AMITSUR COHOMOLOGY OF CUBIC EXTENSIONS OF ALGEBRAIC INTEGERS

BY

DAVID E. DOBBS†

ABSTRACT

Let K be the rational field Q or a complex quadratic number field other than $Q(\sqrt{-3})$. Let L be a normal three-dimensional field extension of K. If R and S are the rings of algebraic integers of K and L respectively, then the Amitsur cohomology group $H^2(S/R, U)$ is trivial. Inflation and class numbers give information about cohomology arising from certain nonnormal cubic extensions.

1. Introduction

As in [4] and [5], we are interested in the Amitsur cohomology group $H^2(S/R, U)$ arising from an extension $R \subset S$ of rings of algebraic integers. Although this group is finite and a bound can be given for its order [4, Prop. 2.1], it has been computed only in case $R = Z$ and S is quadratic (see [7] and [5]). In this paper, we pursue further the method of [5] and study $H^2(S/R, U)$ by means of its subgroup $H^1(S/R, UK/U)$. We begin in Section 2 with some cocycle computations. These are used in the proof of the main technical result, Theorem 3.2, which involves the structure of the group $U(R)$ of units of R and the Galois theory of the extension $K \subset L$ of quotient fields of R and S. As an application, Theorem 4.1 asserts $H^2(S/R, U) = 0$ in case L/K is three-dimensional normal and K is either Q or a complex quadratic other than $Q(\sqrt{-3})$. As explained in Example 4.3, the inflation results of [4] and [5], in conjunction with class number tables, can then be used to infer vanishing of $H^2(S/Z, U)$ for several nonnormal cubics L/Q to which the criterion in [4, Remark 4.3] fails to apply.

---

† This work was supported in part by NSF Grant GP-28409.

Received June 25, 1972

We employ the standard terminology concerning Amitsur cohomology and assume familiarity with the methods and notation of [5].

2. Odd-dimensional extensions

The *standing hypotheses for this section* are that R is a domain with quotient field K, that S is a flat R-subalgebra of a field extension L of K and that multiplication induces an isomorphism $S \otimes_R K \xrightarrow{\cong} L$.

As usual, write $L^i = \overset{i}{\underset{K}{\otimes}} L$ and $S^i = \overset{i}{\underset{R}{\otimes}} S$. Since flatness allows us to view $S^i \subset L^i$, we may identify the i-th cochain group of the Amitsur complex $C(S/R, UK/U)$ with $U(L^{i+1})/U(S^{i+1})$. In particular, if we define

$$C(S,R) = \{\xi \in U(L^2) : d^1(\xi) \in U(S^3) \subset U(L^3)\}$$

where d^* is the coboundary map of $C(L/K, U)$, then the first cocycle group of $C(S/R, UK/U)$ is $\{\xi \cdot U(S^2) : \xi \in C(S,R)\}$. For $\xi \in C(S,R)$, let $[\xi]$ denote the cohomology class of $\xi \cdot U(S^2)$ in $H^1(S/R, UK/U)$. Finally, let $t : L^2 \to L^2$ be the K-algebra isomorphism satisfying $t(x \otimes y) = y \otimes x$.

PROPOSITION 2.1. *Let $\xi \in C(S,R)$. Then $t(\xi) \in C(S,R)$ and $\xi t(\xi) \in U(S^2)$. Hence $[\xi] = -[t(\xi)]$.*

PROOF. Let $\xi = \Sigma\ \alpha_i \otimes \beta_i$. Then

$$d^1(\xi) = \varepsilon_0(\xi)\varepsilon_1(\xi)^{-1}\varepsilon_2(\xi)$$

$$= (\Sigma\ 1 \otimes \alpha_i \otimes \beta_i)(\Sigma\ \alpha_i \otimes 1 \otimes \beta_i)^{-1}(\Sigma\ \alpha_i \otimes \beta_i \otimes 1) \in U(S^3) \subset U(L^3).$$

Let k be the twist homomorphism $L^3 \to L^3$ given by $k(x \otimes y \otimes z) = z \otimes y \otimes x$. Since $k(S^3) \subset S^3$, we have $k(d^1(\xi)) = \varepsilon_2(t(\xi))\varepsilon_1(t(\xi))^{-1}\varepsilon_0(t(\varepsilon)) = d^1(t(\xi)) \in U(S^3)$; i.e., $t(\xi) \in C(S,R)$.

Next, apply the contraction homomorphism $c : L^3 \to L^2$, given by $c(x \otimes y \otimes z) = xz \otimes y$, to $d^1(\xi)$ to get $t(\xi)(\Sigma\ \alpha_i\beta_i \otimes 1)^{-1}\xi \in c(U(S^3)) \subset U(S^2)$. However, applying the contraction $L^3 \to L$ to $d^1(\xi)$ shows $\Sigma\ \alpha_i\beta_i \in U(S)$. Hence $\Sigma\ \alpha_i\beta_i \otimes 1 \in U(S^2)$, and so $\xi t(\xi) \in U(S^2)$. Finally, $[\xi] = -[t(\xi)]$ since $[\xi] + [t(\xi)] = [\xi t(\xi)] = 0$.

COROLLARY 2.2. *Assume that L is an odd-dimensional Galois extension of*

K and that S is the integral closure of R in L. Let $\xi \in C(S,R)$. Then $[\xi]=0$ $\Leftrightarrow$ there exists $l \in U(L)$ such that $\xi(t(\xi))^{-1}(l \otimes l^{-1}) \in U(S^2)$.

PROOF. By [5, Th. 3.8], $[L:K]^2[\xi]=0$. Since $[L:K]^2$ is odd, $[\xi]=0$ $\Leftrightarrow 2[\xi]=0 \Leftrightarrow [\xi]=-[\xi]=[t(\xi)] \Leftrightarrow [\xi(t(\xi))^{-1}]=0 \Leftrightarrow$ there exists $l \in U(L)$ such that $\xi(t(\xi))^{-1}(l \otimes l^{-1}) \in U(S^2)$.

3. Vanishing of cohomology

The *standing hypotheses for this section* are that R is a domain with quotient field K, that L is a (finite) n-dimensional Galois field extension of K with Galois group G, and that S is the integral closure of R in L.

PROPOSITION 3.1. *Assume that R is integrally closed, S is a flat R-module and G is cyclic. Then:*

i) *There is an exact sequence of abelian groups $0 \to X \to H^1(S/R, UK/U) \to U(R)/N(U(S))$, where N is the field norm $U(L) \to U(K)$ and X satisfies $n \cdot X = 0$.*

ii) *Assume that for every $r \in U(R)$, there exists a positive integer m which is relatively prime to n and satisfies $r^m = 1$. Then $n \cdot H^1(S/R, UK/U) = 0$.*

PROOF. (i) Since R is integrally closed, the multiplication map $S \otimes_R K \to L$ is an isomorphism. The proof of [5, Th. 3.8] therefore provides an exact sequence $0 \to X \to H^1(S/R, UK/U) \to H^1(S/R, (UK/U)^0)$ with $n \cdot X = 0$. However [5, Th. 3.1] embeds $H^1(S/R, UK/U)^0)$ in the group cohomology group $H^1(G, (UK/U)(S)) = H^1(G, U(L)/U(S))$ which, by Hilbert's Theorem 90, itself embeds in $H^2(G, U(S))$ via the connecting homomorphism. As $U(S)^G = U(R)$, the usual computation of cohomology for a cyclic group shows $H^2(G, U(S)) = U(R)/N(U(S))$, and (i) is proved.

ii) Since $n^2 \cdot H^1(S/R, UK/U) = 0$ by [5, Th. 3.8], the hypotheses of (ii) imply that the composition $H^1(S/R, UK/U) \to H^1(S/R, (UK/U)^0) \to U(R)/N(U(S))$ is the zero map. Hence $H^1(S/R, UK/U) = X$, and (ii) follows from (i).

THEOREM 3.2. *Assume that R is integrally closed, S is a flat R-module, $n=3$ and $U(R)$ is a torsion group with no element of order 3. Then $H^1(S/R, UK/U) = 0$.*

PROOF. Let $\xi \in C(S,R)$. We must show $[\xi]=0$.

Let $\xi = \sum \alpha_i \otimes \beta_i$ and $G=\{1,g,g^2\}$. Under the isomorphism $U(L^2) \to \prod_G U(L) = U(L)\times U(L)\times U(L)$, let ξ be sent to (a,b,c); i.e.

$$a = \sum \alpha_i\beta_i, \quad b = \sum \alpha_i g(\beta_i) \quad \text{and} \quad c = \sum \alpha_i g^2(\beta_i).$$

Now under the algebra isomorphism $L^3 \to \prod_{G^2} L$,

$$d^1(\xi) = (\sum 1\otimes\alpha_i\otimes\beta_i)(\sum \alpha_i\otimes 1\otimes\beta_i)^{-1}(\sum \alpha_i\otimes\beta_i\otimes 1)$$

corresponds, after some computation, to $(a,a,a,g(a),\ bg(b)c^{-1},\ bg(c)a^{-1},\ g^2(a),\ g^2(b)ca^{-1},\ cg^2(c)b^{-1})$. Since G maps S into itself and $d^1(\xi)\in U(S^2)$, it follows that each of the entries of this nine-tuple lies in $U(S)$.

As above, let N be the field norm $U(L)\to U(K)$. Since $a \in U(S)$, multiplying the fifth and eighth entries of the above nine-tuple shows

$$N(b) = bg(b)g^2(b) \in U(S)\cap K = U(R).$$

Considering the sixth and ninth entries shows $N(c)\in U(R)$.

Case 1. $N(b)=N(c)$. We shall apply the criterion in Corollary 2.2. Since $N(g(c)) = N(c) = N(b)$, Hilbert's Theorem 90 provides $l\in U(L)$ such that $g(c)b^{-1} = lg(l)^{-1}$. Then $cg^2(b)^{-1} = g^2(g(c)b^{-1}) = g^2(l)\,l^{-1}$. Since $t(\xi)$ corresponds to the triple $(a, g(c), g^2(b))\in\prod_G U(L)$, we see that $\xi t(\xi)^{-1}(l\otimes l^{-1})$ corresponds to $(1, bg(c)^{-1}lg(l)^{-1},\ cg^2(b)^{-1}lg^2(l)^{-1}) = (1,1,1)$. Hence $\xi t(\xi)^{-1}(l\otimes l^{-1}) = 1 \in U(S^2)$ and $[\xi]=0$.

General case. As $U(R)$ has no element of order 3, every element of $U(R)$ has order relatively prime to 3. Then Proposition 3.1 (ii) implies $3\cdot H^1(S/R, UK/U) = 0$. In particular, $[\xi^3] = 3[\xi] = 0$, and so there exists $l\in U(L)$ such that $\omega = \xi^3(l\otimes l^{-1})\in U(S^2)$.

Choose positive integers p and q, each congruent to 1 modulo 3, such that $N(b)^{3p+1} = 1 = N(c)^{3q+1}$. (For example, if the order $\nu(b)$ of $N(b)$ is congruent to 1 (resp., 2) modulo 3, take p so that $3p+1=\nu(b)$, (resp., $3p+1=2\nu(b)$).) If $m = p+q+3pq$, then $N(b)^{3m+1} = 1 = N(c)^{3m+1}$.

Since $\omega^m\in U(S^2)$, we see that $\omega^m\xi\in C(S,R)$ and $[\omega^m\xi]=[\xi]$. Observe that $\omega^m\xi$ corresponds to the triple $(a^{3m+1}, b^{3m+1}(lg(l)^{-1})^m, c^{3m+1}(lg^2(l^{-1}))^m)$. However

$N(b^{3m+1}(lg(l^{-1}))^m) = 1 = N(c^{3m+1}(lg^2(l^{-1}))^m)$ and Case 1 applies to show $[\omega^m \xi] = 0$. Hence $[\xi] = 0$, completing the proof.

COROLLARY 3.3. *Assume that R is Dedekind, $n = 3$ and $U(R)$ is a torsion group with no element of order* 3. *Then the canonical map* [3] *from $H^2(S/R, U)$ to the split Brauer group $B(S/R)$ is a monomorphism.*

PROOF. It is well-known that R is (integrally closed) regular and S is a module-finite faithful projective (flat) R-algebra. Theorem 3.2 and [5, Corollary 1.5] therefore apply, and complete the proof.

4. Applications

We begin by applying Corollary 3.3 to rings of algebraic integers.

THEOREM 4.1. *Let K be the rational field Q or a complex quadratic number field other than $Q(\sqrt{-3})$. Let L be a normal three-dimensional field extension of K. If R and S are the rings of algebraic integers of K and L respectively, then $H^2(S/R, U) = 0$.*

PROOF. We may apply Corollary 3.3 since L/K is Galois, R is Dedekind and the order of $U(R)$ is either 2 or 4. Hence $H^2(S/R, U) \to B(S/R)$ is a monomorphism. A well-known application of global class field theory asserts that $B(S/R)$ vanishes, since it is annihilated by both 2 and $[L:K] = 3$. Thus, $H^2(S/R, U) = 0$.

THEOREM 4.2. *Let L be a nonnormal three-dimensional field extension of Q, F a normal closure of L/Q, and K the unique quadratic subfield of F. Let R, S and T be the rings of algebraic integers of K, L and F respectively. Then:*

i) *$L = Q(\alpha)$ for some root α of $x^3 + px + q \in Q[x]$. If $D = -4p^3 - 27q^2$, then $K = Q(\sqrt{D})$.*

ii) *The order of $H^2(S/Z, U)$ divides 3^{216}.*

iii) *There exist monomorphisms $H^2(S/Z, U) \to H^2(T/Z, U)$ and $H^2(T/Z, U) \to H^0(T/R, \mathrm{Pic})$. Hence, the orders of $H^2(S/Z, U)$ and $H^2(T/Z, U)$ each divide the class number of T.*

iv) *Assume that $D < 0$ and $K \neq Q(\sqrt{-3})$. Then there is an exact sequence $0 \to H^1(T/R, U) \to \mathrm{Pic}(R) \to H^0(T/R, \mathrm{Pic}) \to 0$. Hence, the orders of $H^2(S/Z, U)$ and $H^2(T/Z, U)$ each divide the class number of R.*

PROOF. As L/Q is not normal, $[F:L]=2$ and $\mathrm{Gal}(F/Q)=S_3$, the unique nonabelian group of order 6. Since S_3 has but one subgroup of index 2, Galois theory implies F has a unique quadratic subfield K.

i) By the primitive element theorem, $L=Q(\alpha)$ for some root α of an irreducible monic polynomial $f(x)\in Q[x]$. By a linear substitution, we may assume $f(x) = x^3 + px + q$. As L/Q is nonnormal, it is well-known that

$$D = -4p^3 - 27q^2$$

is not the square of a rational number. To establish (i), it therefore suffices to show $\sqrt{D}\in F$.

Let β and γ be the other roots of $f(x)$ in F. Since $\alpha^3 + p\alpha = \beta^3 + p\beta(=-q)$ and $\alpha \neq \beta$, we have $\alpha^2+\beta^2+\alpha\beta+p=0$, and an application of the quadratic formula yields $\sqrt{-3\alpha^2-4p}\in F$. Similarly $\sqrt{-3\beta^2-4p}$ and $\sqrt{-3\gamma^2-4p}$ lie in F. By using the algorithm that expresses symmetric functions in terms of elementary symmetric functions, we find $(-3\alpha^2-4p)(-3\beta^2-4p)(-3\gamma^2-4p) = -27q^2-36p^3+96p^3-64p^3=D$, and (i) is proved.

ii) As the multiplicative group of roots of unity inside T is cyclic, the Dirichlet unit theorem implies that $U(T)$ can be generated by at most $1+5=6$ elements. Then [4, Prop. 2.1] shows $H^2(S/Z,U)$ is a finite group of order at most $3^{(6(3!)^2)}=3^{216}$. However $H^2(S/Z,U)$ is 3-torsion [1, Th. 6] and, hence, has order a power of 3, thus proving (ii).

iii) By [4, Remark 3.3] or [5, Th. 2.7], the kernel of the inflation map $\inf: H^2(S/Z,U)\to H^2(T/Z,U)$ is annihilated by 4. Since $H^2(S/Z,U)$ is 3-torsion, inf is a monomorphism.

Since Q has but one real place, global class field theory implies that the Brauer group $B(Z)=0$. As $\mathrm{Pic}(Z)=0$, the Chase-Rosenberg exact sequence [3, Th. 7.6] therefore shows $H^2(T/Z,U)\cong H^0(T/Z,\mathrm{Pic})$. Since $H^0(T/Z,\mathrm{Pic})\subset H^0(T/R,\mathrm{Pic})$ $\subset \mathrm{Pic}\,(T)$ and the class number of T is the order of $\mathrm{Pic}(T)$, (iii) now follows.

iv) Since $D<0$, (i) shows K is complex. As $K\neq Q(\sqrt{-3})$, Theorem 4.1 implies $H^2(T/R,U)=0$. Then (iv) follows readily from (iii) and the Chase-Rosenberg exact sequence.

EXAMPLE 4.3. Let S be the ring of algebraic integers of the cubic number field L generated over Q by a root of the irreducible polynomial $x^3 + px + q = x^3 + 6x + 6$ (resp., $x^3 + 6x + 1, x^3 + 7x + 7, x^3 - 3x + 8, x^3 + 6x + 8$). Now, L/Q is not normal (since $-4p^3 - 27q^2$ is not the square of a rational number) and S has class number 3 (see the tables in [8]). Moreover, the criterion in [4, Remark 4.3] gives no information about $H^2(S/Z, U)$. However, using Theorem 4.2 (i), we see that the related quadratic field is $K = Q(\sqrt{-m})$ where $m = 51$ (resp., 11, 55, 5, 2). From tables in [2], the class number of the algebraic integers of K is 2 (resp., 1, 4, 2, 1). Apply Theorem 4.2 (ii) and (iv) to conclude $H^2(S/Z, U) = 0$.

There are cases not resolved by Theorem 4.2 (iv), however. For example, the ring of algebraic integers arising from a root of $x^3 + 4x + 6$ and the ring of algebraic integers of the corresponding quadratic $Q(\sqrt{-307})$ each have class number 3.

EXAMPLE 4.4. In view of the preceding examples, it seems worthwhile to observe some applications of [4, Remark 4.3] which do not follow from Theorem 4.2 (iv).

a) First, take $p = 4$ and $q = 1$ (in the notation of Theorem 4.2). Then S has class number 2 [8, p.76] and, since $B(Z) = 0$, [4, Remark 4.3] implies $H^2(S/Z, U) = 0$. Note that Theorem 4.2 (iv) does not yield this information, since $K = Q(\sqrt{-283})$ and tables in [2] show that the class number of R is 3.

b) For a noncubic application, let $R \subset S$ be the rings of algebraic integers of subfields $K \subset L$ of the cyclotomic field F generated (over Q) by a primitive 2^m-th root of unity. Then the canonical map $H^2(S/R, U) \to B(S/R)$ is a monomorphism. For the proof, let T be the ring of algebraic integers of F. By [9, Satz C, p. 244], the class number of T is odd. However [6, Satz, p. 93] shows that the class number of S divides that of T and, hence, is also odd. Since $[L:K] | [F:Q] = \phi(2^m) = 2^{m-1}$, [4, Remark 4.3] applies to complete the proof.

REFERENCES

1. S. A. Amitsur, *Complexes of rings*, Israel J. Math. **2** (1964), 143–154.

2. Z. I. Borevich and I. R. Shafarevich, *Number Theory* (English translation), Academic Press, New York, 1966.

3. S. U. Chase and A. Rosenberg, *Amitsur cohomology and the Brauer group*, Mem. Amer. Math. Soc., No. 52, 1965.

4. D. E. Dobbs, *Amitsur cohomology of algebraic number rings*, Pacific J. Math. **39** (1971), 631–635.

5. D. E. Dobbs, *On inflation and torsion of Amitsur cohomology*, Canad. J. Math. **XXIV** (1972), 239–260.

6. P. Fürtwangler, *Über die Klassenzahlen Abelscher Zahlkörper*, J. Reine Angew. Math. **134** (1908), 91–94.

7. R. A. Morris, *On the Brauer group of Z*, Pacific J. Math. **39** (1971), 619–630.

8. L. W. Reid, *A table of class numbers for cubic number fields*, Amer. J. Math. **23** (1901), 68–84.

9. H. Weber, *Theorie der Abel'schen Zahlkörper*, Acta Math. **8** (1886), 193–263.

RUTGERS UNIVERSITY
NEW BRUNSWICK, N. J. 08903, U.S.A.