54. A Note on the Galois Cohomology Group of the Ring of Integers in an Algebraic Number Field

By Hideo YOKOI
Nagoya Institute of Technology, Nagoya

(Comm. by Zyoiti SUETUNA, M.J.A., April 13, 1964)

1. **Introduction.** Let K be a finite Galois extension of a finite algebraic number field F and let $G=G(K/F)$ be the Galois group of K/F. Denote by $\mathfrak{o}_K$ and $\mathfrak{o}_F$ the rings of integers in K and F respectively. As usual, we shall denote by $H^r(G, A)$ the r-dimensional Galois cohomology group of G acting on a G-module A. Following Artin-Tate-Chevalley, we shall consider $H^r(G, A)$ also for negative r.

In (1) we proved the following

Theorem 1. *If we assume that the 0-dimensional Galois cohomology group $H^0(G, \mathfrak{o}_K)$ of $\mathfrak{o}_K$ with respect to K/F is trivial, then the Galois cohomology group of $\mathfrak{o}_K$ with respect to K/Ω is trivial for every dimension and for any intermediate field Ω of K/F.*

Later we obtained in (2) and (3) the following

Theorem 2. *Let K/F be a cyclic extension of prime order p. Then, for every dimension r, all the Galois cohomology groups $H^r(G, \mathfrak{o}_K)$ of $\mathfrak{o}_K$ with respect to K/F are isomorphic with each other.*

From these results, it is generally conjectured that all the Galois cohomology groups $H^r(G, \mathfrak{o}_K)$ of $\mathfrak{o}_K$ with respect to K/F have the same order. In this note we shall prove that this is in fact the case if K/F is a cyclic extension of any finite degree.

2. Let F be an algebraic number field of degree m and let K/F be a cyclic extension of degree n. Denote by $G=G(K/F)$ the Galois group of K/F. Then there exists a number B in K, by the theorem on existence of normal basis,[1] such that the conjugates $B^{(0)}, B^{(1)}, \cdots, B^{(n-1)}$ of B form a basis of K over F, i.e. a normal basis of K/F. Since we may choose an integer c such that cB becomes an integer in K, we can assume from the beginning, without losing generality, that B is an integer in K.

Further, let $\{\omega_1, \omega_2, \cdots, \omega_m\}$ be an arbitrary integral basis of F, and denote by $\mathfrak{o}^*$ the module generated by $\omega_i B^{(j)}$ $(i=1, 2, \cdots, m;\ j=0, 1, \cdots, n-1)$. Since $\omega_i B^{(j)}$ $(i=1, 2, \cdots, m;\ j=0, 1, \cdots, n-1)$ are linearly independent over the rational number field Q, the rank of the module $\mathfrak{o}^*$ is $N=mn$, and $\mathfrak{o}^*=\mathfrak{o}_F B^{(0)}+\mathfrak{o}_F B^{(1)}+\cdots+\mathfrak{o}_F B^{(n-1)}$ is a direct decomposition of the module $\mathfrak{o}^*$. Here, $\mathfrak{o}_F$ means the module of all integers

1) Cf. e.g. E. Noether [4], M. Deuring [5] etc.

in F: $\mathfrak{o}_F=[\omega_1, \omega_2, \cdots, \omega_m]$. On the other hand, the rank of the module $\mathfrak{o}_K$ of all integers in K is also $N=mn$. Therefore, the index $[\mathfrak{o}_K:\mathfrak{o}^*]$ of $\mathfrak{o}^*$ in $\mathfrak{o}_K$ is finite, namely the residue module $\tilde{\mathfrak{o}}=\mathfrak{o}_K/\mathfrak{o}^*$ of $\mathfrak{o}_K$ modulo $\mathfrak{o}^*$ is a finite module. Since $\mathfrak{o}_K$ and $\mathfrak{o}^*$ are G-modules, the residue module $\tilde{\mathfrak{o}}$ can be regarded as a G-module.[2)]

Since G is a cyclic group, from the well-known theorem in cohomology theory[3)] we obtain $H^{2r}(G, \mathfrak{o}_K)\cong H^0(G, \mathfrak{o}_K)$, $H^{2r-1}(G, \mathfrak{o}_K)\cong H^1(G, \mathfrak{o}_K)$ for every integer r. We generally denote by $Q(M)$ the Herbrand quotient $[H^0(G, M)]/[H^1(G, M)]$ of a G-module M if $H^0(G, M)$ and $H^1(G, M)$ are finite groups, i.e. if M is an Herbrand module. Since $\mathfrak{o}^*$ is a G-regular G-module, the Galois cohomology group $H^r(G, \mathfrak{o}^*)$ of $\mathfrak{o}^*$ is trivial for every dimension r. Therefore, the module $\mathfrak{o}^*$ is an Herbrand module and the Herbrand quotient $Q(\mathfrak{o}^*)$ of $\mathfrak{o}^*$ is equal to 1. Since the module $\tilde{\mathfrak{o}}$ is a finite G-module, the Herbrand quotient $Q(\tilde{\mathfrak{o}})$ of $\tilde{\mathfrak{o}}$ is defined and equal to 1. On the other hand, since the module $\mathfrak{o}_K$ is a finitely generated G-module, $\mathfrak{o}_K$ is an Herbrand module and the Herbrand quotient $Q(\mathfrak{o}_K)$ of $\mathfrak{o}_K$ is equal to $Q(\mathfrak{o}^*)\cdot Q(\tilde{\mathfrak{o}})=1$.

Consequently, the order of $H^0(G, \mathfrak{o}_K)$ is equal to the order of $H^1(G, \mathfrak{o}_K)$. Thus we have the following

Theorem 3. *Let K be a finite cyclic Galois extension of a finite algebraic number field F, and let $G=G(K/F)$ be the Galois group of K/F. Denote by $\mathfrak{o}_K$ the module of all algebraic integers in K. Then the Galois cohomology group $H^r(G, \mathfrak{o}_K)$ of $\mathfrak{o}_K$ with respect to K/F has the same order for every dimension r.*

References

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

[2] ——: On an isomorphism of Galois cohomology groups $H^r(G, \mathfrak{o}_K)$ of integers in an algebraic number field. Proc. Japan Acad., **38**, 499–501 (1962).

[3] ——: On the Galois cohomology group of the ring of integers in an algebraic number field. Acta Arithmetica, **VIII**, 243–250 (1963).

[4] E. Noether: Normalbasis bei Körpern ohne höhere Verzweigung. J. reine angew. Math., **167**, 147–152 (1931).

[5] M. Deuring: Galoische Theorie und Darstellungstheorie. Math. Annalen, **107**, 140–144 (1932).

[6] C. Chevalley: Class field theory. Nagoya University, pp. 34–39 § 6, (1953–1954).

---

2) For these three G-modules $\mathfrak{o}_K$, $\mathfrak{o}^*$, $\tilde{\mathfrak{o}}$ the sequence $0\to\mathfrak{o}^*\to\mathfrak{o}_K\to\tilde{\mathfrak{o}}\to 0$ is clearly exact, and this induces the following exact sequence of Galois cohomology groups: $\to H^r(G, \mathfrak{o}^*)\to H^r(G, \mathfrak{o}_K)\to H^r(G, \tilde{\mathfrak{o}})\to H^{r+1}(G, \mathfrak{o}^*)\to$. Since $\mathfrak{o}^*$ is a G-regular G-module, we obtain the following isomorphism for every dimension r and for any Abelian Galois group G: $H^r(G, \mathfrak{o}_K)\cong H^r(G, \tilde{\mathfrak{o}})$.

3) Cf. e.g. C. Chevalley [6].