ON THE GALOIS COHOMOLOGY OF THE RING OF INTEGERS IN AN ALGEBRAIC NUMBER FIELD

M. P. LEE AND M. L. MADAN

Notation. Z = the ring of rational integers,
Q = the field of rational numbers,
K = a field of algebraic numbers of finite degree over Q,
F = a finite normal extension of K,
O_K, O_F = the ring of all integers of K, F respectively,
G = Galois group of F over K.

Introduction. G operates in a natural way on the additive groups of F and O_F. It is well known that $H^r(G, F^+)$, the r-dimensional cohomology group of G with F^+ as coefficients-module is trivial for all integer values of r. In [6]–[9] Yokoi has obtained the following results concerning $H^r(G, O_F^+)$:

THEOREM I. *If the* 0-*dimensional cohomology group* $H^0(G, O_F)$ *is trivial,* (*we write* O_F *for* O_F^+), *then* $H^r(V, O_F)$ *is trivial in all dimensions for all subgroups* V *of* G.

THEOREM II. *If* G *is cyclic of prime order, the groups* $H^r(G, O_F)$ *are isomorphic in all dimensions.*

THEOREM III. *If* G *is arbitrary cyclic, all the groups* $H^r(G, O_F)$ *have the same order.*

On the basis of these results he conjectured in [9] that the groups $H^r(G, O_F)$ have the same order also in the case when G is not cyclic. In the present note, we shall show that the conjecture is false. We shall also demonstrate how the problem of determining $H^r(G, O_F)$ can be localized. In the end, we shall make some remarks concerning proofs of Theorems I, II and III and give a generalization of Theorem I in the case where G is nilpotent.

Counterexample. Let $K=Q$, F be the splitting field of $f(x)=x^3-2$ over K, θ be the real root of $f(x)$ and $E=Q(\theta)$. $F=E(\eta)$, where η is a primitive 3rd root of unity. G is generated by two elements σ and τ satisfying the generating relations $\sigma^3=\tau^2=1$, $\sigma^2\tau=\tau\sigma$. The action of G on F is given by: $\sigma(\theta)=\theta\eta$, $\sigma(\eta)=\eta$, $\tau(\theta)=\theta$, $\tau(\eta)=-1-\eta$.

We shall first find an integral basis of F over K. O_E, the ring of all integers in E, is a principal ideal domain having a Z-basis consisting

Received by the editors September 1, 1967.

of 1, θ, θ^2. Consider the O_E-module $M=O_E+O_E\beta$, where $\beta=(2+\eta)(1+\theta)^{-1}$. β satisfies the equation $x^2-(\theta^2-\theta+1)x+(\theta^2-1)=0$ and so β is in O_F. It can be easily verified that the relative discriminant of M is $(1+\theta)O_E$. $\text{Norm}_{E/\mathfrak{Q}}(1+\theta)=3$ implies that $1+\theta$ is a prime element of O_E. Thus $\{1, \beta\}$ is an integral basis of F over E [2, p. 129] and hence $\{1, \theta, \theta^2, \beta, \beta\theta, \beta\theta^2\}$ is an integral basis of F over K.

It is now a simple matter to see that the set $\{b_i: i=1, \cdots, 6\}$, where $b_1=\theta+\theta^2$, $b_2=(\theta^2-2\theta+\theta\beta-2\beta)$, $b_3=\theta$, $b_4=\theta\beta+\theta^2\beta-2\theta$, $b_5=1$, $b_6=\beta-\theta^2$, is a Z-basis for O_F. The action of G on O_F is given by the table:

	b_1	b_2	b_3	b_4	b_5	b_6
σ	b_2	$-b_1-b_2$	b_4	$-b_3-b_4$	b_5	b_6+b_1
τ	b_1	$-b_1-b_2$	b_3	$-b_3-b_4$	b_5	$b_5-b_6-b_1$

Let $\alpha=\sum_{i=1}^6 \alpha_i b_i \in O_F$. The trace of α, $N(\alpha)=3(2\alpha_5+\alpha_6)b_5$. Therefore $H^0(G, O_F)\cong(O_F^G)/N(O_F)\cong Z_3$. Let us now examine $H^1(G, O_F)$. If $h: G\to O_F$ is any 1-cocycle, the group relations of G yield the conditions: $(\tau+1)h(\tau)=0$, $(\sigma^2+\sigma+1)h(\sigma)=0$ and $(\sigma\tau+1)(h(\tau)-h(\sigma))=0$. These conditions imply $h(\tau)=x_1b_1+(2x_5+2x_1)b_2+x_3b_3+2x_3b_4+x_5b_5+(-2x_5)b_6$ and $h(\sigma)=y_1b_1+(3x_1+4x_5-y_1)b_2+y_3b_3+(3x_3-y_3)b_4$, where $x_1, x_3, x_5, y_1, y_3 \in Z$. Choose $\alpha\in O_F$ as follows:

$$\alpha=\sum_{i=1}^{6}\alpha_i b_i, \quad \alpha_1=2x_5+x_1-y_1, \quad \alpha_2=-x_5-x_1, \quad \alpha_3=x_3-y_3,$$

$\alpha_4=-x_3$, $\alpha_6=x_5$ and α_5 may be chosen arbitrarily. A simple calculation shows that $h(\tau)=(\tau-1)\alpha$ and $h(\sigma)=(\sigma-1)\alpha$. Thus every 1-cocycle is a coboundary and $H^1(G, O_F)=0$. Yokoi's conjecture is thereby disproved.

Localization. For a prime divisor $\mathfrak{p}$ of K, let $\mathfrak{A}$ be a fixed prime divisor of F lying above $\mathfrak{p}$. Let $O\mathfrak{Q}$ be the ring of integers of $F\mathfrak{Q}$, the completion of F at $\mathfrak{A}$, and $G\mathfrak{Q}$ be the local group. We have the following:

THEOREM 1. *$H^r(G, O_F)\cong\prod_{\mathfrak{p}}H^r(G_{\mathfrak{Q}}, O_{\mathfrak{Q}})$ for all integers r.*

PROOF. Let $\tilde{O}_F=\prod_{\mathfrak{P}} O_{\mathfrak{P}}$, $\tilde{O}_K=\prod_{\mathfrak{p}} O_{\mathfrak{p}}$, the first product taken over all prime divisors $\mathfrak{P}$ of F. O_F is diagonally embedded in $\tilde{O}_F$. Also $\tilde{O}_K$ is canonically embedded in $\tilde{O}_F$. Let $O^{(\mathfrak{p})}=\prod_{\mathfrak{P}/\mathfrak{p}} O_{\mathfrak{P}}$. $O^{(\mathfrak{p})}$ is G-module.

By Shapiro's well-known lemma, $H^r(G, O^{(\mathfrak{p})}) \cong H^r(G_{\mathfrak{Q}}, O_{\mathfrak{Q}})$. Now $\tilde{O}_F \cong \prod_{\mathfrak{p}} O^{(\mathfrak{p})}$. Therefore $H^r(G, \tilde{O}_F) \cong \prod_{\mathfrak{p}} H^r(G, O^{(\mathfrak{p})}) \cong \prod_{\mathfrak{Q}} H^r(G_{\mathfrak{Q}}, O_{\mathfrak{Q}})$. Thus the isomorphism we wish to establish is equivalent to $H^r(G, \tilde{O}_F) \cong H^r(G, O_F)$, for all r. Let $[F: K] = n$ and $w_1, \cdots, w_n$ be a normal basis of F over K consisting of integers. Let $\mathfrak{M} = O_K w_1 + \cdots + O_K w_n$. The index $[O_F: \mathfrak{M}] = l$ is finite. Therefore $\mathfrak{M}$ contains the ideal $\mathfrak{A} = (l)$ of O_F. $\mathfrak{A}\tilde{O}_F \subset \tilde{\mathfrak{M}} = \tilde{O}_K w_1 + \cdots + \tilde{O}_K w_n$. Therefore $\mathfrak{A}\tilde{O}_F + O_F \subset \tilde{\mathfrak{M}} + O_F$. But $\mathfrak{A}\tilde{O}_F + O_F = \tilde{O}_F$ [5, p. 195]. Therefore $\tilde{\mathfrak{M}} + O_F = \tilde{O}_F$. Thus

$$\frac{\tilde{O}_F}{\tilde{\mathfrak{M}}} \cong \frac{\tilde{\mathfrak{M}} + O_F}{\tilde{\mathfrak{M}}} \cong \frac{O_F}{O_F \cap \tilde{\mathfrak{M}}} \cong \frac{O_F}{\mathfrak{M}}.$$

These are module-isomorphisms. $\mathfrak{M}$, $\tilde{\mathfrak{M}}$ being G-regular, their cohomology is trivial. Therefore

$$H^r(G, \tilde{O}_F) \cong H^r(G, \tilde{O}_F/\tilde{\mathfrak{M}}) \cong H^r(G, O_F/\mathfrak{M}) \cong H^r(G, O_F).$$

This completes the proof of Theorem 1.

REMARKS. 1. A shorter and simpler proof of Theorem 1, which is also valid in a more general situation, can be constructed in the following way: Triviality of $H^0(G, O_F)$ is equivalent to the existence of an element α in O_F of trace 1. The endomorphism ϕ_α of O_F defined by $\phi_\alpha(\beta) = \alpha\beta$ has the identity mapping as its trace. $H^r(G, O_F) = 0$ follows from a very elementary result [1, p. 18, Satz 11] in the cohomology theory of finite groups. To show $H^r(V, O_F) = 0$ for any subgroup V of G, we note trace $(\alpha) = 1$ implies $\gamma = \sum \sigma_j(\alpha)$ has trace 1 w.r.t. V, where σ_j is a representative system of right-cosets.

2. For proving Theorem II, it is enough to show that $H^0(G, O_F)$, $H^1(G, O_F)$ have the same order because any element of the cohomology group other than identity is of order p. Theorem II follows from Theorem III or from a theorem of Tate [3, p. 57, Theorem 10.3].

3. A generalization of Theorem I may be given as follows:

THEOREM 2. *If G is a nilpotent group and $H^i(G, O_F)$ is trivial for some integer i, then $H^r(V, O_F)$ is trivial for all integral values of r and for all subgroups V of G.*

PROOF. It has recently been proved [4] that a finite group G is nilpotent if and only if for every finite G-module M, any relation $H^i(G, M) = 0$ implies all relations $H^r(G, M) = 0$ $(r = 0, \pm 1, \pm 2, \cdots)$.

Let $w_1, \cdots, w_n$ be a normal basis for F over K chosen such that $w_i \in O_F$, $i = 1, \cdots, m$. Let $\mathfrak{M} = O_K w_1 + \cdots + O_K w_n$. $H^r(G, \mathfrak{M}) = 0$ for all r and it follows from this and the exactness of the sequence

$$0 \to \mathfrak{M} \to O_F \to O_{F/\mathfrak{M}} \to 0$$

that $H^r(G, O_F) = H^r(G, O_{F/\mathfrak{M}})$ for all r. Thus if $H^i(G, O_F) = 0$ for some i, $H^i(G, O_{F/\mathfrak{M}}) = 0$. But $\mathfrak{M}$ is of finite index in O_F, hence $O_{F/\mathfrak{M}}$ is a finite G-module. Since G is nilpotent, applying the above stated theorem we have $H^r(G, O_F) = 0$ for all r. Applying Theorem I we obtain Theorem II.

4. Using an argument similar to that in 3, we see that our counter-example also provides a further example to establish the necessity that G be nilpotent in order for $H^i(G, M) = 0$ to imply $H^r(G, M) = 0$ for all r and all finite G-modules M.

Bibliography

1. E. Artin, *Kohomologie endlicher Gruppen*, Lecture notes, Hamburg, 1957.

2. ———, *Theory of algebraic numbers*, Lecture notes, Goettingen, 1959.

3. C. Chevalley, *Class field theory*, Nagoya Univ., 1953–1954.

4. K. Hoecksman et al., *A cohomological characterization of finite nilpotent groups*, Arch. Math. **19** (1968), 225–244.

5. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

6. H. Yokoi, *On the ring of integers in an algebraic number field as a representation module of Galois group*, Nagoya Math. J. **16** (1960), 83–90.

7. ———, *On an isomorphism of Galois cohomology groups* $H^n(G, O_K)$ *of integers in an algebraic number field*, Proc. Japan Acad. **38** (1962), 499–501.

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

9. ———, *A note on the Galois cohomology group of the ring of integers in an algebraic number field*, Proc. Japan Acad. **40** (1964), 245–246.

Ohio State University