Galois action on Fermat curves and Heisenberg extensions

Rachel Pries

Colorado State University
rachelpries@gmail.com

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

Thanks to organizers!

CTNT 2016 Research Conference
August 14, 2016

Outline

1. Warm-up: an exceptional extension L/K of number fields

2. Warm-up: an exceptional curve $X/\mathbb{Q}$.

3. Anderson: Galois action on relative homology $M = H_1(X - Z, Y)$

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

Step 1: Explicit formula for Galois action

Step 2: Computing differential maps in Galois cohomology

(A) Kummer maps $X(K) \to H^1(G_K, M)$

(B) Kernel of differential map d_2

(C) Heisenberg extensions

1. What is special about this number field?

Fix p odd prime. Let ζ be a pth root of unity.

Consider the cyclotomic field $K = \mathbb{Q}(\zeta)$.

Definition: Let L be the splitting field of $1-(1-x^p)^p$.

Then $L = K(\sqrt[p]{1-\zeta^i} : 1 \leq i \leq p-1)$.

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

The Galois group Q of L/K is an elementary abelian p-group.

Question: What is the rank of Q?

Note that $(1-\zeta^i)/(1-\zeta^{-i}) = -\zeta^i$.
Note that $\zeta_{p^2} \in L$.

What is special about this number field?

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

The Galois group Q of L/K is an elementary abelian p-group.

Note $\mathrm{rank}(Q) \leq r+1$ because L/K generated by pth roots of elements in subgroup $B \subset K^*/(K^*)^p$ generated by ζ_p and $1-\zeta_p^i$ for $1 \leq i \leq r$.

For given p, is $\mathrm{rank}(Q) = r+1$?

What is special about this number field?

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

The Galois group Q of L/K is an elementary abelian p-group.

Note $\mathrm{rank}(Q) \leq r+1$ because L/K generated by pth roots of elements in subgroup $B \subset K^*/(K^*)^p$ generated by ζ_p and $1-\zeta_p^i$ for $1 \leq i \leq r$.

For given p, is $\mathrm{rank}(Q) = r+1$?

Fact

The rank of Q equals $r+1$ if and only if Vandiver's Conjecture is true for the prime 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.

2. What is special about this curve?

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 $g = \frac{(p-1)(p-2)}{2}$.

2. What is special about this curve?

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 $xyz = 0$.

2. What is special about this curve?

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 $U = X - Z$ where Z is closed subscheme of p points where $z = 0$.

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

Debarre/Klassen: if $C/\mathbb{Q}$ is a smooth plane curve of degree d, then:

($d \geq 7$) the number of points of C of degree $< d-1$ over $\mathbb{Q}$ is finite;

($d \geq 8$) all but finitely many points of C of degree $d-1$ arise by intersecting C with rational line through rational point of C.

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 c. Embed $\iota : X \to \mathrm{Jac}(X)$ by $\iota(P) = [P - c]$.
Let $T = \iota(X) \cap \mathrm{Jac}_{\mathrm{tors}}$. **Rohrlich:** $\iota(C) \subset T$.

Coleman/Tamagawa/Tzermias: $\iota(C) = T$ for $p \geq 5$.

Why are this field and this curve in the same talk?

Theorem - Anderson

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

Let S be the generalized Jacobian of X with conductor Z.

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

Then L is the number field generated by the pth roots of b in $S(\overline{\mathbb{Q}})$.

Similar results: Ihara, Coleman,

Theorem: - Greenberg (paraphrased) Let $p \geq 5$ and let L_0 be the field generated over $K = \mathbb{Q}(\zeta)$ by the pth roots of real cyclotomic units of K. Then L_0 is the field generated by the points of order p on $\mathrm{Jac}(X)$.

3. Galois action on homology

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

Let $\Lambda_1 = (\mathbb{Z}/p)[\mu_p \times \mu_p]$, generators ε_0 and ε_1.

The Jacobian (and other (co)homology groups) are Λ_1-modules

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 pth roots).

Theorem - Anderson

$M = H_1(U, Y)$ is a free Λ_1-module of rank 1 with generator β.

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 Λ_1-module of rank 1 with generator β,

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

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 σ fixes L.

Galois action on homology

The G_K-action on $H_1(U,Y)$ factors through $Q = \mathrm{Gal}(L/K)$.

For $q \in Q$, write $q\beta = B_q\beta$ for some $B_q \in \Lambda_1 = (\mathbb{Z}/p)[\mu_p \times \mu_p]$.

Write $B_q = \sum_{0\le i,j<p} b_{i,j}\varepsilon_0^i\varepsilon_1^j$ (where $\varepsilon_0, \varepsilon_1$ generate $\mu_p \times \mu_p$)

Anderson: in theory, determines the action of G_K on $H_1(U,Y)$.

(i) B_q is a symmetric unit ($b_{i,j} = b_{j,i}$).

(ii) $(B_q - 1)\beta \in H_1(U)$,
i.e., $B_q - 1 \in (1-\varepsilon_0)(1-\varepsilon_1)\Lambda_1$ (augmentation ideal).
'rows' and 'columns' of $B_q - 1$ sum to zero mod p.

(iii) (Cliff note version) There are maps $\Lambda_0^* \xrightarrow{d'} (\Lambda_1^*)^{\mathrm{sym}} \xrightarrow{d''} \Lambda_2^*$ and $B_q \in \mathrm{Ker}(d'')$.
There is $\Gamma_q \in \Lambda_0^{sh}$, unique up to $\mathrm{Ker}(d')^{sh}$, s.t. $(d')^{sh}(\Gamma_q) = B_q$.

The logarithmic derivative of Γ_q in $\Omega(\Lambda_0^{sh})$ is represented by the class of $(q-1)\circ[0,1]$ in $H_1(\mathbb{A}^1 - \mu_p^*)$.

Step 1: Explicit formula for Galois action on homology

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 $B_q \in M$.

Fix generators of $Q \simeq (\mathbb{Z}/p)^{r+1}$: σ acts by multiplication by ζ on ζ_{p^2};
τ_j acts by multiplication by ζ on $\sqrt[p]{1-\zeta_p^{-j}}$ for $1 \leq j \leq r$.

Fix $Q \simeq (\mathbb{Z}/p)^{r+1}$ with $q \mapsto (c_0, \ldots, c_r)$. For $1 \leq j \leq r$, let $c_{p-j} = c_j + jc_0$. Let $c = \sum_{i=1}^{p-1} c_i$ and F a root of $F^p - F + c = 0$.
Let $\gamma_q(\varepsilon) = \sum_{i=1}^{p-1} (\frac{c_i + c - F}{i}) \varepsilon^i - \sum_{i=1}^{p-1} \frac{c_i}{i}$.
Let $\Lambda_0 = \mathbb{Z}/p[\mu_p]$ and $y = \varepsilon - 1$ (y nilpotent since $y^p = 0$). For $\gamma \in y\Lambda_0$, define $E(\gamma) = \sum_{i=0}^{p-1} f^i/i!$.
Let $T = \sum_{p}^{2p-1} \gamma_q(\varepsilon_0\varepsilon_1)^i/i!$ (error term since $(\varepsilon_0\varepsilon_1)^p \neq 1$).

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

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

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

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)

σ acts by multiplication by ζ on ζ_9 and
τ acts by multiplication by ζ on $\sqrt[3]{1-\zeta^{-1}}$.

$M = \mathbb{Z}/3[\mu_3 \times \mu_3]$ generated by ε_0 and ε_1

Our formula simplifies to:

$$B_\sigma - 1 = -(\varepsilon_0 + \varepsilon_1)(1-\varepsilon_0)(1-\varepsilon_1) = \text{“}\begin{pmatrix} 0 & -1 & 1 \\ -1 & -1 & -1 \\ 1 & -1 & 0 \end{pmatrix}\text{”}$$

and

$$B_\tau - 1 = (-1 + \varepsilon_0\varepsilon_1)(1-\varepsilon_0)(1-\varepsilon_1) = \text{“}\begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \end{pmatrix}\text{”}$$

Explicit formula, first observation about B_q

Example: when $p = 5$, then $Q = \langle \sigma, \tau_1, \tau_2 \rangle \simeq (\mathbb{Z}/5)^3$.

Let $x = \varepsilon_0 - 1$ and $y = \varepsilon_1 - 1$.

$$(B_\sigma - 1)/(xy) =$$
$$(x+y)(-2 - xy + 2x^2y^2 + (x+y)(-1+2xy)) + 2xy(1-xy)$$

$$(B_{\tau_1} - 1)/(xy) =$$
$$(x+y)(-1 + 2xy + 2x^2y^2 + (x+y)(1-x-y-xy))$$
$$+xy(-1 - xy + 2x^2y^2)$$

$$(B_{\tau_2} - 1)/(xy) =$$
$$(x+y)(1 - xy - 2x^2y^2 - (x+y)(1+2xy)) + xy(1 - 2xy + 2x^2y^2)$$

Proposition: KR^2V

If $p \geq 5$, then $(B_q - 1)/xy \in \langle xy, x+y \rangle M$ (constant coefficient 0).

Explicit formula: 2nd - 3rd observations about B_q

Recall $q \in Q$ acts by multiplication by B_q on $\beta \in H_1(U, Y)$.

Proposition: $KR^2\,V$

Consider the norm $N_q = \sum_{i=0}^{p-1} (B_q)^i$. Then $N_q = 0$ for all p and all $q \in Q$,

(except when $p = 3$ and q does not fix ζ_9,
in which case $N_\sigma = (1 + \varepsilon_0 + \varepsilon_0^2)(1 + \varepsilon_1 + \varepsilon_1^2)$).

Also, there is a conjugation action of $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/p)^*$ on Q.

Proposition: $KR^2\,V$. Let $\rho_a \in \mathrm{Perm}(M)$ be given by $\varepsilon_0^i \varepsilon_1^j \mapsto \varepsilon_0^{ia} \varepsilon_1^{ja}$.

Then $B^a_{\tau_{ia}} = \rho_a(B_{\tau_i})$ and $\mathrm{Ker}(B_{\tau_{ia}} - 1) = \rho_a(\mathrm{Ker}(B_{\tau_i} - 1))$,

Step 2: Compute Galois cohomology

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

(A) Kummer map: $X(K) \to H^1(G_K, M)$ (with restricted ramification)

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

(B) Differential $d_2 : H^1(N, M)^Q \to H^2(Q, M)$
$N = G_L$ (with restricted ramification), Galois group of ray class field

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.

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

Kummer map

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

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

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

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

Example of Kummer map

We compute the Kummer map $\kappa^{ab} : U(K) \to H^1(G_{K,S}, \pi_1^{ab}(U))$ on the points of $Y(K) = \{(\zeta^i, 0), (0, \zeta^j) : i, j \in \mathbb{Z}/p\}$.

Lemma

The cocycle $q \mapsto \zeta_1^j(B_q - 1)$ is a cocycle representing $\kappa^{ab}((0, \zeta^j))$.
The cocycle $q \mapsto (1 - \zeta_0^i)(B_q - 1)$ is a cocycle representing $\kappa^{ab}((\zeta^i, 0))$.

The cocycles representing $\kappa^{ab}(Y(K))$ are all trivial in $H^1(G_{K,S}, \pi_1^{ab}(U))$ because they are of the form $q \mapsto m(B_q - 1)$ for some $m \in M$.

Proof: Let $\beta \in H_1(U, Y)$ be the path in U from $(1, 0)$ to $(0, 1)$.

Then $\zeta_1^j \beta$ is a path from $(1, 0)$ to $(0, \zeta^j)$.

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

$q \in \mathrm{Gal}(L/K)$ to $q(\zeta_1^j \beta) - \zeta_1^j \beta = q(\zeta_1^j \beta) - \zeta_1^j \beta = \zeta_1^j (B_q - 1)\beta$.

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

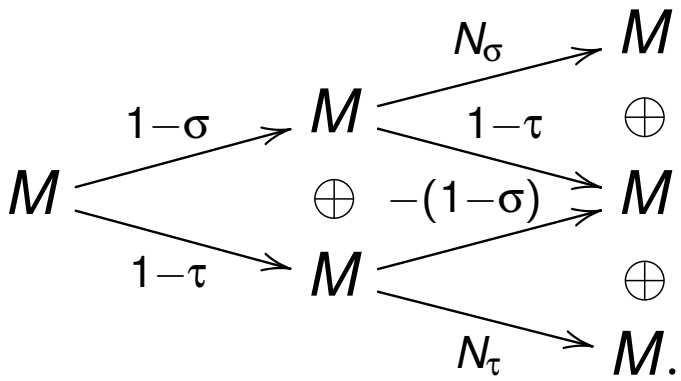
$$0 \to H^1(Q, M) \to \mathbf{H^1}(\mathbf{G}, \mathbf{M}) \to \mathrm{Ker}(d_2) \to 0,$$

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 (Ker/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, ϕ factors through $\phi^{\mathrm{ab}} : N^{\mathrm{ab}} \to M$.
Since ϕ 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 τ fixes ζ_9 and σ 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: Find subspace of $\phi \in H^1(N, M)^Q$ s.t. ϕ of a_0, a_1, c satisfy Theorem $\mathrm{Ker}(d_2)$ restrictions.

Example: When $p = 3$, have explicit basis for $\mathrm{Ker}(d_2)$.
Let $\eta \in L$ be the prime above 3. Let $n_4 \in N$ be in ray class group with modulus η^{20}. Then $\mathrm{Ker}(d_2)$ contains the map ϕ such that $\phi(n_4) = (1 + \varepsilon_0 + \varepsilon_0^2)(1 + \varepsilon_1 + \varepsilon_1^2)$.

(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: $KR^2\,V$

For all p, there is a 'Heisenberg' subspace $\mathrm{Ker}(\overline{d}_2) \hookrightarrow \mathrm{Ker}(d_2)$

and $\mathrm{Im}(B_q - 1) \cap M^Q \hookrightarrow \mathrm{Ker}(\overline{d}_2)$ for any $q \in Q$ fixing ζ_{p^2}.

Example: $p = 5$, $\dim(\mathrm{Im}(B_q - 1) \cap M^Q) = 8$ and $\dim(\mathrm{Ker}(\overline{d}_2)) = 9$

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

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

Heisenberg extensions

H_p: upper triangular 3×3 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 ι_1, ι_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 $1 \leq l \leq p-1$, let $a = \zeta_p^l$ and $b = 1 - \zeta_p^l$ and let

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

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

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

$$c_l = \prod_{J=1}^{p-1} (1 - \zeta_p^{lJ} w^l)^J,$$

and $\tau_0(c_l) = \frac{(1-w^l)^p}{1-\zeta_p^l} c_l$ and other τ_i act by multiplication by ζ_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: $KR^2\,V$

$|\bar{N}| = p^r$ 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.
$(\sigma_j - 1)f_i - (\sigma_i - 1)f_j = 0$

Algebraic work: image contains copy of $\mathrm{Im}(B_q - 1) \cap M^Q$.

Next steps

(I) Need more info on structure of ray class fields of L for $p \geq 5$.
Understand difference between $\mathrm{Ker}(\bar{d}_2)$ and $\mathrm{Ker}(d_2)$.

Example: When $p = 3$, then $\bar{\phi}$ determined by $m = \bar{\phi}(\bar{c}_{0,1})$.
Magma: $\bar{\phi} \in \mathrm{Ker}(\bar{d}_2)$ iff $m \in H_1(U)$ (dim 4)
and $-m_{11} + m_{10} + m_{01} - m_{00} = 0$
So $3 = \dim(\mathrm{Ker}(\bar{d}_2))$ while $\dim(\mathrm{Ker}(d_2)) = 4$.

(II) Need computation of Kummer map on points of $\mathrm{Jac}(X)(K)$.

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 arising in the Hochschild-Serre spectral sequence for short exact sequence of Galois groups with restricted ramification.

Heisenberg extensions play a key role in the outcome.

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

Fun application! using structure of B_q

Let $\ell \neq p$ be prime. Let f be the order of ℓ mod p.

Let χ be a character of order p on $\mathbb{F}$.

Jacobi sum $J(i,j) := J(\chi^i, \chi^j) = \sum_{a+b=1} \chi^i(a)\chi^j(b)$.

Consider Fermat curve $X/\mathbb{F}$ where $\mathbb{F} = \mathbb{F}_{\ell^f}$.

The zeta function $Z(X/\mathbb{F}, T) = L(X/\mathbb{F}, T)/(1-T)(1-|\mathbb{F}|T)$.

Weil: $L(X/\mathbb{F}, T) = \prod_{1 \leq i,j \leq p-1,\ i \neq j} (1 - J(i,j)T)$.

Iwasawa: $J(i,j) \equiv 1 \bmod (1-\zeta_p)^3$ for $p \geq 5$.

Fun application! using structure of B_q

Application: let $\mathbb{F} = \mathbb{F}_{\ell^f}$

Then $L(X/\mathbb{F}, T) \equiv (1-T)^{2g} \bmod p$.

Note: this can also be proven using facts about Jacobi sums.

Proof: $B_q - 1$ acts on $H^1(U, Y)$ nilpotently.
So char. poly. of B_q on $H_1(X)$ is $(1-T)^{2g}$ for all q.

Example: $p = 3$

If $\ell \equiv 1 \bmod 3$, then $L(X/\mathbb{F}_\ell, T) = 1 + AT + LT^2$,
where $A \equiv 1 \bmod 3$ is such that $4L = A^2 + 27B^2$.

If $\ell \equiv 2 \bmod 3$, then $L(X, \mathbb{F}_{\ell^2}) = 1 + 2LT + L^2T^2$.

What is special about this number field?

Lemma: Vandiver's Conjecture true for p implies Q has rank $r+1$.

Proof: Let E be the units in $\mathcal{O}_K$ and $E^+ = E \cap K^+$.

Let $C = V \cap E$ be the cyclotomic units where $V \subset K^*$ is generated by $\{\pm\zeta_p, 1-\zeta_p^i : 1 \leq i \leq p-1\}$. Let $C^+ = C \cap \mathcal{O}_{K^+}^*$.

Then h^+ is the index of C^+ in E^+.

If Vandiver's conjecture is true for p, then E/E^p is generated by C.

Recall L/K generated by pth roots of elements in subgroup $B \subset K^*/(K^*)^p$ generated by ζ_p and $1-\zeta_p^i$ for $1 \leq i \leq r$.

Then $B = \langle 1-\zeta_p, B' \rangle$ where $B' \subset K^*/(K^*)^p$ is generated by the cyclotomic units C. By Vandiver hypothesis, $B' = E/E^p$.

By Dirichlet's unit theorem, $E \simeq \mathbb{Z}^{r-1} \times \mu_p$ so B' has rank r.