PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 90, Number 4, April 1984

CYCLIC STICKELBERGER COHOMOLOGY AND DESCENT OF KUMMER EXTENSIONS

LINDSAY N. CHILDS

ABSTRACT. Let R be a field, $S = R[\zeta]$, ζ an nth root of unit, $\Delta = \mathrm{Gal}(S/R)$. The group of cyclic Kummer extensions of S on which Δ acts, modulo those which descend to R, is isomorphic to a group of roots of unity and to a second group cohomology group of Δ 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 nth root of unity to R, $\Delta = \mathrm{Gal}(S/R)$. 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 Δ-normal, that is, Δ extends to a set of R-algebra, G-module automorphisms of T. We identify the group of Δ-normal Galois extensions of S modulo those which descend with a certain twisted cyclic second cohomolgy group whose definition involves a formal analogue of the Stickelberger element in cyclotomic field theory. If $n = p$, then Δ-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 Δ-normal, then there is a Kummer extension $U = S[z]$, z^n an nth 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 Δ is a cyclic group of order m.

1. Cyclic Stickelberger cohomology. Let Δ be cyclic of order m, generated by ω, A a Δ-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

$$\to A \xrightarrow{T} A \xrightarrow{N} A \xrightarrow{T} A \xrightarrow{N} \to$$

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 $\sum_{i=1}^{n} \omega^i$.

Now suppose A is n-torsion, $a^n = 1$ for all a in A, and let $t\colon \Delta \to (\mathbf{Z}/n\mathbf{Z})^*$ 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 Δ on A, namely for $a \in A$, $\delta \in \Delta$, $\delta * a = t(\delta)^{-1}\delta(a)$. Since t is a homomorphism and A is n-torsion, this action is well

Received by the editors April 7, 1983 and, in revised form, July 8, 1983.
1980 *Mathematics Subject Classification.* Primary 13B05.

0002-9939/84 $1.00 + $.25 per page

defined. Thus A becomes a $\mathbf{Z}\Delta$-module via this twisted action, call it A_t, and we define the Stickelberger cohomology $H_t^i(\Delta, A)$ by $H_t^i(\Delta, A) = H^i(\Delta, A_t)$ for $i \geqslant 0$. (Extending to all i to get the Tate groups is clear.)

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

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

Since $H_t^i(\Delta, A)$ may be viewed as ordinary group cohomology,

(1.1) $H_t^i(\Delta, A) = 0$ whenever Δ and A have relatively prime orders, e.g. whenever m and n are relatively prime.

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

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

PROOF. $(\mathbf{Z}/p^s\mathbf{Z})^* \cong (\mathbf{Z}/p\mathbf{Z})^* \times P_s$ via $e \to (e^{p^{s-1}}, e^{p-1})$, where P_s is cyclic of order p^{s-1}. The "take the class mod p^r" map from $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$ to $(\mathbf{Z}/p^r\mathbf{Z})^*$ 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 $(\mathbf{Z}/p\mathbf{Z})^*$. Suppose e has order $m \bmod p^r$, 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 $c \geqslant 1$, then $(e^{p-1})^{p^{c-1}}$ has order p, and so is in $\ker(P_{r+1} \to P_r)$. Hence e^{p-1} has order p^{c-1} in P_r. Thus the order of $e \bmod p^{r+1}$ is p times the order of $e \bmod p^r$.

(Note that the lemma may fail when $r = 1:2$ has order $p - 1 \bmod p^2$ 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 σ. Let R be a field of characteristic $> p$, and $\mu_n =$ the group of nth roots of unity in some algebraic closure of R generated by ζ. Let $S = R[\zeta]$, and $\Delta = \operatorname{Gal}(S/R)$ of order m.

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

Let $\operatorname{Gal}(R, G)$ 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, $\operatorname{Gal}(S, G)$ consists of Kummer extensions, and $\operatorname{Gal}(S, G) \cong U(S)/U(S)^n$ as follows: with ζ and σ fixed as above, let $s \in U(S)$, set $T = S[z]$ with $z^n = s$, $z^\sigma = \zeta z$; then T is a Galois extension of S with group G. Conversely, given a Galois extension T of S, let $T_\zeta = \{x \in T \mid x^\sigma = \zeta x\}$, then $T_\zeta = Sz$ 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 $\{x \in T \mid x^\sigma = \zeta^h x\} = Sz^h$ for any h.

Define $\mathrm{Gal}_\Delta(S, G)$ 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 Δ lifts to a *set* of G-module automorphisms. $\mathrm{Gal}_\Delta(S, G)$ may be viewed as an analogue of the nomal Azumaya algebras studied in [**4** and **3**], so we call $\mathrm{Gal}_\Delta(S, G)$ the group of Δ-normal Galois extensions.

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

THEOREM 3.1. $\mathrm{Gal}_\Delta(S, G)/\mathrm{Im}(j) \cong \mu_n/\mu_n^m$.

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

We induce a map φ from $\mathrm{Gal}_\Delta(S, G)$ to μ_n/μ_n^m by associating T to γ.

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

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

$$(st^{\omega n})^{(e^m-1)/n} (ct^{\omega-e})^\kappa = \gamma (t^{\omega n})^{(e^m-1)/n} (t^{\omega-e})^\kappa.$$

But

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

hence, since ω has order m on S,

$$(t^{\omega n})^{(e^m-1)/n} t^{(\omega-e)\kappa} = t^{\omega(e^m-1)} t^{\omega(\omega^m - e^m)} = 1.$$

Thus φ is a well-defined map from $\mathrm{Gal}_\Delta(S, G)$ to μ_n/μ_n^m.

To show φ 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 $(sr)^\omega = (sr)^e (cd)^{n\omega}$, so the image of sr is

$$\gamma_{sr} = (sr)^{(e^m-1)/n} (cd)^\kappa = \gamma_s \gamma_r.$$

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

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

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 Δ and G are commuting groups of automorphisms of T. Conversely, if Δ 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 ω lifts to an automorphism of T, commuting with G, of order m.

Now ω has order m on T iff $z^{\omega^m} = z$, that is, $z^{1-e^m} = c^{\kappa}$, or $z^{e^m-1}c^{\kappa} = 1$. Here m is the order of $e \bmod m$, since the homomorphism $t\colon \Delta \to (\mathbf{Z}/n\mathbf{Z})^*$ is 1-1. Thus, in particular, n divides $e^m - 1$, and ω has order m on T iff

$$1 = z^{e^m-1}c^{\kappa} = (z^n)^{(e^m-1)/n}c^{\kappa} = s^{(e^m-1)/n}c^{\kappa} = \gamma.$$

That completes the proof.

COROLLARY 3.2. *Let p divide m, and let T be a Δ-normal Galois extension of S. Then there exists a Galois extension U of S with group G, $U = S[w]$, $w^n = \xi$, an nth 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 nth root of unity ξ. Let $U = S[w]$ with $w^n = \xi^{-1}$. Then under the correspondence between $\mathrm{Gal}(S, G)$ and $U(S)/U(S)^n$, $T \cdot U$ corresponds to the class of $s\xi^{-1}$, and by the proof of ontoness of φ 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 Δ-normal Galois extension of S, then T descends to R,*

for $\mu_n^m = \mu_n$, hence φ is trivial.

Now we relate the question of descent to Stickelberger cohomology.

THEOREM 3.4. $\mathrm{Gal}_{\Delta}(S, G)/\mathrm{Im}(j) \cong H_t^2(\Delta, U(S)/U(S)^n)$.

PROOF. We first show $\mathrm{Gal}_{\Delta}(S, G) \cong \ker \tau$. Let T be a Kummer extension, $T = S[z]$, $z^n = s$, $z^{\sigma} = \zeta z$. Suppose ω lifts to a G-module automorphism of T. Then

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

Since

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

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

Conversely, if $s^{\omega - t(\omega)} = c^{\omega n}$ is in $U(S)^n$, let $T = S[z]$, $z^n = s$ and define ω 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 ω of T which commutes with G, so T is Δ-normal.

Now we show $\mathrm{Im}(j) \cong \mathrm{Im}(\eta)$. 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.

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 ω has order m on T and $t(\omega) = e$, then

$$s^{(e^m-1)/n} c^\vartheta \equiv 1 \pmod{U(S)^n}.$$

Since p 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 $s \equiv (c^{-h})^\vartheta \pmod{U(S)^n}$.

Conversely, suppose s represents a class in $\operatorname{Im}\eta$. Then $s \equiv d^\vartheta \pmod{U(S)^n}$; altering s by nth 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,

$$s^{\omega - e} = d^{\kappa(\omega - e)} = d^{\omega(\omega^m - e^m)} = \left(d^{\omega(1-e^m)/n}\right)^n$$

since ω has order m on S. Hence, $c = d^{(1-e^m)/n}\xi$ for ξ some nth root of unity.

But then $\gamma = s^{(e^m-1)/n} c^\kappa$, and, substituting for s and c,

$$\gamma = d^{\kappa(e^m-1)/n} d^{((1-e^m)/n)\kappa} = \xi^\kappa \in \mu_n^m.$$

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 nth root of unity ξ 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 p divides m (the only nontrivial case), the map from $H_t^2(\Delta, U(S)/U(S)^n)$ to μ_n/μ_n^m maps the class of $s \bmod U(S)^n$ to γ_s. If $s = \xi$, an nth root of unity, then $\gamma_\xi = \xi^{(e^m-1)/n}$. Since $(e^m - 1)/n$ is prime to n, then γ_ξ is trivial, i.e. ξ is in $\operatorname{Im}\eta$, iff ξ is in $\mu_n^m = \mu_{n/(m,n)}$.

REMARK. The map j from $\operatorname{Gal}(R, G)$ to $\operatorname{Gal}(S, G)$ 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

$$H^p\left(\Delta, \operatorname{Ext}_{\mathbf{Z}}^q(\mu_n, U(S))\right) \overset{p}{\Rightarrow} \operatorname{Ext}_{\mathbf{Z}\Delta}^{p+q}(\mu_n, U(S))$$

[**9**, p. 351] yields an exact sequence of low degree:

$$\begin{aligned}(3.6)\qquad \cdots \operatorname{Ext}_{\mathbf{Z}\Delta}^1(\mu_n, U(S)) &\to H^0\left(\Delta, \operatorname{Ext}_{\mathbf{Z}}^1(\mu_n, U(S))\right) \\ &\to H^2\left(\Delta, \operatorname{Hom}_{\mathbf{Z}}(\mu_n, U(S))\right) \cdots.\end{aligned}$$

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

REFERENCES

1. S. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), pp. 15–33.

2. S. Chase and A. Rosenberg, *A theorem of Harrison, Kummer theory and Galois algebras*, Nagoya Math. J. **27** (1966), 663–685.

3. L. Childs, *Normal algebras and the Teichmüller cocycle map*, J. Algebra **23** (1972), 1–17.

4. S. Eilenberg and S. Mac Lane, *Normality of algebras and the Teichmüller cocycle map*, Trans. Amer. Math. Soc. **64** (1948), 1–20.

5. A. Frohlich, *Stickelberger without Gauss sums*, Algebraic Number Fields (A. Frohlich, ed.), Academic Press, New York, 1977, pp. 589–608.

6. D. K. Harrison, *Abelian extensions of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), pp. 1–14.

7. P. Ribenboim, 13 *lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

8. S. Chase, *Galois objects and extensions of Hopf algebras*, Lecture Notes in Math., vol. 97, Springer-Verlag, New York, 1969.

9. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, N.J., 1956.

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