TWO THEOREMS ON GALOIS COHOMOLOGY[1]

MICHAEL ROSEN

1. **Introduction.** Let k and K be algebraic number fields, K a finite extension of k with Galois group G. H. Yokoi has considered the ring of integers O_K in K as a $Z[G]$ module (see [2]). In particular, he has proven

THEOREM. *If both K and k are Galois over the rationals Q, and G is cyclic of prime order, then $H^m(G, O_K) \approx H^n(G, O_K)$ for all integers m and n.*

We will prove a generalization of this. Namely

THEOREM 1. *If G is a cyclic group, then* $\operatorname{ord} H^m(G, O_K) = \operatorname{ord} H^n(G, O_K)$ *for all integers m and n.*

Notice that we have dropped the hypothesis that both k and K be Galois over the rationals.

To see how Theorem 1 generalizes Yokoi's result, remember that if G has prime order p, then multiplication by p annihilates all the cohomology groups. Thus in this case the cohomology groups are determined up to isomorphism by their order.

The technique used to prove Theorem 1 can be used to prove other results of a similar nature. In the same situation as above let us consider U_K, the units of K, as a $Z[G]$ module. Then we have

THEOREM 2. *Let G be a cyclic group, and suppose that no infinite prime of k is ramified in K. If* $\operatorname{ord} G = n$, *then* $n \operatorname{ord} H^{2r}(G, U_K) = \operatorname{ord} H^{2s+1}(G, U_K)$ *for all integers r and s.*

The hypothesis about no infinite prime ramifying is satisfied, for example, when K is totally real or when n is odd.

2. **Proofs of the theorems.** The proofs of both theorems are easy consequences of the following lemma which is a direct generalization of a result of Chevalley in Herbrand quotients (see [1]). It has come to my attention that this generalization has been discovered independently by Dr. J. Smith of Michigan University.

We need some notation. From now on G will be a cyclic group of order n, σ a generator of G, and when $d \mid n$, $G(d)$ will be the unique

Received by the editors October 18, 1965 and, in revised form, March 24, 1966.

[1] This paper was written when the author held an O.N.R. Research Associateship (O.N.R. 432).

subgroup of G having order d. $K(d)$ will be the cyclotomic field of dth roots of unity, $O(d)$ the ring of integers in $K(d)$, and $\zeta(d)$ a primitive dth root of unity.

When d is a prime power, p^i, $(1-\zeta(d))$ is a prime ideal in $O(d)$, whose residue class field has p elements. On the other hand, when d is composite $1-\zeta(d)$ is a unit. This is seen as follows. Let $d=p_1p_2q$, where p_1 and p_2 are distinct primes. Notice that $\zeta(d)^{p_1q}=\zeta(p_2)$ and $\zeta(d)^{p_2q}=\zeta(p_1)$. This shows that $1-\zeta(d)$ divides both $1-\zeta(p_1)$ and $1-\zeta(p_2)$. Taking absolute norms, we see that the norm of $1-\zeta(d)$ divides both p_1 and p_2. Thus the norm of $1-\zeta(d)$ is a unit, and consequently $1-\zeta(d)$ is a unit.

Let A be a finitely generated $Z[G]$ module. The Herbrand quotient, $q(A)$, is defined to be the ratio of ord $H^0(G, A)$ to ord $H^1(G, A)$.

Let $A^{G(d)}$ be the subset of A left fixed by $G(d)$, and define $r(d)$ to be the Z rank of $A^{G(d)}$.

LEMMA. *Let $n=\prod_p p^{t(p)}$ be the prime decomposition of n. Then $q(A)=\prod_{p|n} p^{s(p)}$ where*

$$s(p) = t(p)r(n) - \sum_{i=1}^{t(p)} \phi(p^i)^{-1}(r(n/p^i) - r(n/p^{i-1})).$$

PROOF. Notice to begin with that $Q[G]\approx Q[x]/(x^n-1)$ where x is an indeterminate. We have $x^n-1=\prod_{d|n}\Phi_d(x)$ where $\Phi_d(x)$ is the cyclotomic polynomial of dth roots of unity. Consequently, $Q[G] \approx \sum_{d|n} K(d)$. Each $K(d)$ becomes an irreducible $Q[G]$ module, where σ acts as multiplication by $\zeta(d)$.

Consider $V=Q\otimes A$. V is a $Q[G]$ module. Thus $V\approx \sum_{d|n} a(d)K(d)$ where the $a(d)$ are certain nonnegative integers. We easily deduce the existence of a $Z[G]$ submodule B of A such that A/B is finite, and $B\approx \sum_{d|n} a(d)O(d)$. From the well known properties of the Herbrand quotient we have

$$q(A) = q(B) = \prod_{d|n} q(O(d))^{a(d)}.$$

We now compute $q(O(d))$. For $d=1$, $O(d)=Z$ acted on trivially by G. Let $N=\sum_{i=0}^{n-1}\sigma^i$. Then $H^0(G, Z)=Z/NZ=Z/nZ$. Since G is cyclic $H^1(G, Z)\approx H^{-1}(G, Z)=Z_N/(1-\sigma)Z=(o)$. Thus $q(O(1))=n$.

For $d\neq 1$ we have $O(d)^G=(o)$ since σ acts as multiplication by $\zeta(d)$. Therefore ord $H^0(G, O(d))=1$. On the other hand, $O(d)_N = \{a\in O(d) \mid Na=o\} = O(d)$, and $(1-\sigma)O(d) = (1-\zeta(d))$. Thus $H^1(G, O(d))\approx H^{-1}(G, O(d))=O(d)/(1-\zeta(d))$. The remarks preceding this lemma now show that $q(O(d))=1$ if d is composite and $q(O(d)) =p^{-1}$ if $d=p^i$ is a prime power.

Putting together the information we now have, we get that $q(A) = \prod_{p|n} p^{s(p)}$ where

$$s(p) = t(p)a(1) - \sum_{i=1}^{t(p)} a(p^i).$$

To relate the $a(d)$ with the $r(d)$ notice that the Z rank of $A^{G(d)}$ is equal to the Q dimension of $V^{G(d)}$. The group $G(n/p^i)$ is generated by σ^{p^i}. From the way that σ acts it follows that $V^{G(n/p^i)} = \sum_{j=0}^{i} a(p^j)K(p^j)$. Therefore, $r(n/p^i) = \sum_{j=0}^{i} \phi(p^j)a(p^j)$. Solving for $a(p^i)$ we get that $a(p^i) = \phi(p^i)^{-1}(r(n/p^i) - r(n/p^{i-1}))$. This completes the proof.

Proof of Theorem 1. Since G is cyclic the cohomology groups are periodic of order 2. It is thus sufficient to show that $q(O_K) = 1$. If $[K:Q] = N$, then the Z rank of $O_K^{G(d)} = N/d$. Substituting this information into the formula of the lemma we see that, indeed, $q(O_K) = 1$.

Corollary. *If G is cyclic of square free order then $H^n(G, O_K) \approx H^m(G, O_K)$ for all integers m and n.*

Proof. The restriction map gives a monomorphism of the p-primary component of $H^i(G, O_K)$ into $H^i(G(p), O_K)$. It follows that the p-primary components of the cohomology groups under consideration are elementary. These groups are thus determined up to isomorphism by their order.

Proof of Theorem 2. Let K be an algebraic number field. Denote by $r_1(K)$ the number of real primes of K, and by $r_2(K)$ one half the number of complex primes. The Dirichlet Unit Theorem states that rank $(U_K) = r_1(K) + r_2(K) - 1$. If k is a subfield of K, the condition that no infinite prime ramify in K means that the extension of every real place is real. This implies rank $(U_K) = [K:k]$ rank $(U_k) + [K:k] - 1$. Using the notation of the lemma, with $A = U_K$, we have $r(1) = dr(d) + d - 1$. Substituting this into the formula of the lemma we get $s(p) = -t(p)$ and thus $q(U_K) = n^{-1}$. This finishes the proof.

Bibliography

1. C. Chevalley, *Class field theory*, Nagoya University, Japan, 1953–1954.

2. H. Yokoi, *On the Galois cohomology group of the ring of integers in an algebraic number field*, Acta Arith. **8** (1962/1963), 243–250.

Brandeis University