let $w^{\mathrm{ab}} : Q \times Q \to N^{\mathrm{ab}}$.

Consider the differential $d_2 : H^1(N, M)^Q \to H^2(Q, M)$.

Suppose $N$ acts trivially on $M$ (true here by Anderson)

Then $\phi \in H^1(N, M)^Q$ "is" a $Q$-invariant homomorphism $\phi : N \to M$.
Since $M$ is abelian, $\phi$ factors through $\phi^{\mathrm{ab}} : N^{\mathrm{ab}} \to M$.
Since $\phi$ is fixed by $Q$, it determines a map $\phi_* : H^2(Q, N^{\mathrm{ab}}) \to H^2(Q, M)$.

**Proposition:** *$KR^2V$*

Then $d_2(\phi) = \pm \phi_* w^{\mathrm{ab}}$.

# Kernel of $d_2 : H^1(N,M)^Q \to H^2(Q,M)$

Recall the section $s : Q \to G$ with $Q = \langle \tau_0, \tau_1 \ldots, \tau_r \rangle$.

Let $a_i = s(\tau_i)^p$ and $c_{i,j} = s(\tau_j)s(\tau_i)s(\tau_j)^{-1}s(\tau_i)^{-1}$.

Then $a_i, c_{i,j} \in N = \mathrm{Ker}(G \to Q)$.

**Theorem:** *$KR^2V$*

Let $\phi : N \to M$ be in $H^1(N,M)$. Then $\phi \in \mathrm{Ker}(d_2)$ iff $(\phi(a_i), \phi(c_{i,j}))$ is in image of map in a cohomology complex associated with $Q$.

Explicitly, $\phi \in \mathrm{Ker}(d_2)$ if and only if $\phi(a_i) = N_{\tau_i}$ $(= 0$ for $p \geq 5)$
and, for some map of sets $f : \{0, \ldots, r\} \to M$,
$\phi(c_{i,j}) = (B_{\tau_j} - 1)f(i) - (B_{\tau_i} - 1)f(j)$ (note this is in $H_1(U)$).

# Application: Kernel of $d_2$ when $p = 3$

Let $p = 3$. Then $L = \mathbb{Q}(\zeta_9, \sqrt[3]{1-\zeta^{-1}})$.

Then $Q = \langle \sigma, \tau \rangle$ where $\tau$ fixes $\zeta_9$ and $\sigma$ fixes $\sqrt[3]{1-\zeta^{-1}}$.

Recall the section $s : Q \to G = G_{K,S}$.

Let $a_0 = s(\sigma)^3$, $a_1 = s(\tau)^3$, and $c = s(\tau)s(\sigma)s(\tau)^{-1}s(\sigma)^{-1}$.

Then $a_0, a_1, c \in N = G_{L,T}$ since they are in kernel of $G \to Q$.

## Example when $p = 3$

Let $\phi : N \to M$ be in $H^1(N, M)^Q$. Then $\phi \in \mathrm{Ker}(d_2)$ if and only if

$\phi(a_0) = tN_\sigma = t(1+\varepsilon_1+\varepsilon_0^2)(1+\varepsilon_1+\varepsilon_1^2)$ for $t \in \mathbb{Z}/3$,

$\phi(a_1) = 0$, and $\phi(c) \in H_1(U)$.

# Application: When $p = 3$ then $\dim(\mathrm{Ker}(d_2)) = 4$

**Proof sketch:**
Magma: $\dim_{\mathbb{F}_3}(N) = 10$, $\dim(M) = 9$ so $\dim(H^1(N, M)) = 90$.

Magma: $\dim(H^1(N, M)^Q) = 14$.
$\phi \in H^1(N, M)$ is fixed by $q \in Q$ iff $\phi(q \cdot_{\mathrm{conj}} n) = B_q \cdot \phi(n)$ for all $n \in N$.

Magma: find element of $H^2(N, Q)$ classifying split exact sequence:
Use $\omega \in H^2(N, Q)$ for section $s$ of $0 \to N \to G \to Q \to 0$.
Determine $a_0 = s(\sigma)^3$, $a_1 = s(\tau)^3$, and $c = [s(\tau), s(\sigma)]$

Magma: The subspace of $\phi \in H^1(N, M)^Q$ s.t. $\phi$ of $a_0$, $a_1$, $c$ satisfying Theorem $\mathrm{Ker}(d_2)$ restrictions has dimension 4.

Algebra: have explicit basis for $\mathrm{Ker}(d_2)$ when $p = 3$.
spanned by dimension 3 subspace arising from Heisenberg extensions and dimension 1 subspace arising from cyclotomic extension $\mathbb{Q}(\zeta_{p^3})$.

# (C) Heisenberg extensions

For all $p$, we determine a lower bound for $\dim(\mathrm{Ker}(d_2))$.

Let $M = H_1(U, Y)$ be relative homology of Fermat curve.

The differential map is $d_2 : H^1(N, M)^Q \to H^2(Q, M)$.

**Theorem: $KR^2V$**

For all $p$, there is a 'Heisenberg' subspace $\mathrm{Ker}(\overline{d}_2) \hookrightarrow \mathrm{Ker}(d_2)$ that can be described explicitly.

**Example:** $p = 5$, then $\dim(\mathrm{Ker}(\overline{d}_2)) = 9$.

So $\dim(H^1(G, M)) \geq 42$.

Note $\dim(H_1(U) \cap M^Q) = 9$.

# Heisenberg extensions

$H_p$: upper triangular $3 \times 3$ matrices with coeffs in $\mathbb{Z}/p$, 1's on diagonal.

$U_p$: normal subgroup, upper right is the only non-zero off diagonal.

The extension $1 \to U_p \to H_p \to (\mathbb{Z}/p)^2 \to 1$ classified by

the cup product $\iota_1 \cup \iota_2$ in $H^2((\mathbb{Z}/p)^2, \mathbb{Z}/p)$

where $\iota_1$, $\iota_2$ in $H^1((\mathbb{Z}/p)^2, \mathbb{Z}/p)$ given by two projections $(\mathbb{Z}/p)^2 \to \mathbb{Z}/p$.

## (special case of) Theorem of Sharifi

Let $F = K(\sqrt[p]{a}, \sqrt[p]{b})$ with $\mathrm{Gal}(F/K) \simeq (\mathbb{Z}/p)^2$.

There is an $H_p$-Galois field extension $R/K$ dominating $F/K$

iff $\kappa(a) \cup \kappa(b) = 0$ in $H^2(G_K, \mathbb{Z}/p)$.

# Heisenberg extensions

Fix $1 \leq I \leq p-1$, let $a = \zeta_p^I$ and $b = 1 - \zeta_p^I$ and let

$$F_I = K(\sqrt[p]{\zeta_p^I}, \sqrt[p]{1 - \zeta_p^I}).$$

Steinberg relation: the cup product $\kappa(a) \cup \kappa(b) = 0$ is zero.

So there is $R_I/K$ dominating $F_I/K$ such that $\mathrm{Gal}(R_I/K) \simeq H_p$.
Also, $R_I/F_I$ has modulus (conductor) $p^2 + p(p-1)/2$.
In fact, $R_I = F_I(\sqrt[p]{c_I})$ where, for $w = \zeta_{p^2}$,

$$c_I = \prod_{J=1}^{p-1} (1 - \zeta_p^{IJ} w^I)^J,$$

and $\tau_0(c_I) = \frac{(1-w^I)^p}{1-\zeta_p^I} c_I$ and other $\tau_i$ act by multiplication by $\zeta_p$.

Example: When $p = 3$, then $c_1 = (1 - w^4)(1 - w^7)^2$.

# Heisenberg extensions

Let $\tilde{R}$ be the compositum of $R_l$ for $1 \leq l \leq p-1$.

The field extension $\tilde{R}/K$ is Galois and ramified only over $p$.

Let $\bar{N} = \mathrm{Gal}(\tilde{R}/L)$ which is a quotient of $N$.

Recall $s$ section of $1 \to N \to G \to Q \to 1$, where $N = G$.

Recall $c_{i,j} = [s(\tau_j), s(\tau_i)] \in N$ and $r = (p-1)/2$.

**Proposition: $KR^2V$**

$|\bar{N}| = p^r$ and $\bar{N}$ is generated by the images of $c_{0,j}$ for $1 \leq j \leq r$.

$(M^Q)^r \simeq H^1(\overline{N}, M)^Q \hookrightarrow H^1(N, M)^Q$.

# This gives a lower bound for $\mathrm{Ker}(d_2)$ because....

$\mathrm{Ker}(N \to \bar{N})$ acts trivially on $M$, so $H^1(\bar{N}, M)^Q \hookrightarrow H^1(N, M)^Q$

Elements of $H^1(\bar{N}, M)^Q$ are $Q$-invariant maps $\bar{\phi} : \bar{N} \to M$.
$Q$-invariance means $\bar{\phi}(q \cdot \bar{n}) = q \cdot \bar{\phi}(\bar{n})$.
Note $q \cdot \bar{n} = \bar{n}$ since action is by conjugation and $U_p$ central in $H_p$.

Also $\bar{N}$ generated by $\bar{c}_{0,j}$ for $1 \leq j \leq r$.
$\bar{\phi} : \bar{N} \to M$ is $Q$-invariant iff $\bar{\phi}(c_{0,j}) \in M^Q$ (fixed by mult. by $B_q$).

Theorem $\mathrm{Ker}(\bar{d}_2)$: $\bar{\phi} \in \mathrm{Ker}(\bar{d}_2)$ iff $(\bar{\phi}(c_{0,j}))$ is in image of map in cohomology complex.

Explicitly, $\bar{\phi}(c_{0,j}) = (\tau_j - 1)f_0 - (\sigma - 1)f_j$ for some $f_0, \ldots, f_r$ s.t.
$(\sigma_j - 1)f_i - (\sigma_i - 1)f_j = 0$

**Abstract:** Fix $p$ odd prime. Let $K = \mathbb{Q}(\zeta_p)$.
Let $X$ be the Fermat curve $x^p + y^p = z^p$.

We extend work of Anderson about action of absolute Galois group $G_K$ on a relative homology group of $X$. He proved that the action factors through $Q = \mathrm{Gal}(L/K)$ where $L$ is splitting field of $1 - (1 - x^p)^p$.

For $p$ satisfying Vandiver's conjecture, we find explicit formula for the action of $q \in Q$ on the relative homology.

Using this, we determine the maps between several Galois cohomology groups which arise in connection with obstructions for rational points on a generalized Jacobian of $X$.

We obtain information about a differential map in the Hochschild-Serre spectral sequence for short exact sequence of Galois groups with restricted ramification.

This is joint work with R. Davis, V. Stojanoska, and K. Wickelgren.
Thanks!