Pacific Journal of Mathematics

AMITSUR COHOMOLOGY OF QUADRATIC EXTENSIONS: FORMULAS AND NUMBER-THEORETIC EXAMPLES

RICHARD THOMAS BUMBY AND DAVID EARL DOBBS

Vol. 60, No. 1 September 1975

PACIFIC JOURNAL OF MATHEMATICS
Vol. 60, No. 1, 1975

AMITSUR COHOMOLOGY OF QUADRATIC EXTENSIONS: FORMULAS AND NUMBER-THEORETIC EXAMPLES

RICHARD T. BUMBY AND DAVID E. DOBBS

Computations of Amitsur cohomology (in the units functor U) for extensions of rings of algebraic integers have been achieved in two ways: via Mayer-Vietoris sequences (by Morris and Mandelberg) and via cohomology in the functor UK/U (by the second-named author). One of the goals of these computations has been to shed light on the Chase-Rosenberg homomorphism from Amitsur cohomology to the split Brauer group. In this paper we obtain, for quadratic ring extensions, formulas for cohomology in U and in UK/U, which have wider application than the corresponding work of Morris and Mandelberg. Our formulas lead to examples showing that the Chase-Rosenberg homomorphism, arising from a quadratic extension of rings of algebraic integers, need not be injective or surjective.

Our methods are direct and, in particular, avoid explicit use of Mayer-Vietoris sequences. Section 2 studies the embedding of certain Amitsur cochains in Cartesian products. Section 3 contains the cohomology computations which, together with [4, Corollary 1.5] and the Hasse norm principle of class field theory, lead to the desired examples in §4.

We employ the standard notation concerning Amitsur cohomology (cf. [1, p. 29]) and assume familiarity with [4, §1].

2. Cochain and coboundary computations.

The *standing hypotheses* for §§2 and 3 are that R is an integral domain with quotient field K, that S is a flat R-subalgebra of a quadratic (two-dimensional separable) field extension L of K, and that the Galois group G of L/K fixes S as a set.

Note that R-flatness of S allows us to view $S^i = \otimes_R^i S$ as an R-subalgebra of $L^i = \otimes_K^i L$. Since G maps S into itself, the explicit K-algebra isomorphism $L^i \to \Pi_{G^{i-1}} L$ given in [1, Lemma 5.1] may be used to identify S^i with a subring of $\Pi_{G^{i-1}} S$. Provided that S is taken to act on S^i by multiplication with the first tensor factor, this identification clearly holds as S-algebras.

Denote the action of the nonidentity element σ of G by $a \to a'$. It was shown in the proof of [4, Proposition 1.8] that the Amitsur coboundary d^1: $U(L^2) \to U(L^3)$, viewed as a homomorphism from $\Pi_G U(L)$ to $\Pi_{G^2} U(L)$, sends (a,b) to $(a,a,a',a^{-1}bb')$. (Observe that the indices of the above, and following, Cartesian products are subjected to lexicographic order, with $1 \leqq \sigma$.) A similar routine computation reveals that d^2: $U(L^3) \to U(L^4)$ sends (a,b,c,d) to

$$(1, ba^{-1}, 1, ab^{-1}, a'c^{-1}, b'c^{-1}, c'a^{-1}, d'd^{-1}b^{-1}c).$$

Inasmuch as these formulas also describe the coboundaries in the Amitsur complex $C(S/R, U)$, it becomes imperative to know which tuples in $\Pi_{G^{i-1}} U(S)$ arise from elements of $U(S^i)$, for $i = 2,3$. The next two propositions settle this issue.

First, we give a key definition. Let I be the ideal of S generated by $\{a - a' \colon a \in S\}$.

PROPOSITION. (i) $S^2 = \{(a,b) \in S \times S \colon a \equiv b(I)\}$.
(ii) $U(S^2) = [U(S) \times U(S)] \cap S^2$.

Proof. (i): Let $(a,b) \in S^2$; in other words, suppose that there exists $\xi = \Sigma \alpha_i \otimes \beta_i \in S^2$ such that $a = \Sigma \alpha_i \beta_i$ and $b = \Sigma \alpha_i \beta_i'$. If $m \colon L^2 \to L$ is the multiplication map, applying m and $m(1 \otimes \sigma)$ to ξ shows that S contains both a and b. It is clear that $a - b \in I$; i.e., $a \equiv b(I)$.

Conversely, let $(a,b) \in S \times S$ with $a \equiv b(I)$. Since $(a,b) = (a,a) + (0, b-a)$, it suffices to prove that S^2 contains both (a,a) and $\{0\} \times I$. For the former, observe that $(a,a) = a \otimes 1$. For the latter, our earlier remarks establish that S^2 is an S-submodule of $S \times S$, so that we need only to prove $(0, c - c') \in S^2$ for each $c \in S$. This, however, is immediate: $(0, c - c') = c \otimes 1 - 1 \otimes c$.

(ii): As the injection $S^2 \to S \times S$ is a ring homomorphism, it is clear that $U(S^2) \subset [U(S) \times U(S)] \cap S^2$. For the reverse inclusion, (i) reduces us to showing that, if a and b in $U(S)$ satisfy $a \equiv b(I)$, then $a^{-1} \equiv b^{-1}(I)$. As $a^{-1} - b^{-1} = a^{-1}b^{-1}(b-a)$, the proof is complete.

We pause to observe that the proof of part (i) of the preceding proposition was obtained by rendering basis-free Morris' proof of [7, Lemma 4.0]. The computational method used to establish (ii) replaces the Mayer-Vietoris argument of [7, Theorem 4.1].

PROPOSITION. (i) $S^3 = \{(a,b,c,d) \in S \times S \times S \times S \colon a \equiv b \equiv c(I), a + c \equiv b + d(I^2)\}$.
(ii) $U(S^3) = [U(S) \times U(S) \times U(S) \times U(S)] \cap S^3$.

Proof. (i): Let $(a,b,c,d) \in S^3$; i.e., suppose that $\xi = \Sigma \alpha_i \otimes \beta_i \otimes \gamma_i \in S^3$ satisfies $a = \Sigma \alpha_i \beta_i \gamma_i$, $b = \Sigma \alpha_i \beta_i \gamma_i'$, $c = \Sigma \alpha_i \beta_i' \gamma_i'$ and $d = \Sigma \alpha_i \beta_i' \gamma_i$. It is clear that $a \equiv b \equiv c(I)$. Moreover $a + c \equiv b + d(I^2)$ since $a - b + c - d = \Sigma \alpha_i (\beta_i - \beta_i')(\gamma_i - \gamma_i')$.

Conversely, if a,b,c,d in S satisfy $a \equiv b \equiv c(I)$ and $a + c \equiv b + d(I^2)$, note that

$$(a,b,c,d) = (a,a,a,a) + (0,0,c-a,c-a)$$
$$+ (0,b-a,0,a-b)$$
$$+ (0,0,0,-a+b-c+d).$$

Since $(a,a,a,a) = a \otimes 1 \otimes 1$ and S^3 is an S-submodule of $S \times S \times S \times S$, it suffices to prove that S^3 contains $(0,0,e-e',e-e')$, $(0,e-e',0,e'-e)$ and $(0,0,0,(e-e')(f-f'))$ for each e and f in S. To this end, we need only to consider $(e \otimes 1 - 1 \otimes e) \otimes 1$, $1 \otimes (e \otimes 1 - 1 \otimes e)$ and

$$(e \otimes 1 - 1 \otimes e) \otimes f - (f'e \otimes 1 - f' \otimes e) \otimes 1,$$

respectively.

(ii): By reasoning as in the preceding proposition, it suffices to show that, if $a,b,c,d \in U(S)$ satisfy $a \equiv b \equiv c(I)$ and $a + c \equiv b + d(I^2)$, then $a^{-1} + c^{-1} \equiv b^{-1} + d^{-1}(I^2)$. Taking congruences modulo I^2, we have

$$\begin{aligned} a^{-1} - b^{-1} + c^{-1} - d^{-1} &\equiv a^{-1}b^{-1}c^{-1}d^{-1}[bc(a-b+c) \\ &\quad - ac(a-b+c) + ab(a-b+c) - abc] \\ &= a^{-1}b^{-1}c^{-1}d^{-1}[-c(a-b)^2 - a(b-c)^2 \\ &\quad + b(c-a)^2] \\ &\equiv 0, \end{aligned}$$

to complete the proof.

3. Formulas for cohomology. It will be convenient to let N denote the field norm $N_{L/K}: U(L) \to U(K)$ and to view $H^1(S/R, UK/U)$ as a subgroup of $H^2(S/R, U)$ by means of the (injective) connecting homomorphism (cf. [**4**, p. 240], [**5**]). In conjunction with the standing hypotheses announced earlier, we now *assume* that S is not contained in K. This readily implies that the multiplication map $S \otimes_R K \to L$ is an isomorphism since $[L : K] = 2$.

THEOREM. *Let* $A = \{x \in U(S): x \equiv 1(I^2)\}$ *and* $B = \{x \in U(S): x \equiv 1(I)\}$. *Then*:

(i) $H^1(S/R, UK/U) \cong [N(U(L)) \cap A]/N(B)$.

(ii) $H^2(S/R, U) \cong [K \cap A]/N(B)$.

(iii) $H^2(S/R, U)/H^1(S/R, UK/U) \cong [K \cap A]/[N(U(L)) \cap A]$.

Proof. (i): As usual, the R-flatness of S and the isomorphism $S \otimes_R K \to L$ yield $C^n(S/R, UK/U) \cong U(L^{n+1})/U(S^{n+1})$. If $D =$

$\{\xi \in U(L^2): d^1(\xi) \in U(S^3)\}$, then the first cocycle group of $C(S/R, UK/U)$ is $\{\xi \cdot U(S^2): \xi \in D\}$, so that a standard isomorphism theorem implies $H^1(S/R, UK/U) \cong D/[d^0(U(L)) \cdot U(S^2)]$. Since N is given by $N(a) = aa'$, the material in §2 permits us to identify D with

$$\begin{aligned} E &= \{(a,b) \in U(L) \times U(L): a \in U(S), N(b) \in U(S), \\ &\qquad N(a) \equiv N(b) \times (I^2)\} \\ &= \{a(1,c) \in U(L) \times U(L): a \in U(S), c \in U(L), N(c) \in A\}. \end{aligned}$$

As d^0 is given by $d^0(v) = v^{-1} \otimes v$, Hilbert's Theorem 90 shows that $d^0(U(L))$ is regarded as $\{1\} \times \ker(N)$; the preceding identification of D with E then causes $d^0(U(L)) \cdot U(S^2)$ to be identified with

$$F = [\{1\} \times \ker(N)] \cdot \{a(1,c) \in U(S) \times U(S): c \in B\}.$$

Thus, $H^1(S/R, UK/U) \cong E/F$. Observe that the homomorphism $h: U(L) \times U(L) \to U(L) \times U(K)$, given by $h(x,y) = (x, N(yx^{-1}))$, carries E onto $U(S) \times [N(U(L)) \cap A]$ and F onto $U(S) \times N(B)$. Since $\ker(h) \subset F$, standard isomorphism theorems apply, and establish (i).

(ii): The material in section 2 allows us to describe the second cocycle and coboundary groups of $C(S/R, U)$, so that $H^2(S/R, U) \cong J/M$, where

$$\begin{aligned} J = \{(a, a, a', d) \in U(S) \times U(S) \times U(S) \times U(S): \\ a' \equiv d(I^2),\ d'd^{-1} = a(a')^{-1}\} \end{aligned}$$

and

$$\begin{aligned} M = \{(a, a, a', a^{-1}bb') \in U(S) \times U(S) \times U(S) \times U(S): \\ b \in U(S),\ a \equiv b(I)\}. \end{aligned}$$

Projection onto the last two coordinates is an isomorphism that identifies J with

$$\begin{aligned} P &= \{(a,d) \in U(S) \times U(S): a \equiv d(I^2),\ d'd^{-1} = a'a^{-1}\} \\ &= \{a(1,c) \in U(S) \times U(S): c' = c, c \equiv 1(I^2)\} \end{aligned}$$

and identifies M with

$$\begin{aligned} Q &= \{(a, (a')^{-1}bb') \in U(S) \times U(S): b \in U(S),\ a' \equiv b(I)\} \\ &= \{a(1, N(c)) \in U(S) \times U(S): c \in B\}. \end{aligned}$$

Thus, $H^2(S/R, U) \cong P/Q$. Since K is the fixed field of G, the isomorphism given by $(x,y) \to (x, yx^{-1})$ carries P onto $U(S) \times$

$(K \cap A)$. As Q is sent onto $U(S) \times N(B)$, isomorphism theorems apply again, and establish (ii).

(iii): It suffices to prove that the isomorphism in (i) is the restriction to $H^1(S/R, UK/U)$ of the isomorphism in (ii). Let $\xi = \Sigma\alpha_i \otimes \beta_i \in D$; set $a = \Sigma\alpha_i\beta_i$ and $b = \Sigma\alpha_i\beta_i'$. It is routine to check that the connecting homomorphism sends the $H^1(S/R, UK/U)$-cohomology class of ξ to the coset in J/M represented by $(a, a, a', a^{-1}bb')$. The map in (ii) then sends this coset (cohomology class) to the $N(B)$-coset represented by $N(ba^{-1})$. This is precisely the effect of the isomorphism in (i) on the cohomology class of ξ, and so the proof is complete.

REMARK. Suppose $U(S) \cap K \subset R$. If $W = \{x \in U(R): x \equiv 1(I^2)\}$, then the formulas in the preceeding theorem may be restated as $H^1(S/R, UK/U) \cong [N(U(L)) \cap W]/N(B)$, $H^2(S/R, U) \cong W/N(B)$, and $H^2(S/R, U)/H^1(S/R, UK/U) \cong W/[N(U(L)) \cap W]$. This formula for $H^2(S/R, U)$ was obtained by Mandelberg **[6**, Theorem 4.24] for the special case in which R is integrally closed, S is integral over R, $\mathrm{char}(K) \neq 2$, and there exists $a \in S$ such that S is R-free with basis $\{1, a\}$. As our work does not place restrictions on characteristic or bases, it applies to examples such as:

(i) $R = \mathbf{F}_2[t]$, $L =$ splitting field of $x^2 + x + 1$ over K;

(ii) $R = \mathbf{Z}[(-30)^{1/2}]$, $L = K(6^{1/2})$ for which **[6**, Theorem 4.24] cannot be used.

4. Number-theoretic examples. We fix *notation and assumptions* for the remarks and examples given below: L is a biquadratic field extension of $\mathbf{Q}$, R is the ring of algebraic integers of a quadratic subfield K of L, and S is a ring properly containing R and contained in the ring of algebraic integers of L. The standing hypotheses of §§2 and 3 hold in this context. We also define I as in §2, and let N, A and B be as in the theorem of §3. Note that I^2 may be interpreted as the discriminant ideal of S/R. Because of the explicit description of the algebraic integers in biquadratic fields given by Williams **[10]**, we will customarily leave to the reader, without further comment, verification of the values and basic properties of the ideals I^2 occurring in our examples. One such result, which occurs frequently in our examples, states: whenever $K = \mathbf{Q}(d^{1/2})$ and $L = K((d_1)^{1/2})$ and we write $d_1d_2 = dk^2$ with *discriminants* d, d_1, and d_2; then $I^2 = (k)$.

Since L/K is a quadratic extension of algebraic number fields, the expressions studied in §3 may be reinterpreted. The Hasse norm theorem **[8**, page 185] implies that an element $x \in K \cap A$ belongs to $N(U(L))$ precisely in case x is a local norm at all places. At a place of K which splits in L, all elements are norms. Moreover, x is a local norm at any place arising from an inertial prime, since norms are characterized as being of even order and $x \in A \subset U(S)$ has order zero. If p is a ramified prime of R, then $p \mid I^2$, and so $x \equiv 1(p)$; in case p does not lie over (2) in $\mathbf{Z}$, this congruence suffices to make x a local square, and thus a local norm. The ramified primes lying over (2) require further analysis. While $x \equiv 1(I^2)$ does suffice to show that x is a local norm in general, a discussion of the relevant local class field theory would lead us far afield. For application to our examples, however, we need only consider such primes in biquadratic extensions of $\mathbf{Q}$. This reduces the problem to computing the properties of a finite number of extensions of $\mathbf{Q}_2$. Hence we will not distinguish the primes dividing (2) from other primes. Finally, if an archimedean place does not split, we obtain an embedding of K in $\mathbf{R}$ with $\mathbf{R} \otimes_K L \cong \mathbf{C}$; at such a place, x is a local norm if and only if x is positive in $\mathbf{R}$. Thus, $x \in K \cap A$ belongs to $N(U(L))$ precisely when x is positive at each real place of K which does not split in L.

The exact sequence

$$0 \rightarrow H^1(S/R, UK/U) \rightarrow H^2(S/R, U) \xrightarrow{\rho} B(S/R)$$

was developed in [**4**, Corollary 1.5] in order to study the map ρ appearing in [**2**, Theorem 7.6]. Examples in which ρ is an isomorphism abound ([**2**, Corollary 7.7], [**3**, Corollary 4.2]); we shall use this sequence to give some examples for which ρ fails to be an isomorphism. Our examples include the first for which $H^2(S/R, U) \neq 0$. In addition, they are simpler than one might imagine in light of recent results of Mandelberg [**6**, Corollary 4.25 and Remark 4.26], in which $H^2(S/R, U)$ is shown to vanish for a wide range of quadratic extensions of rings of algebraic integers in imaginary quadratic fields.

Before presenting our examples, we pause to note that previous calculations showing $H^2(T/\mathbf{Z}, U) = 0$ for an order T in a quadratic extension of $\mathbf{Q}$([**7**, Theorems 3.0 and 3.2], [**4**, Proposition 1.9 and Remark 1.10(b)], [**6**, Theorem 4.27]) follow from the theorem in §3 and the observation that no discriminant divides 2. Indeed, no proper extension of $\mathbf{Z}$ has discriminant 1 [**9**, Proposition 3-7-15 and Theorem 5–4–10]. Moreover, no extension of $\mathbf{Z}$ has discriminant 2, because of the theorem of Stickelberger [**9**, Proposition 4–8–19], whose proof yields the statement: the discriminant of any finite extension of a principal ideal domain is congruent to a square modulo (4). We conjecture that the theorem in §3 generalizes to a class of higher-dimensional extensions, with "I^2" replaced by "the discriminant" in the definition of A; if so, the preceding argument implies $H^2(T/\mathbf{Z}, U) = 0$ for such extensions $T/\mathbf{Z}$.

EXAMPLE 1. This example treats various imaginary K. First, let K be either (i) $\mathbf{Q}((-30)^{1/2})$ or (ii) $\mathbf{Q}((-42)^{1/2})$; let $L = K((6)^{1/2})$. Then

$I^2 = (2)$ in (i) and $I^2 = (1)$ in (ii). For both cases, $K \cap A = \{\pm 1\}$ and $B = U(S) \subset \{\pm(5+2(6)^{1/2})^n : n \in \mathbf{Z}\}$. As $N(B) = \{1\}$, the formula in §3 implies that $H^2(S/R, U) \cong \mathbf{Z}/2\mathbf{Z}$. Since K has no real places, $H^1(S/R, UK/U) \cong \mathbf{Z}/2\mathbf{Z}$ also, and ρ is the zero map.

Next, let K be any imaginary quadratic algebraic number field other than $\mathbf{Q}((-3)^{1/2})$ and $\mathbf{Q}((-1)^{1/2})$. As $U(R) = \{\pm 1\}$, we find that $H^2(S/R, U)$ is nonzero (and, hence, isomorphic to $\mathbf{Z}/2\mathbf{Z}$) if and only if $N(B) = \{1\}$ and I^2 is either (1) or (2). One verifies from **[10]** that $I^2 = (1)$ when the discriminant d of K can be written as $d = d_1 d_2$, such that $L = K((d_1)^{1/2}) = \mathbf{Q}((d_1)^{1/2}, (d_2)^{1/2})$ and d_1, d_2 are each discriminants. Similarly, $I^2 = (2)$ arises from $4d = d_1 d_2$. In these cases, $U(S)$ is contained in the real quadratic subfield of L and, hence, is equal to B.

To fabricate examples, (including (i) and (ii) above), let d_1 be a positive square-free rational integer such that each unit of $\mathbf{Q}((d_1)^{1/2})$ has norm 1. (For instance, choose square-free positive d_1 divisible by a prime congruent to 3 modulo 4.) Then choose square-free negative $d_2 \in \mathbf{Z}$ such that $(d_1, d_2) = (1)$ and not both d_1, d_2 are congruent to 3 modulo 4. Set $K = \mathbf{Q}((d_1 d_2)^{1/2})$ and $L = K((d_1)^{1/2})$. The preceding work shows that $H^2(S/R, U) \cong \mathbf{Z}/2\mathbf{Z} \cong H^1(S/R, UK/U)$ and ρ is the zero map. Note that $I^2 = (2)$, so that L/K is ramified, if one of d_1, d_2 is even and the other is congruent to 3 modulo 4; in the remaining case, $I^2 = (1)$ and L/K is unramified.

If $K = \mathbf{Q}((-3)^{1/2})$, the general version of Stickelberger's theorem implies that $H^2(S/R, U) = 0$ for each quadratic extension S of R, since, by analogy with the case $R = \mathbf{Z}$, it shows that no difference of units could be divisible by a discriminant.

EXAMPLE 2. Let K be real and L complex. Then $K \cap A$ has the form $\{\pm \alpha^n : n \in \mathbf{Z}\}$ if $I^2 | (2)$; otherwise, $K \cap A = \{\alpha^n\}$. In either case, $N(U(L))$ does not contain -1 (since norms are totally positive) and $N(B)$ contains α^2. The possible cases are tabulated below.

	$K \cap A$	$N(U(L)) \cap A$	$N(B)$	$H^2(S/R, U)$	$H^1(S/R, UK/U)$
(a)	$\{\pm\alpha^n\}$	$\{\alpha^n\}$	$\{\alpha^n\}$	$\mathbf{Z}/2\mathbf{Z}$	0
(b)	$\{\pm\alpha^n\}$	$\{\alpha^n\}$	$\{\alpha^{2n}\}$	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z}$
(c)	$\{\pm\alpha^n\}$	$\{\alpha^{2n}\}$	$\{\alpha^{2n}\}$	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$	0
(d)	$\{\alpha^n\}$	$\{\alpha^n\}$	$\{\alpha^n\}$	0	0
(e)	$\{\alpha^n\}$	$\{\alpha^n\}$	$\{\alpha^{2n}\}$	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z}$
(f)	$\{\alpha^n\}$	$\{\alpha^{2n}\}$	$\{\alpha^{2n}\}$	$\mathbf{Z}/2\mathbf{Z}$	0

As $H^1(S/R, UK/U) = \ker(\rho)$ and the split Brauer group $B(S/R)$ is known to be $\mathbf{Z}/2\mathbf{Z}$, case (c) cannot arise. A direct proof of this will now be given. If case (c) holds, then $I^2|(2)$; moreover, neither α nor $-\alpha$ is totally positive, whence $N_{K/\mathbf{Q}}(\alpha) = -1$. As every odd divisor of the discriminant d of K is congruent to 1 modulo 4, d cannot be expressed as the product of two negative discriminants. Thus $I^2 = (2)$, and $R = \{a + b\underline{D}^{1/2}: a, b \in \mathbf{Z}\}$ for some $\underline{D} \equiv 2(4)$. If $\alpha = a + b\underline{D}^{1/2}$, then $N_{K/\mathbf{Q}}(\alpha) = -1$ implies that a and b are each odd; this contradicts $\alpha \equiv 1(I^2)$, thus proving (again) that case (c) cannot arise.

We now proceed to show that the other five cases do arise. First, examples giving (a) and (b) with $I^2 = (1)$ are (a) $K = \mathbf{Q}(6^{1/2})$, $L = K((-2)^{1/2})$ and (b) $K = \mathbf{Q}(3^{1/2})$, $L = K((-1)^{1/2})$. Whenever $I^2 = (1)$, we are in case (a) or (b); the difference is whether the extension L contains $(-\alpha)^{1/2}$ (case (a)) or not (case (b)). If $I^2 = (2)$, we must have $K = \mathbf{Q}(\underline{D}^{1/2})$ with $\underline{D} > 0$ and $\underline{D} \equiv 2(\text{mod } 4)$ and $L = K((\underline{D}_1)^{1/2})$ with $\underline{D}_1 | \underline{D}$, $\underline{D}_1 < 0$, and $\underline{D}_1 \equiv 3$ (mod 4). As in our analysis of case (c), a unit, β, with $N_{K/\mathbf{Q}}(\beta) = -1$ cannot belong to $K \cap A$. On the other hand, $\beta \in B$. Thus, when R contains such β, any L with $I^2 = (2)$ gives case (a). If R contains no such β, every unit belongs to A, and the test is as in the case of $I^2 = (1)$. Thus $K = \mathbf{Q}(10^{1/2})$, $L = K((-5)^{1/2})$ or $K((-1)^{1/2})$ gives (a) since $N_{K/\mathbf{Q}}(3 + 10^{1/2}) = -1$. If $K = \mathbf{Q}(34^{1/2})$, the fundamental unit is $35 + 6(34)^{1/2} = (18^{1/2} + 17^{1/2})^2$; then $L = K((-17)^{1/2})$ gives (a), while $L = K((-1)^{1/2})$ gives (b).

In constructing examples of (d), (e) and (f), we expect that R and S will have the same units (actually, if $I^2 \nmid 2$, any new units must be roots of unity). Case (d) then requires that there be units congruent to 1 modulo I but not modulo I^2, whose square is congruent to 1 modulo I^2. Some examples of (d) can be constructed with $I^2 = (4)$ if $K = \mathbf{Q}(\underline{D}^{1/2})$ with $\underline{D} > 0$, $\underline{D} \equiv 1$ (mod 4), when the fundamental unit of R has norm -1. In this case, there are units of norm -1 congruent to 1 modulo 2; these cannot be congruent to 1 modulo 4. To achieve $I^2 = (4)$, take $L = K((\underline{D}_1)^{1/2})$ with $\underline{D}_1 < 0$, $\underline{D}_1 | \underline{D}$, $\underline{D}_1 \equiv 3$ (mod 4) (e.g., $\underline{D}_1 = -1$). Thus we could take $K = \mathbf{Q}(5^{1/2})$, $L = K((-1)^{1/2})$. Here $B = \{(2 + (5)^{1/2})^n\}$ and $A = N(B) = \{(2 + (5)^{1/2})^{2n}\}$.

Another family of examples of (d) can be constructed as follows. Choose $\underline{D} > 0$, $\underline{D} \equiv 3$ (mod 4) with fundamental unit of $R = \mathbf{Z}[\underline{D}^{1/2}]$ denoted β where $\beta \equiv \underline{D}^{1/2}(\text{mod } 2)$ and $\beta > 0$ (e.g. $\underline{D} = 3$, $\beta = 2 + (3)^{1/2}$). Then $(\beta^{n+1} - \beta^{-n})/(\beta - 1)$ is an odd integer c_n such that $\beta^{2n+1} \equiv 1 \ (\text{mod } c_n)$. Take $L = K((-2c_n)^{1/2})$ which has $I^2 = (4c_n)$. Thus $B = \{\beta^{2(2n+1)k}\}$ and $A = N(B) = \{\beta^{4(2n+1)k}\}$. On the other hand, if $K = \mathbf{Q}((13 \cdot 17)^{1/2})$, case (d) cannot arise for any L (for any unit $\alpha \equiv 1$ (mod 2), $\alpha \equiv 1$ (mod 8)).

It is easy to give examples over any R for which $A = B$: e.g. by choosing odd factors of I^2 one can force the elements of B to be congruent to 1 modulo 8 and hence to belong to A. The generator, α, of A must have $N_{K/\mathbf{Q}}(\alpha) = +1$. Indeed, $\alpha \equiv 1$ (I^2) requires $\alpha' \equiv 1(I^2)$

since I^2 is a rational ideal, and $\alpha' = -\alpha^{-1}$ would require $2 \in I^2$. Both conjugates of α have the same sign: if positive, then (e); if negative, then (f). If $K = \mathbf{Q}(d^{1/2})$ and $L = \mathbf{Q}((d_1)^{1/2}, (d_2)^{1/2})$ where d, d_1, d_2 are discriminants and $d_1 d_2 = dk^2$, then $I^2 = (k)$, so one can easily find extensions having any value of I^2 which satisfies: (i) odd primes dividing d do not occur, (ii) other odd primes occur to at most the first power, (iii) 2 occurs to a power depending on the power of 2 occurring in d, d_1, and d_2 (at most the third power).

If the positive generator β of the units of R with norm 1 has odd order modulo any divisor of I^2, then the generator of A cannot be negative. This makes examples of case (e) easy to construct over any R. For example, if $R = \mathbf{Z}[2^{1/2}]$, $\beta = 3 + 2(2)^{1/2}$ has order 3 modulo 7. Taking $L = K((-7)^{1/2})$, $I^2 = (7)$, and hence $A = \{\beta^{3n}\} = A \cap N(U(L))$. This procedure produces examples over any real quadratic R for which the map ρ is neither a monomorphism nor an epimorphism.

To produce examples of (f) requires more care since we must find a possible value of I^2 arising from an L/K of this type modulo which $(-\beta)$ has odd order. To do this, consider the factors of $t_{2k+1} = (\beta^{k+1} + \beta^{-k})/(\beta + 1)$ or $t_{2k} = \beta^k + \beta^{-k}$ for possible values of I^2. If K is generated by the square root of a square-free positive *even* integer, 2 will occur to at most the first power in I^2; thus, there is no difficulty synthesizing examples of L from the t_n. If $R = \mathbf{Z}[2^{1/2}]$, $t_3 = 5$ and $t_2 = 6$. For $L = K((-3)^{1/2})$, $I^2 = (3)$ and $A = \{(-\beta)^{2n}\}$; for $L = K((-5)^{1/2})$, $I^2 = (10)$ and $\beta^3 = 99 + 70(2)^{1/2} \equiv -1(I^2)$, giving $A = \{(-\beta)^{3n}\}$. If $K = \mathbf{Q}(d^{1/2})$ with $d > 0$ and divisible by a prime of the form $4k - 1$, then every odd value of I^2 can be realized. Thus over $K = \mathbf{Q}(21^{1/2})$, the fundamental unit is $(5 + 21^{1/2})/2$, $t_2 = 5$, $t_3 = 4$, $t_4 = 23$, $t_5 = 19$. We can get $I^2 = (5)$, (23), or (19) from $L = K((-15)^{1/2})$, $K((-23)^{1/2})$, or $K((-19)^{1/2})$, respectively.

In the remaining cases, synthesis of examples may be required to follow a different route. To illustrate, consider $K = \mathbf{Q}(17^{1/2})$ for which $\beta = (4 + 17^{1/2})^2 = 33 + 8(17)^{1/2}$. Here $t_{2n} \equiv 2 \pmod 8$, $t_{2n+1} \equiv 1 \pmod 8$; hence one would have difficulty identifying any t_n which could be divisible by an admissible I^2. However, if q is any prime of the form $4k - 1$ which is also a quadratic non residue modulo 17, then: (i) q is an inertial prime of K; (ii) the units of R modulo q form a cyclic group of order $q^2 - 1$; (iii) the subgroup of elements of norm 1 has order $q + 1$; (iv) an element of the subgroup which is the square of an element not in the subgroup has order divisible by the largest power of 2 dividing $q + 1$, and has a power which is congruent to -1 modulo q; (v) thus q must divide some t_n. For this particular K, we may take $L = K((-q)^{1/2})$ where q is a prime congruent to 3, 7, 11, 23, 27, 31, 39, or 63 modulo 68. This procedure can be modified to cover those choices of R, whether or not they contain units of norm -1, whose discriminant over $\mathbf{Q}$ is divisible only by primes of the form $4k+1$. Over any real quadratic field K, one can give infinitely many choices of L which give (e) and infinitely many L which give (f).

The values of $H^2(S/R, U)$ given above exceed the bounds given by Mandelberg for special types of quadratic ring extensions [**6**, Corollary 4.25 and Remark 4.26]. On the other hand, they do sharpen the bound of $\prod_{i=1}^{8} (\mathbf{Z}/2\mathbf{Z})$ which follows from the bound on the cochain group given by Dobbs [**3**, Proposition 2.1]. We hope that our examples will serve to clarify the role of the units of finite order in the computation of Amitsur cohomology.

References

1. S. U. Chase, D. K. Harrison, and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Memoirs Amer. Math. Soc., No. 52 (Amer. Math. Soc., Providence, R. I., 1965).
2. S. U. Chase and A. Rosenberg, *Amitsur cohomology and the Brauer group*, Memoirs Amer. Math. Soc., No. 52 (Amer. Math. Soc., Providence, R. I., 1965).
3. D. E. Dobbs, *Amitsur cohomology of algebraic number rings*, Pacific J. Math., **39** (1971), 631–635.
4. ———, *On inflation and torsion of Amitsur cohomology*, Canad. J. Math., **24** (1972), 239–260.
5. ———, *Amitsur cohomology of cubic extensions of algebraic integers*, Israel J. Math., **14** (1973), 213–220.
6. K. I. Mandelberg, *Amitsur cohomology for certain extensions of rings of algebraic integers*, submitted for publication.
7. R. A. Morris, *On the Brauer group of* **Z**, Pacific J. Math., **39** (1971), 619–630.
8. J. T. Tate, *Global class field theory*, in Algebraic Number Theory, edited by J. W. S. Cassels and A. Frohlich (Thompson, Washington, D. C., 1967).
9. E. Weiss, *Algebraic Number Theory*, (McGraw-Hill, New York, 1963).
10. K. S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull., **13** (1970), 519–526.

Received May 9, 1974 and in revised form August 5, 1974. A major portion of the work done by the second author was done at the Number Theory Institute in Ann Arbor during the summer of 1973. We are grateful to the University of Michigan for its hospitality, and to the National Science Foundation for making possible the stimulating atmosphere of that Institute. The second-named author was supported in part by NSF Grant GP–28409A # 1.

Rutgers University

Vol. 60, No. 1 CONTENTS

Pacific Journal of Mathematics
Vol. 60, No. 1 September, 1975