CYCLIC STICKELBERGER COHOMOLOGY AND DESCENT OF KUMMER EXTENSIONS

LINDSAY N. CHILDS

Abstract. Let \( R \) be a field, \( S = R[\xi] \), \( \xi \) an \( n \)th root of unit, \( \Delta = \text{Gal}(S/R) \). The group of cyclic Kummer extensions of \( S \) on which \( \Delta \) acts, modulo those which descend to \( R \), is isomorphic to a group of roots of unity and to a second group cohomology group of \( \Delta \) whose definition involves a “Stickelberger element”.

Let \( R \) be a field, \( p \) an odd prime, \( n = p^r \), \( S \) the field obtained from \( R \) by adjoining a primitive \( n \)th root of unity to \( R \), \( \Delta = \text{Gal}(S/R) \). Every Galois extension \( T \) of \( S \) with group \( G \), cyclic of order \( n \) (in the sense of Chase, Harrison and Rosenberg [1]), is a Kummer extension. We consider when such a \( T \) descends to \( R \), that is, \( T = S \otimes_R T_0 \) for some Galois extension \( T_0 \) of \( R \). A necessary condition is that \( T \) be \( \Delta \)-normal, that is, \( \Delta \) extends to a set of \( R \)-algebra, \( G \)-module automorphisms of \( T \). We identify the group of \( \Delta \)-normal Galois extensions of \( S \) modulo those which descend with a certain twisted cyclic second cohomology group whose definition involves a formal analogue of the Stickelberger element in cyclotomic field theory. If \( n = p \), then \( \Delta \)-normal Galois extensions descend and the cohomology group vanishes. In general, the cohomology group is isomorphic to a certain group of roots of unity; hence if \( T \) is \( \Delta \)-normal, then there is a Kummer extension \( U = S[z] \), \( z^n \) an \( n \)th root of unity, so that the Harrison product \( T \cdot U \) descends.

Throughout the paper, \( G \) is a cyclic group of order \( n = p^r \), and \( \Delta \) is a cyclic group of order \( m \).

1. Cyclic Stickelberger cohomology. Let \( \Delta \) be cyclic of order \( m \), generated by \( \omega \), \( A \) a \( \Delta \)-module written multiplicatively. Then, as is well known, the usual group cohomology \( H^n(\Delta, A) \), \( n > 0 \), may be computed as the homology of the sequence

\[
\rightarrow A \rightarrow A \rightarrow A \rightarrow A \rightarrow
\]

where \( T \) is the map which raises to the \( \omega - 1 \) power,

\[
a^T = a^{\omega - 1} = a^{\omega a^{-1}},
\]

and \( N \) is the map which raises to the power \( \Sigma_{i=1}^n \omega^i \).

Now suppose \( A \) is \( n \)-torsion, \( a^n = 1 \) for all \( a \) in \( A \), and let \( t: \Delta \rightarrow (\mathbb{Z}/n\mathbb{Z})^* \) be a homomorphism. (By abuse of notation, we will view \( t(\delta) \), \( \delta \in \Delta \), as an integer.) Then we may define a \( t \)-twisted action of \( \Delta \) on \( A \), namely for \( a \in A \), \( \delta \in \Delta \), \( \delta \ast a = t(\delta)^{-1}(\delta(a)) \). Since \( t \) is a homomorphism and \( A \) is \( n \)-torsion, this action is well
defined. Thus $A$ becomes a $\Lambda$-module via this twisted action, call it $A_t$, and we define the Stickelberger cohomology $H^i_t(\Lambda, A)$ by $H^i_t(\Lambda, A) = H^i(\Lambda, A_t)$ for $i \geq 0$. (Extending to all $i$ to get the Tate groups is clear.)

We call $H^i_t(\Lambda, A)$ the $i$th Stickelberger cohomology because if we set $\tau(a) = T \ast_a$, $\eta(a) = N \ast a$ for $a \in A$, then $\eta(a)$ is a acted on by $\theta = \sum_{\delta \in \Delta} \delta^{-1}t(\delta)$, a formal analogue of the classical Stickelberger element in cyclotomic field theory.

In particular, $H^2_t(\Lambda, A) = \text{Ker } \tau/\text{Im } \eta$, where $\text{Ker } \tau = \{a \in A \mid a^\delta = a^{t(\delta)} \text{ for all } \delta \in \Delta\}$, the $t$-eigenspace of $A$, and so $H^2_t(\Lambda, A)$ may be viewed as a measure of the failure of the Stickelberger element $\theta$ to project onto the $t$-eigenspace of $A$.

Since $H^i_t(\Lambda, A)$ may be viewed as ordinary group cohomology,

$$\text{(1.1) } H^i_t(\Lambda, A) = 0 \text{ whenever } \Lambda \text{ and } A \text{ have relatively prime orders, e.g. whenever } m \text{ and } n \text{ are relatively prime.}$$

One objective of this paper is to describe a situation where $H^2(\Lambda, A) \neq 0$.

An alternative approach to a kind of Stickelberger cohomology may be found in [5].

2. We will need the following lemma of elementary number theory, which should be well known, but for which we know no convenient reference.

**Lemma 2.1.** Let $r \geq 2$ and $e$ have order $m$ mod $p^r$, where $p$ is an odd prime dividing $m$. Then $e$ has order $mp$ mod $p^{r+1}$. Hence $(e^m - 1)/p^r$ is relatively prime to $p$.

**Proof.** $(\mathbb{Z}/p^r\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z})^* \times P_r$ via $e \rightarrow (e^{p-1}, e^{p-1})$, where $P_r$ is cyclic of order $p^{r-1}$. The “take the class mod $p^r$” map from $(\mathbb{Z}/p^r\mathbb{Z})^*$ to $(\mathbb{Z}/p\mathbb{Z})^*$ induces the same map from $P_{r+1}$ onto $P_r$ whose kernel is the unique subgroup of $P_{r+1}$ of order $p$, and induces an isomorphism on $(\mathbb{Z}/p\mathbb{Z})^*$. Suppose $e$ has order $m$ mod $p^r$, $p$ dividing $m$. Then $e^{p-1}$ is nontrivial in $P_r$, hence also in $P_{r+1}$. If, in $P_{r+1}$, $e^{p-1}$ has order $p^c$, some $c \geq 1$, then $(e^{p-1})^{p^c}$ has order $p$, and so is in ker$(P_{r+1} \rightarrow P_r)$. Hence $e^{p-1}$ has order $p^{r-1}$ in $P_r$. Thus the order of $e$ mod $p^{r+1}$ is $p$ times the order of $e$ mod $p^r$.

(Note that the lemma may fail when $r = 1 : 2$ has order $p - 1$ mod $p^2$ when $p = 1093$ or 3511. The statement of the lemma for $r = 1$ relates to the Wieferich-Miramanoff criteria for the first case of Fermat's Last Theorem. (See [7].))

3. Descent of Kummer extensions. Let $p$ be an odd prime, and $G$ a cyclic group of order $n = p^r$ generated by $\sigma$. Let $R$ be a field of characteristic $> p$, and $\mu_n$ the group of $n$th roots of unity in some algebraic closure of $R$ generated by $\xi$. Let $S = R[\xi]$, and $\Delta = \text{Gal}(S/R)$ of order $m$.

Let $t: \Delta \rightarrow \mathbb{Z}$ be defined by $t(\delta) = \xi^\delta$ for $\delta \in \Delta$, $1 \leq t(\delta) < n$. Then $t$ induces an injection, also called $t$, from $\Delta$ to $(\mathbb{Z}/n\mathbb{Z})^*$.

Let $\text{Gal}(R, G)$ be the Harrison [6] group of isomorphism classes (as $R$-algebras and $RG$-modules) of Galois extensions of $R$ with group $G$. Then, as is well known, $\text{Gal}(S, G)$ consists of Kummer extensions, and $\text{Gal}(S, G) \cong U(S)/U(S)^\sigma$ as follows: with $\xi$ and $\sigma$ fixed as above, let $s \in U(S)$, set $T = S[z]$ with $z^n = s$, $z^\sigma = \xi z$; then $T$ is a Galois extension of $S$ with group $G$. Conversely, given a Galois extension $T$ of $S$, let $T_z = \{x \in T \mid x^\sigma = \xi x\}$, then $T_z = Sz$ for some invertible $z$ in $T$, and...
$z^n = s \in U(S)$ yields the corresponding class in $U(S)/U(S)^n$. Note that $\{x \in T \mid x^n = \xi^h x\} = Sx^h$ for any $h$.

Define $\text{Gal}_A(S, G)$ to be the set of $S$-algebra, $G$-module isomorphism classes of Galois extensions of $S$ with group $G$ which have representatives $T$ on which $\Delta$ lifts to a set of $G$-module automorphisms. $\text{Gal}_A(S, G)$ may be viewed as an analogue of the nomal Azumaya algebras studied in [4 and 3], so we call $\text{Gal}_A(S, G)$ the group of $\Delta$-normal Galois extensions.

Let $j: \text{Gal}(\bar{R}, G) \to \text{Gal}(S, G)$ be the homomorphism induced by sending a Galois extension $U$ of $R$ to $U \otimes_R S$. Clearly, $\text{Im}(j) \subset \text{Gal}_A(S, G)$ and is the group of Galois extensions of $S$ which descend. We prove

**Theorem 3.1.** $\text{Gal}_A(S, G)/\text{Im}(j) \cong \mu_n/\mu_n^m$.

**Proof.** Let $T = S[z]$ be a Kummer extension with group $G$, where $z^n = s$. Then $s$ is defined up to an $n$th power. Suppose $T$ is $\Delta$-normal, so that $\omega \in \Delta$ lifts to an automorphism of $T$. Since $\Delta$ commutes with $G$, $(z^\omega)^s = (z^s)^\omega = \xi^s(z^\omega)$, so $z^\omega = c_\omega z^{(s^\omega)}$ for some $c \in S$, so $s^\omega = s^{(s^\omega)c_\omega}$. Let $\omega = t(\omega)$. By iterating $\omega$, one easily checks that $z^\omega = z^{c^\kappa}$ where $\kappa = \sum_{k=0}^{m-1} \omega^{m-k} c^k$. Define $\gamma$ by $\gamma = s^{(s^{-1})/n} c^\kappa$. Then $\gamma$ is an $n$th root of unity. For, since $z^\omega = z^{c^\kappa}$, $s^\omega = s^{e^\kappa}$. Since $\omega$ has order $m$ in $S$, $s^\omega = s$, so $1 = s^{e^\kappa} c^\kappa = \gamma^n$.

We induce a map $\varphi$ from $\text{Gal}_A(S, G)$ to $\mu_n/\mu_n^m$ by associating $T$ to $\gamma$.

We show that $\varphi$ is well defined. First, given $s$, $c$ is defined only up to an $n$th root of unity. Multiplying $c$ by $\xi$, an $n$th root of unity, multiplies $\gamma$ by $\xi^n = \xi^m$. So the map $s \to \gamma$ is well defined.

To show that the map $s \to \gamma$ yields a well-defined map $\varphi$ on $\text{Gal}_A(S, G)$, we replace $s$ by $st^\omega$ for $t \in S$. Then $(st^\omega)^s = (st^\omega)^t(c t^{\omega-e})^n$, so $c$ is replaced by $ct^{\omega-e}$, and $\gamma$ by

$$(st^\omega)^n c(t^{\omega-e})\gamma = \gamma(t^\omega)^n c(t^{\omega-e})\gamma.$$  

But

$$(\omega - e)\gamma = (\omega - e) \sum_{k=0}^{m-1} e^k \omega^{m-k} = (\omega^m - e^m) \omega;$$

hence, since $\omega$ has order $m$ on $S$,$$(t^\omega)^n c(t^{\omega-e})\gamma = t^{\omega(e^m-1)} t^{\omega(\omega^m-e^m)} = 1.$$Thus $\varphi$ is a well-defined map from $\text{Gal}_A(S, G)$ to $\mu_n/\mu_n^m$.

To show $\varphi$ is a homomorphism observe that if $s, r$ are in $U(S)$ with $s^\omega = s^e c^{n\omega}$, $r^\omega = r^e d^{n\omega}$, then $(sr)^\omega = (sr)^t(c d)^n\omega$, so the image of $sr$ is

$$\gamma_{sr} = (sr)^t c^{n-1} c^n = \gamma_s \gamma_r.$$Ontoness of $\varphi$ is trivial if $p$ does not divide $m$. If $p$ divides $m$, let $s$ be a primitive $n$th root of unity. Then $s^\omega = s^e c^{n\omega}$ for $c = 1$, and $\gamma = s^{(s^{-1})/n}$ is again a primitive $n$th root of unity by Lemma 2.1. So the image of $s$ is a primitive $n$th root of unity. Hence $\varphi$ is onto.

Finally, we show that $\ker \varphi = \text{Im}(j)$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
A Galois extension $T$ of $S$ is the image of a Galois extension $U$ of $R$ iff $T \cong S \otimes_R U$. In that case, $T$ is a Galois extension of $R$ with group $\Delta \times G$; thus $\Delta$ and $G$ are commuting groups of automorphisms of $T$. Conversely, if $\Delta$ lifts to a group of automorphisms of $T$ commuting with $G$, then by the theorem of natural irrationality, $T$ is a Galois extension of $R$ with group $G$ and $S \otimes_R T^\Delta \cong T$.

Therefore, since $\Delta = \langle \omega \rangle$ is cyclic of order $m$, $T$ descends to $R$ iff $\omega$ lifts to an automorphism of $T$, commuting with $G$, of order $m$.

Now $\omega$ has order $m$ on $T$ iff $z^m = z$, that is, $z^{m-1} \cdot e^m = e^x$, or $z^{m-1}c^x = 1$. Here $m$ is the order of $e$ mod $m$, since the homomorphism $\iota: \Delta \to (\mathbb{Z}/n\mathbb{Z})^*$ is 1-1. Thus, in particular, $n$ divides $e_m - 1$, and $\omega$ has order $m$ on $T$ iff

$$1 = z^{e_m - 1}c^x = (z^n)^{(e_m - 1)/n}c^x = s^{(e_m - 1)/n}c^x = \gamma.$$  

That completes the proof.

**Corollary 3.2.** Let $p$ divide $m$, and let $T$ be a $\Delta$-normal Galois extension of $S$. Then there exists a Galois extension $U$ of $S$ with group $G$, $U = S[\omega]$, $\omega^n = \xi$, an $n$th root of unity, such that $T \cdot U$ descends to $R$.

**Proof.** Let $T = S[z]$, $z^n = s$, let $\gamma_s = \xi^{(e_m - 1)/n}$ for some $n$th root of unity $\xi$. Let $U = S[w]$ with $w^n = \xi^{-1}$. Then under the correspondence between $\text{Gal}(S, G)$ and $U(S)/U(S)^n$ of $T \cdot U$ corresponds to the class of $\xi^{-1}$, and by the proof of ontoness of $\varphi$ above, $\varphi(U)$ is the class of $\xi^{-(e_m - 1)/n}$. Hence $\varphi(T \cdot U) = 1$ and $T \cdot U$ descends.

**Corollary 3.3.** If $m$ is prime to $p$ and $T$ is a $\Delta$-normal Galois extension of $S$, then $T$ descends to $R$,

for $\mu_m = \mu_n$, hence $\varphi$ is trivial.

Now we relate the question of descent to Stickelberger cohomology.

**Theorem 3.4.** $\text{Gal}_A(S, G)/\text{Im}(\iota) \cong H^2(\Delta, U(S)/U(S)^n)$.

**Proof.** We first show $\text{Gal}_A(S, G) \cong \ker \tau$. Let $T$ be a Kummer extension, $T = S[z]$, $z^n = s$, $z^\sigma = \xi z$. Suppose $\omega$ lifts to a $G$-module automorphism of $T$. Then

$$(z^\omega)^\sigma = (z^\sigma)^\omega = (\xi z)^\omega = \xi^{t(\omega)}z^\omega.$$  

Since

$$\{t \in T \mid t^\sigma = \xi^{t(\omega)}t\} = Sz^{t(\omega)},$$

therefore $z^\omega = z^{t(\omega)}c^\omega$ for some $c$ in $S$, hence $s^{(e_m - 1)/n}c^\omega = c^\omega n$ in $U(S)^n$. Thus $s^{\omega - t(\omega)}$ is trivial in $U(S)/U(S)^n$.

Conversely, if $s^{\omega - t(\omega)}$ is in $U(S)^n$, let $T = S[z]$, $z^n = s$ and define $\omega$ on $T$ by $z^\omega = z^{t(\omega)}c^\omega$. Since $(t(\omega), n) = 1$ and $s, c$ are in $U(S)$, this defines an automorphism $\omega$ of $T$ which commutes with $G$, so $T$ is $\Delta$-normal.

Now we show $\text{Im}(\iota) \cong \text{Im}(\eta)$. By (1.1) and Theorem 3.1 this follows immediately if $p$ does not divide $m$. So assume $p$ divides $m$.

First suppose $T$ descends.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Mod $U(S)^n$, $c^\kappa = c^\vartheta$, where
\[ \vartheta = \sum_{k=0}^{m-1} \omega^{-k} t(\omega^k) = \sum_{\delta \in \Delta} \delta^{-1} t(\delta). \]

Hence, if $\omega$ has order $m$ on $T$ and $t(\omega) = e$, then
\[ s^{(e^{m-1})/n} c^\vartheta \equiv 1 \pmod{U(S)^n}. \]

Since $\vartheta$ divides $m$, we know, by Lemma 2.1, that $(e^{m-1})/n$ is relatively prime to $n$. Thus, if $(e^{m-1})/n h \equiv 1 \pmod{n}$, then $s \equiv (c^\vartheta)^h \pmod{U(S)^n}$.

Conversely, suppose $s$ represents a class in $\text{Im} \eta$. Then $s \equiv d^\vartheta \pmod{U(S)^n}$; altering $s$ by $n$th powers as needed, we may assume $s = d^\kappa$ for some $d$ in $U(S)$, where $\kappa = \sum_{i=0}^{m-1} \omega^{m-i} e^i$. Then,
\[ s^{\omega^m - e} = d^\kappa (\omega - e) = d^{\omega^m - e^m} = \left( d^{(1-e^m)/n} \right)^n \]
since $\omega$ has order $m$ on $S$. Hence, $c = d^{(1-e^m)/n} = \xi$ for some $n$th root of unity.

But then $\gamma = s^{(e^{m-1})/n} c^\kappa$, and, substituting for $s$ and $c$,
\[ \gamma = d^{(e^{m-1})/n} d^{(1-e^m)/n} \xi \equiv \xi^e \in \mu_n^m. \]

By Theorem 3.1, $T$ descends, completing the proof of Theorem 3.4.

Our computation of the Stickelberger 2-cohomology yields the following result, which may be of some arithmetic interest.

**Corollary 3.5.** Given an $n$th root of unity $\xi$ in $S$, the equation $\xi \equiv d^\vartheta \pmod{U(S)^n}$ may be solved for $d$ in $S$ iff $\xi^{n/(m,n)} = 1$.

For if $\vartheta$ divides $m$ (the only nontrivial case), the map from $H^2_2(\Delta, U(S)/U(S)^n)$ to $\mu_n/\mu_n^n$ maps the class of $s$ mod $U(S)^n$ to $\gamma_s$. If $s = \xi$, an $n$th root of unity, then $\gamma_s = \xi^{(e^{m-1})/n}$. Since $(e^m - 1)/n$ is prime to $n$, then $\gamma_s$ is trivial, i.e. $\xi$ is in $\text{Im} \eta$, iff $\xi$ is in $\mu_n/(m,n)$.

**Remark.** The map $j$ from $\text{Gal}(R, G)$ to $\text{Gal}(S, G)$ and its kernel has been studied from a cohomological viewpoint by Chase and Rosenberg [2]. The referee has kindly pointed out that Theorem 3.1 may also be viewed, in part, cohomologically. Namely, the spectral sequence
\[ H^p(\Delta, \text{Ext}^q_Z(\mu_n, U(S))) \rightarrow \text{Ext}^q_Z(\mu_n, U(S)) \]
[9, p. 351] yields an exact sequence of low degree:
\[ \cdots \text{Ext}^1_Z(\mu_n, U(S)) \rightarrow H^0(\Delta, \text{Ext}^1_Z(\mu_n, U(S))) \rightarrow H^2(\Delta, \text{Hom}_Z(\mu_n, U(S))) \rightarrow \cdots. \]

Now $\text{Hom}_Z(\mu_n, U(S))$ may be identified with $Z/nZ$ (with trivial action), and, for $\Delta$ cyclic of order $n$, $H^2(\Delta, Z/nZ) \cong \mu_n/\mu_n^n$. On the other hand, from [8, Corollary 17.19, p. 126] we may identify $\text{Ext}^1_Z(\mu_n, U(S))$ and $H^0(\Delta, \text{Ext}^1_Z(\mu_n, U(S)))$ with $\text{Gal}(R, Z/nZ)$ and $\text{Gal}^1(S, Z/nZ)$, respectively. Thus the map $\varphi: \text{Gal}^1(S, G)/\text{Im}(j) \rightarrow \mu_n/\mu_n^n$ may be viewed as a realization of the sequence (3.6).
REFERENCES


DEPARTMENT OF MATHEMATICS AND STATISTICS, STATE UNIVERSITY OF NEW YORK, ALBANY, NEW YORK 12222