Can. J. Math., Vol. XXXIV, No. 3, 1982, pp. 686–690

A STICKELBERGER CONDITION ON CYCLIC GALOIS EXTENSIONS

L. N. CHILDS

Let R be a commutative ring, C a finite abelian group, S a Galois extension of R with group C, in the sense of [**1**]. Viewing S as an RC-module defines the Picard invariant map [**4**] from the Harrison group Gal (R, C) of isomorphism classes of Galois extensions of R with group C to Cl (RC), the class group of RC. The image of the Picard invariant map is known to be contained in the subgroup h Cl (RC) of primitive elements of Cl (RC) (for definition see below). Characterizing the image of the Picard invariant map has been of some interest, for the image describes the extent of failure of Galois extensions to have normal bases.

Let R be the ring of integers of an algebraic number field K. If S is the ring of integers of a tame(ly ramified) Galois extension L of K with group C, then viewing S as an RC-module yields a class in Cl (RC). The image of this map is of interest for the same reason. L. McCulloh [**8**] showed that in case C has prime order l and K contains a primitive lth root of unity, then the image consists of elements of Cl (RC) which are in the kernel Cl^0 (RC) of the map induced by the trivial character on C and which are in the subgroup Cl^0 $(RC)^J$ generated by the images of elements of Cl^0 (RC) under action by elements of the Stickelberger ideal J of $\mathbf{Z}$ (Aut C).

The two questions concerning the images should be related, for in the number field case, connected Galois extensions of R are rings of integers of unramified, hence tame extensions of K [**1**, 1.5(d)]. The purpose of this note is to show that for any commutative ring R and for C cyclic of odd prime power order l^n, primitive elements of Cl (RC) lie in Cl^0 $(RC)^J$.

It follows that Galois extensions of R with group C yield classes which are products of images of Stickelberger elements. Concerning the corresponding result for tame extensions, only McCulloh's result [**8**] is known.

Stickelberger conditions. Let l be an odd prime, C the cyclic group of order l^n, G = Aut (C). Then $G \simeq (\mathbf{Z}/l^n\mathbf{Z})^*$ via the map which sends δ in G to the class of the integer $t(\delta)$, $0 < t(\delta) < l^n$, $(t(\delta), l) = 1$, such that $\delta(\sigma) = \sigma^{t(\delta)}$ for all σ in C. The inverse isomorphism is given by sending the class of the integer a, $(a, l) = 1$ to δ_a, where $\delta_a(\sigma) = \sigma^a$ for σ in C.

Received October 26, 1980 and in revised form March 10, 1981. This work was partially supported by N.S.F. Grant MCS7902106.

In QG is the Stickelberger element

$$\theta = \sum_{a \in (\mathbf{Z}/l^n\mathbf{Z})^*} \left\langle \frac{a}{l^n} \right\rangle \delta_a^{-1} = \frac{1}{l^n} \sum_{\delta \in G} t(\delta)\delta^{-1}$$

where $\langle \ \rangle$ denotes fractional part. The Stickelberger ideal J of $\mathbf{Z}G$ is defined as $J = \mathbf{Z}G \cap \mathbf{Z}G\theta$. The ideal J has been the object of considerable interest in cyclotomic field theory and Galois module theory in recent years; see, for example, [**5**], [**6**] or [**7**, page 12].

The ideal J has a convenient alternate description.

PROPOSITION 1 (Iwasawa). *Let A be the $\mathbf{Z}$-submodule of $\mathbf{Z}G$ generated by l^n and*

$$\{a - \delta_a | a \in (\mathbf{Z}/l^n\mathbf{Z})^*\} = \{t(\delta) - \delta | \delta \in G\}.$$

Then $J = A\theta$.

A proof of this may be found in [**7**], page 11, or [**5**], Lemma 3, page 593.

In order to obtain our main result we need to characterize the submodules of $\mathbf{Z}G$-modules generated by images of elements of J. The following result was obtained for $n = 1$ by McCulloh [**8**, (4.1.5)].

PROPOSITION 2. *Let M be a $\mathbf{Z}G$-module, written multiplicatively. For m in M, the following conditions are equivalent.*

(i) $m \in M^J$ = *submodule of M generated by* $\{m^\gamma | m \in M, \gamma \in J\}$

(ii) $m^\alpha \in M^J$ *for all α in A*

(iii) *there exists a in M such that $m^\alpha = a^{\alpha\theta}$ for all α in A.*

Proof. (iii) $\Rightarrow$ (ii) is trivial.

(i) $\Rightarrow$ (iii): If $m = \prod b_i^{\beta_i}$, $b_i \in M$, $\beta_i \in J$, let $\beta_i = \alpha_i\theta$, $\alpha_i \in A$. Then

$$m^\alpha = \prod b_i^{\beta_i\alpha} = \prod b_i^{\alpha_i\theta\alpha} = (\prod b_i^{\alpha_i})^{\theta\alpha}.$$

(iii) follows.

(ii) $\Rightarrow$ (i). We divide the proof into two cases, $n = 1$ and $n > 1$. We write $a \equiv b \pmod{M^J}$ if ab^{-1} is in M^J.

$n = 1$. We have $m^l \in M^J$ and $m^{t(\delta)-\delta} \in M^J$ for all δ in G by (ii). Since $l\theta \in J$,

$$1 \equiv m^{-l\theta} \equiv m^{-\Sigma t(\delta)\delta^{-1}} = \prod m^{-t(\delta)\delta^{-1}}.$$

Now $m^{t(\delta)} \equiv m^\delta$ for all m in M, $\delta \in G$, so

$$1 \equiv \prod m^{-t(\delta)t(\delta^{-1})}.$$

Since $t(\delta)t(\delta^{-1}) \equiv 1 \pmod{l}$,

$$1 \equiv \prod_{\delta \in G} m^{-1} = m^{-(l-1)} \equiv m \pmod{M^J}.$$

Hence $m \in M^J$.

https://doi.org/10.4153/CJM-1982-045-7 Published online by Cambridge University Press

$n > 1$. Since $\theta(t(\delta) - \delta) \in J$ for all $\delta \in G$, we have for any m in M, $\delta \in G$, $1 \equiv m^{\theta(t(\delta)-\delta)}$. Now

$$\theta(t(\delta) - \delta) = \sum_{\gamma \in G} \left(\frac{t(\gamma)t(\delta) - t(\gamma\delta)}{l^n} \right) \gamma^{-1},$$

and $m^\gamma \equiv m^{t(\gamma)} \pmod{M^J}$, by (ii). So

$$1 \equiv m^h$$

where

$$h = \sum_{\gamma} \left(\frac{t(\gamma)t(\delta) - t(\gamma\delta)}{l^n} \right) t(\gamma^{-1}).$$

To show $m \in M^J$ it suffices to show that h is prime to l. For $m^{l^n} \in M^J$ by (ii); if also $m^h \in M^J$ with $(h, l) = 1$, then $m \in M^J$.

Let δ be a generator of G, and $\gamma = \delta^i$. Then

$$h = \sum_{i=1}^{l^{n-1}(l-1)} \left(\frac{t(\delta^i)t(\delta) - t(\delta^{i+1})}{l^n} \right) t(\delta^{-i}).$$

Let s_i be an integer $\geqq 0$ so that $t(\delta^i) = t(\delta)^i - l^n s_i$. Then

$$\begin{aligned} h &= \sum_{i=1}^{l^{n-1}(l-1)} \frac{[(t(\delta)^i - l^n s_i)t(\delta) - (t(\delta)^{i+1} - l^n s_{i+1})]}{l^n} t(\delta^{-i}) \\ &= - \sum_{i=1}^{l^{n-1}(l-1)} \frac{[t(\delta) l^n s_i - l^n s_{i+1}]}{l^n} t(\delta^{-i}) \\ &\equiv - \sum_{i=1}^{l^{n-1}(l-1)} [s_i t(\delta)^{-i+1} - s_{i+1} t(\delta)^{-i}] \pmod{l} \\ &= \sum_{j=2}^{l^{n-1}(l-1)+1} t(\delta)^{-j+1} s_j - \sum_{i=1}^{l^{n-1}(l-1)} t(\delta)^{-i+1} s_i \\ &= t(\delta)^{-l^{n-1}(l-1)} s_{l^{n-1}(l-1)+1} - t(\delta)^0 s_1. \end{aligned}$$

Now $s_1 = t(\delta) - t(\delta)/l^n = 0$; also

$$\begin{aligned} s_{l^{n-1}(l-1)+1} &= \frac{1}{l^n} [t(\delta)^{l^{n-1}(l-1)+1} - t(\delta^{l^{n-1}(l-1)+1})] \\ &= \frac{1}{l^n} [t(\delta)^{l^{n-1}(l-1)} t(\delta) - t(\delta)] = t(\delta) \left[\frac{t(\delta)^{l^{n-1}(l-1)} - 1}{l^n} \right], \end{aligned}$$

and $t(\delta)^{l^{n-1}(l-1)} \equiv 1 \pmod{l^n}$. So

$$\begin{aligned} h &\equiv s_{l^{n-1}(l-1)+1} \equiv t(\delta) \left[\frac{t(\delta)^{l^{n-1}(l-1)} - 1}{l^n} \right] \pmod{l} \\ &\equiv 0 \text{ if and only if } t(\delta)^{l^{n-1}(l-1)} \equiv 1 \pmod{l^{n+1}}. \end{aligned}$$

https://doi.org/10.4153/CJM-1982-045-7 Published online by Cambridge University Press

But δ is a generator of $G = \text{Aut } C$, and $G \simeq (\mathbf{Z}/l^n\mathbf{Z})^*$, $n \geqq 2$ via the map $\delta^i \to t(\delta^i)$. So $t(\delta)$ is a primitive element mod l^n. It is known that if a is a primitive element mod l^n, $n \geqq 2$, then a is a primitive element mod l^m, $m > n$, for all m [**3**, p. 215, E4]. Hence

$$t(\delta)^{l^{n-1}(l-1)} \not\equiv 1 \pmod{l^{n+1}},$$

and so $h \not\equiv 0 \pmod{l}$. That completes the proof of Proposition 2.

Primitive elements. By Cl (RC) we mean the group of isomorphism classes of rank one projective RC-modules. We define h Cl (RC), the subgroup of Cl (RC) consisting of primitive elements. One definition of h Cl (RC) is by the maps:

$$\epsilon_1, \epsilon_2, \Delta : C \to C \times C$$

defined by

$$\epsilon_1(\sigma) = 1 \otimes \sigma$$
$$\epsilon_2(\sigma) = \sigma \otimes 1$$
$$\Delta(\sigma) = \sigma \otimes \sigma$$

for σ in C. A class P in Cl (RC) is primitive if

$$\epsilon_{1*}(P)\epsilon_{2*}(P) = \Delta_*(P)$$

where $(\ )_*$ denotes the induced map on Cl $(\ )$. An equivalent formulation of h Cl (RC) is obtained by the Yoneda lemma [**4**, (2.6)], [**2**, (1.7)]:

$$h \text{ Cl } (RC) \cong \text{Hom } (\text{Alg}_R (RG,), \text{Cl } (\ ))$$

via the maps

$$P \to f, \ f(\xi) = \xi_*(P),$$
$$f \to f(1_{RG}).$$

We prove

THEOREM 3. *Let R be a commutative ring, C a cyclic group of odd prime power order l^n. Then h Cl $(RC) \subseteq \text{Cl}^0 (RC)^J$.*

Proof. Let P be in h Cl (RC) and f be the corresponding element of Hom $(\text{Alg}_R (RC, \ ), \text{Cl } (\ ))$. We first note that if χ_0 in $\text{Alg}_R (RC, R)$ is the trivial character, then χ_0 is the identity element in $\text{Alg}_R (RC, R)$, so $R = f(\chi_0) = \chi_{0*}(P)$, hence $P \in \text{Cl}^0 (RC)$ (cf. [**2**, (1.8)]).

To show P is in $\text{Cl}^0 (RC)^J$ we apply Proposition 2, (ii) and Proposition 1, and show that P^{l^n} is in $\text{Cl}^0 (RC)^J$ and that

$$\delta_*(P) = P^\delta \equiv P^{t(\delta)} \pmod{\text{Cl}^0 (RC)^J}$$

for δ in $G = \text{Aut } (C)$. In fact, we show that P^{l^n} and $P^{\delta - t(\delta)}$ are trivial in Cl (RC).

https://doi.org/10.4153/CJM-1982-045-7 Published online by Cambridge University Press

The multiplication in $\mathrm{Alg}_R\ (RC, RC)$ is given by

$$(\xi.\ \eta)(\sigma) = (\xi \otimes \eta)(\sigma \otimes \sigma) = \xi(\sigma)\eta(\sigma).$$

Hence if t is a positive integer, the map $\hat{t}$ in $\mathrm{Alg}_R\ (RC, RC)$ defined by linearity and $\hat{t}(\sigma) = \sigma^t$, σ in C, may be written as $\hat{t} = 1^t$, where 1 is the identity function on RC. Moreover, for P in $h\ \mathrm{Cl}\ (RC)$,

$$P^t = f(1)^t = f(1^t) = f(\hat{t}).$$

Thus $P^{l^n} = f(\hat{l}^n)$. But $\hat{l}^n(\sigma) = \sigma^{l^n} = 1$ for all σ in C, so $\hat{l}^n$ is the identity element of $\mathrm{Alg}_R\ (RC, RC)$. Thus $P^{l^n} = f(\hat{l}^n) = R$, the identity of $\mathrm{Cl}\ (RC)$.

Also, if $\delta \in \mathrm{Aut}\ (C)$, $\delta(\sigma) = \sigma^{t(\delta)}$ for all σ in C, then $\delta = \widehat{t(\delta)}$ in $\mathrm{Alg}_R\ (RC, RC)$. So

$$P^{t(\delta)} = f(\widehat{t(\delta)}) = f(\delta) = \delta_*(P) = P^\delta.$$

That completes the proof.

COROLLARY 4. *If C is cyclic of odd prime power order, then the image of the Picard invariant map:* $\mathrm{Gal}\ (R, C) \to \mathrm{Cl}\ (RC)$ *is contained in* $\mathrm{Cl}^0\ (RC)^J$.

For $\mathrm{Gal}\ (R, C)$ maps into $h\ \mathrm{Cl}\ (RC)$, by [**2**, (1.2)].

REFERENCES

1. S. Chase, D. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Memoirs Amer. Math. Soc. *52* (1965), 15–33.

2. L. Childs, *The group of unramified Kummer extensions of prime degree*, Proc. London Math. Soc. *35* (1977), 407–422.

3. ——— *A concrete introduction to higher algebra* (Springer Verlag, New York, 1979).

4. L. Childs and A. Magid, *The Picard invariant of a principal homogeneous space*, J. Pure Appl. Algebra *4* (1974), 273–286.

5. A. Frohlich, *Stickelberger without Gauss sums*, in *Algebraic number fields* (Academic Press, London, 1977), 589–608.

6. K. Iwasawa, *Lectures on p-adic L-functions*, Annals of Math. Studies *74* (Princeton, 1972).

7. S. Lang, *Cyclotomic fields* (Springer Verlag, New York, 1978).

8. L. McCulloh, *A Stickelberger condition on Galois module structure for Kummer extensions of prime degree*, in *Algebraic number fields* (Academic Press, London, 1977), 561–588.

State University of New York at Albany,
Albany, New York