# Galois action on the homology of Fermat curves

Rachel Pries

Colorado State University
pries@math.colostate.edu

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

Thanks to Joe!

Silvermania, Brown University
August 12, 2015

**Abstract:** Fix $p$ odd prime. Let $K = \mathbb{Q}(\zeta_p)$.

Let $X$ be the Fermat curve $x^p + y^p = z^p$.

Anderson studied the action of the absolute Galois group $G_K$ on a relative homology group of $X$ (Duke, 1987). He proved that the action factors through $Q = \mathrm{Gal}(L/K)$ where $L$ is the the splitting field of $1-(1-x^p)^p$. Using this, he obtained results about the field of definition of points on a generalized Jacobian of $X$.

We build upon Anderson's work: for $p$ satisfying Vandiver's conjecture, we compute $Q$ and find explicit formula for the action of $q \in Q$ on the relative homology. Using this, we obtain information about maps between several Galois cohomology groups which arise in connection with obstructions to rational points.

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

# Background on Fermat curve

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

Let $X$ be the Fermat curve $x^p + y^p = z^p$, having genus $g = \frac{(p-1)(p-2)}{2}$.

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 $xy = 0$.

# Background on Fermat curve

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

Let $X$ be the Fermat curve $x^p + y^p = z^p$, having genus $g = \frac{(p-1)(p-2)}{2}$.

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 $xy = 0$.

(this is not a talk about) Fermat's Last Theorem: $X(\mathbb{Q}) = Z \cup Y$.

# Other results about rational points

## Theorem - Greenberg (paraphrased)

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

## 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 $\infty$.
Let $b =$ "$(0,1)-(1,0)$", a $\mathbb{Q}$-rational point of $S$.
Then $L$ is the number field generated by the $p$th roots of $b$ in $S(\overline{\mathbb{Q}})$.

Similar results obtained by Ihara and Coleman.

# Étale homology groups (coefficients in $\mathbb{Z}/p$)

There is an action of $\mu_p \times \mu_p$ on $X : x^p + y^p = z^p$ (stabilizing $U$ and $Y$) given by $(\zeta^i, \zeta^j) \cdot [x, y, z] = [\zeta^i x, \zeta^j y, z]$.

Let $\Lambda_1 = (\mathbb{Z}/p)[\mu_p \times \mu_p]$, generators $\varepsilon_0$ and $\varepsilon_1$.

The Jacobian (and other (co)homology groups) are $\Lambda_1$-modules and also modules for $G_K$, the absolute Galois group of $K = \mathbb{Q}(\zeta)$.

Consider the homology group $H_1(U)$, dimension $(p-1)^2$
and its quotient $H_1(X)$, dimension $2g = (p-1)(p-2)$
and the relative homology group $M = H_1(U, Y)$, dimension $p^2$.

Consider the class $\beta \in M$ of 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).

# Galois action on relative homology

Recall $\beta \in H_1(U, Y)$ chosen singular 1-simplex and $\Lambda_1 = (\mathbb{Z}/p)[\mu_p \times \mu_p]$.

**Theorem - Anderson**

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

Let $K = \mathbb{Q}(\zeta)$.

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 $L$.

# More on the Galois action on relative 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 unit $B_q \in \Lambda_1$.

Let $\varepsilon_0, \varepsilon_1$ generate $\mu_p \times \mu_p$. Recall $\Lambda_1 = (\mathbb{Z}/p)[\mu_p \times \mu_p]$.
Write $B_q = \sum_{0 \le i,j < p} b_{i,j} \varepsilon_0^i \varepsilon_1^j$ (view as $p \times p$ matrix).

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

(ii) $B_q - 1$ is in the augmentation ideal $(1-\varepsilon_0)(1-\varepsilon_1)\Lambda_1$.
(rows and columns of $B_q - 1$ sum to zero mod $p$).
Observation: Identify $\Lambda_1$ with $H_1(U,Y)$, then $B_q - 1 \in H_1(U)$.

(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 $\Gamma_q$ in $\Omega(\Lambda_0^{sh})$ is represented by the class of $(q-1)\circ[0,1]$ in $H_1(\mathbb{A}^1 - \mu_p^*)$.
In theory, this determines the action of $G_K$ on $H_1(U,Y)$ completely.

# Our program: for all odd primes $p$

Make Anderson's work more explicit,
(1) Determine $Q = \mathrm{Gal}(L/K)$ and (2) Determine formula for $B_q$

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

(3) Main target: $X(K) \to H^1(G_K, M)$ (with restricted ramification)

Quotient of target: kernel of the differential $d_2 : H^1(N, M)^Q \to H^2(Q, M)$ when $N = G_L$ (with restricted ramification).

Main result so far: for all odd $p$, have bounds on $\mathrm{Ker}(d_2)$
(4) lower bound arising from (mod $p$) Heisenberg extensions of $K$.
(5) upper bound arising from $Q$-invariant local units of $\mathcal{O}_L$.

**Application:** If $p = 3$, then $12 \leq \dim(H^1(G_K, M)) \leq 22$.

# (1) The Galois group $Q$ of $L/K$

**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.

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 $C$.

# (1) The Galois group $Q$ of $L/K$

Let $K = \mathbb{Q}(\zeta_p)$. Let $r = (p-1)/2$. Let $L$ be splitting field of $1-(1-x^p)^p$.

## Proposition: $KR^2V$

If Vandiver's Conjecture is true for the prime $p$, then the Galois group $Q$ of $L/K$ is an elementary abelian $p$-group of rank $r+1$.

**Proof:** $L = K(\sqrt[p]{1-\zeta_p^i} : 1 \leq i \leq p-1)$ so $Q$ is elem. abel. $p$-group and $L/K$ ramified only over $\langle 1-\zeta_p \rangle$.

Note $\text{rank} \leq r+1$ because $L/K$ generated by $p$th roots of elements in subgroup $B \subset K^*/(K^*)^p$ generated by $\zeta_p$ 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 $r$.

# (2) The Galois action

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 $B_q \in M$.

Fixed isomorphism $Q \simeq (\mathbb{Z}/p)^{r+1}$ with $q \mapsto (c_0, \ldots, c_r)$.
Let $c = \sum_{i=1}^{p-1} c_i$ and $F$ a root of $F^p - F + c = 0$.
Let $\gamma(\varepsilon) = \sum_{i=1}^{p-1} (\frac{c_i + c - F}{i}) \varepsilon^i - \sum_{i=1}^{p-1} \frac{c_i}{i}$ where $\varepsilon^p = 1$.

Let $\Lambda_0 = \mathbb{Z}/p[\mu_p]$ and $y = \varepsilon - 1$ nilpotent variable since $y^p = 0$.
For $f \in y\Lambda_0$, define $E(f) = \sum_{i=0}^{p-1} f^i / i!$.

## Theorem: $KR^2V$

The action of $q \in Q$ on $H_1(U, Y)$ is determined explicitly by:
$B_q = E(\gamma_q(\varepsilon_0)) E(\gamma_q(\varepsilon_1)) E(-\gamma_q(\varepsilon_0 \varepsilon_1))$.

# (2) 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 $\sqrt[3]{1-\zeta^{-1}}$.

$M = \mathbb{Z}/3[\mu_3 \times \mu_3]$ generated by $\varepsilon_0$ and $\varepsilon_1$

Our formula simplifies to:

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

and

$$B_\tau - 1 = (\varepsilon_0 + \varepsilon_1) - (\varepsilon_0^2 + \varepsilon_0\varepsilon_1 + \varepsilon_1^2) + \varepsilon_0^2\varepsilon_1^2 = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$$

# (2) Example when $p = 5$

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

$$B_\sigma = 2\varepsilon_0^4\varepsilon_1^3 + \varepsilon_0^4\varepsilon_1^2 + 2\varepsilon_0^4\varepsilon_1 + 2\varepsilon_0^3\varepsilon_1^4 + \varepsilon_0^3\varepsilon_1^3 + \varepsilon_0^3\varepsilon_1^2 + \varepsilon_0^3\varepsilon_1 + \varepsilon_0^2\varepsilon_1^4 + \varepsilon_0^2\varepsilon_1^3 + \varepsilon_0^2\varepsilon_1^2 + 2\varepsilon_0^2\varepsilon_1 + 2\varepsilon_0\varepsilon_1^4 + \varepsilon_0\varepsilon_1^3 + 2\varepsilon_0\varepsilon_1^2 + \varepsilon_0\varepsilon_1 + 4\varepsilon_0 + 4\varepsilon_1 + 2.$$

$$B_{\tau_1} = 2\varepsilon_0^4\varepsilon_1^4 + 4\varepsilon_0^4\varepsilon_1^3 + 4\varepsilon_0^4\varepsilon_1 + 4\varepsilon_0^3\varepsilon_1^4 + 3\varepsilon_0^3\varepsilon_1^3 + 3\varepsilon_0^3 + 3\varepsilon_0^2\varepsilon_1^2 + 4\varepsilon_0^2\varepsilon_1 + 3\varepsilon_0^2 + 4\varepsilon_0\varepsilon_1^4 + 4\varepsilon_0\varepsilon_1^2 + 2\varepsilon_0 + 3\varepsilon_1^3 + 3\varepsilon_1^2 + 2\varepsilon_1 + 3$$

$$B_{\tau_2} = 2\varepsilon_0^4\varepsilon_1^4 + \varepsilon_0^4\varepsilon_1^2 + 2\varepsilon_0^4 + 2\varepsilon_0^3\varepsilon_1^3 + \varepsilon_0^3\varepsilon_1^2 + \varepsilon_0^3\varepsilon_1 + \varepsilon_0^3 + \varepsilon_0^2\varepsilon_1^4 + \varepsilon_0^2\varepsilon_1^3 + \varepsilon_0^2\varepsilon_1^2 + 2\varepsilon_0^2 + \varepsilon_0\varepsilon_1^3 + 2\varepsilon_0\varepsilon_1 + 2\varepsilon_0 + 2\varepsilon_1^4 + \varepsilon_1^3 + 2\varepsilon_1^2 + 2\varepsilon_1 + 4.$$

# (2) Important observation about $B_q$

Recall $q \in Q$ acts by multiplication by $B_q$ on $\beta \in H_1(U, Y)$.
If $q \in Q$, let $N_q = \sum_{i=0}^{p-1} (B_q)^i$.

## Proposition: $KR^2\,V$

The norm $N_q = 0$ for all $q \in Q$ except when $p = 3$ and $q$ does not fix $\zeta_9$.

In that case, $N_\sigma = (1 + \varepsilon_0 + \varepsilon_0^2)(1 + \varepsilon_1 + \varepsilon_1^2)$.

More generally, every line in $(\mathbb{Z}/p)^{r+1}$ gives a linear relation between the elements $B_q$ for $q \in Q$.

# (3) 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 $\pi = \pi_1(X_{\bar{K}}, b)$.

Point in $X(K)$ gives splitting of $1 \to \pi \to \pi_{1,\mathrm{ari}}(X_K) \to G_K \to 1$

Let $\kappa : X(K) \to \mathbf{H^1}(\mathbf{G_K}, \pi)$, $\kappa(x) = [\sigma \mapsto \gamma^{-1}\sigma\gamma]$ where $\gamma$ 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.

# (3) Exact sequence for target for rational points

Let $G = G_{K,S}$ is Galois group of maximal extension of $K$ ramified only over $\langle 1 - \zeta \rangle$ and infinite places.

Let $T$ be the set of primes of $L$ above $p$, together with infinite places.

Let $N = G_{L,T}$, Galois group of max. extension of $L$ ramified only over $T$.

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

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

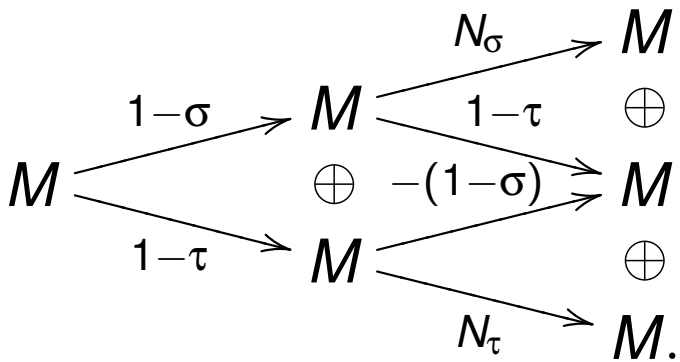
Spectral sequence yields: $0 \to H^1(Q, M) \to \mathbf{H^1(G, M)} \to \mathrm{Ker}(d_2) \to 0$,

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

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




Then $\dim(H^1(Q, M)) = 9$.

For application, need to show $3 \leq \dim(\mathrm{Ker}(d_2)) \leq 13$.

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

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

For us, $Q = \mathrm{Gal}(L/K)$, and $G = G_{K,S}$, and $N = G_{L,T}$.

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

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

Recall the section $s : Q \to G = G_{K,S}$ 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 $a_i, c_{i,j} \in N = G_{L,T}$ since they are in kernel of $G \to Q$.

## Proposition: $KR^2\,V$

We characterize $\mathrm{Ker}(d_2)$ in terms $(\phi(a_i), \phi(c_{i,j})$ being in image of map in a cohomology complex associated with $Q$.

Proof: $\phi \in \mathrm{Ker}(d_2)$ iff $\phi_* w^{\mathrm{ab}} = df$ for some map $f : Q \to M$ of sets.

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 $H_1(U)$).

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

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 $\phi(c) \in H_1(U)$.

# (4) Lower bound: Heisenberg group and 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.
Then $H_p \to H_p/U_p \simeq (\mathbb{Z}/p)^2$.

Two projections $(\mathbb{Z}/p)^2 \to \mathbb{Z}/p$ produce $\iota_1, \iota_2$ in $H^1((\mathbb{Z}/p)^2, \mathbb{Z}/p)$.

The cup product $\iota_1 \cup \iota_2$ in $H^2((\mathbb{Z}/p)^2, \mathbb{Z}/p)$ classifies the extension $1 \to \mathbb{Z}/p \to H_p \to (\mathbb{Z}/p)^2 \to 1$.

## special case of Theorem of Sharifi

Given a field extension $F = K(\sqrt[p]{a}, \sqrt[p]{b})$ of $K$ with $\mathrm{Gal}(F/K) \simeq (\mathbb{Z}/p)^2$, there is a Galois field extension $R/K$ dominating $F/K$ such that $\mathrm{Gal}(R/K) \to \mathrm{Gal}(F/K)$ is isomorphic to $H_p \to (\mathbb{Z}/p)^2$ if and only if $\kappa(a) \cup \kappa(b) = 0$ in $H^2(\mathrm{Gal}_K, \mathbb{Z}/p(2)) \cong H^2(\mathrm{Gal}_K, \mathbb{Z}/p)$.

# (4) lower bound: producing 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 $\mathrm{Gal}(R_l/K) \simeq H_p$.
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 $\tau_i$ act by multiplication by $\zeta_p$.

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

# (4) Lower bound: all 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 $1 \to N \to G_{K,S} \to Q \to 1$, where $N = G_{L,T}$.

Recall $c_{i,j} = [s(\tau_j), s(\tau_i)] \in N$.

## Proposition: $KR^2V$

The order of $\bar{N}$ is $p^r$ where $r = (p-1)/2$
and $\bar{N}$ is generated by the images of $c_{0,j}$ for $1 \leq j \leq r$.

Proof: the image of $c_{0,j}$ in $\mathrm{Gal}(\tilde{R}/L)$ is non-trivial iff $j = l$.

# (4) 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 $B_q$).

**Application:** 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 $3 = \dim(\mathrm{Ker}(\bar{d}_2)) \leq \dim(\mathrm{Ker}(d_2))$.

# (5) Upper bound: Not everything is in $\mathrm{Ker}(d_2)$

## Proposition: $KR^2V$

The codimension of $\mathrm{Ker}(d_2)$ in $H^1(N,M)^Q$ is at least $r=(p-1)/2$.

Elements of $H^1(N,M)^Q$ are $Q$-invariant maps $\phi : N \to M$.
Find $r$-dim space of $Q$-invariant maps $\bar{\phi} : \bar{N} \to M$ not in $\mathrm{Ker}(d_2)$.

$Q$-invariant iff $m_j = \bar{\phi}(\bar{c}_{0,j}) \in M^Q$ (fixed by mult. by $B_q$ for all $q \in Q$).

Earlier proposition: If $m_j \notin H_1(U)$ for any $j$, then $\bar{\phi}$ not in $\mathrm{Ker}(d_2)$.

The element $m = \sum_{i=0}^{p-1} \varepsilon_0^i$ is in $M^Q$ but not in $H_1(U)$.

For application, need to show $\dim(H^1(N,M)^Q) \leq 14$.

# (5) Upper bound - alternative description of $\mathrm{Ker}(d_2)$

Since $N = G_{L,T}$ acts trivially on $M$, then $H^1(N, M) \cong H^1(N, \mathbb{F}_p) \otimes M$.

Koch: there is an exact sequence of $Q$-modules
$0 \to H^1(N, \mathbb{F}_p) \to (O_{p_L}^*/p)^* \xrightarrow{\varphi_2^*} (O_L^*/p)^*$.

We have found a good description of local and global units mod $p$.

## Proposition: $KR^2\,V$

Let $r = (p-1)/2$. Then $H^1(N, \mathbb{F}_p)$ is the kernel of a linear map $(\mathbb{Z}/p)^{1+(p-1)p^{r+1}} \to (\mathbb{Z}/p)^{\frac{1}{2}(p-1)p^{r+1}}$.

Note, $\dim((H^1(N, \mathbb{F}_p) \otimes M)^Q) \leq (1 + (p-1)p^{r+1})\dim(M^Q)$. Way too big!

Currently, looking at $Q$-invariants of $H^1(N, \mathbb{F}_p) \otimes M$.

**Ex:** If $p = 3$, then $\dim(H^1(N, M)^Q) = 14$, finishing the upper bound!