PACIFIC JOURNAL OF MATHEMATICS
Vol. 59, No. 1, 1975

AMITSUR COHOMOLOGY FOR CERTAIN EXTENSIONS OF RINGS OF ALGEBRAIC INTEGERS

KENNETH I. MANDELBERG

The Amitsur cohomology groups $H^1(S/R, \mathrm{Pic})$ and $H^2(S/R, U)$ are computed in a number of cases where $R \subsetneqq S$ are rings of algebraic integers, with most specific results when R is Z and S is the ring of integers in a quadratic number field. These results give information about the Brauer group $\mathrm{Br}(S/R)$, which gives a new proof of its vanishing when $R = Z$ and S is in an infinite class of quadratic extensions.

0. Introduction. Let R be a commutative ring and S a commutative R-algebra. We will write $\mathrm{Br}(R)$ for the Brauer group of central separable R-algebras, and $\mathrm{Br}(S/R)$ for the subgroup of $\mathrm{Br}(R)$ consisting of those elements split by S [1, § 5]. When S is finitely generated and projective over R, [5, Theorem 7.6] yields an exact sequence including

$$(0.1) \qquad \cdots \longrightarrow H^2(S/R, U) \longrightarrow \mathrm{Br}(S/R) \longrightarrow H^1(S/R, \mathrm{Pic}) \longrightarrow H^3(S/R, U)$$

where the groups surrounding $\mathrm{Br}(S/R)$ are Amitsur cohomology groups as is defined in [5].

By using class field theory as in [8], it can be shown that $\mathrm{Br}(\boldsymbol{Z})$ is trivial. In [14], Morris reproves part of this result without the use of class field theory, by using the exact sequence (0.1). Specifically, he shows that $H^2(S/\boldsymbol{Z}, U)$ is trivial where S is the ring of integers in $\boldsymbol{Q}(\sqrt{m})$, for $m \in \boldsymbol{Z}$, and that $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ is trivial when $m = \pm 3$, -1, 2, or 5. In § 3 we extend this result by proving that $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ vanishes on an infinite class of quadratic extensions, and fails to vanish on yet another infinite class. This simultaneously proves $\mathrm{Br}(S/\boldsymbol{Z})$ is trivial for more quadratic extensions S, and demonstrates the difficulty of using sequence (0.1) for further demonstration of this fact.

In § 1 we state the Mayer-Vietoris sequence and prove some related technical lemmas. These are used in § 2 to characterize the group $H^1(S/R, \mathrm{Pic})$ in terms of the units of certain R-algebras related to S. In § 4, by a comparison with Galois cohomology we calculate $H^2(S/R, U)$ in a number of cases where R and S are integral domains and the quotient field of S is a cyclic Galois extension of the quotient field of R.

All unexplained notation can be found in [5], however we recall some frequently used notation. If S is a commutative algebra over a commutative ring R, S^n denotes the R-algebra $S \otimes S \otimes \cdots \otimes S$ (n factors) where $\otimes$ denotes $\otimes_R$. If $0 \leqq i \leqq n$, we will write $\varepsilon_i\colon S^n \to S^{n+1}$ for the R-algebra homomorphism given by

$$s_0 \otimes s_1 \otimes \cdots \otimes s_{n-1} \longmapsto s_0 \otimes s_1 \otimes \cdots \otimes s_{i-1} \otimes 1 \otimes s_i \otimes \cdots \otimes s_{n-1} .$$

We will use U and Pic to denote the functors which assign to each commutative R-algebra its multiplicative group of units, and projective class group [3, II, § 5.4] respectively.

1. The Mayer-Vietoris sequences.

Let

$$\begin{tikzcd} A \arrow[r, "h_2"] \arrow[d, "h_1"'] & B_2 \arrow[d, "f_2"] \\ B_1 \arrow[r, "f_1"] & C \end{tikzcd} \tag{1.1}$$

be a commutative diagram of commutative rings and ring homomorphisms. We say that square (1.1) is cartesian, if for each (b_1, b_2) in $B_1 \times B_2$ with $f_1(b_1) = f_2(b_2)$, there is a unique element a of A with $(b_1, b_2) = (h_1(a), h_2(a))$. Put another way, the square is cartesian if the sequence $0 \to A \xrightarrow{h_1 \times h_2} B_1 \times B_2 \xrightarrow{f_1 - f_2} C$ of abelian groups is exact.

DEFINITION 1.2. If c is a unit of C, we will write M_c for the subgroup $\{(b_1, b_2) \text{ in } B_1 \times B_2 \mid cf_1(b_1) = f_2(b_2)\}$ of $B_1 \times B_2$ endowed with the A-module structure: $a \cdot (b_1, b_2) = (h_1(a)b_1, h_2(a)b_2)$. In the case that (1.1) is cartesian, and either f_1 of f_2 is surjective [13, Theorem 2.1, p. 20] implies that M_c is a finitely generated projective A-module.

In our notation, with the mappings explicitly formulated [2, Theorem 5.3, p. 481, and Theorem 4.3, p. 464] specializes to:

THEOREM 1.3. *Suppose diagram* (1.1) *is cartesian and either* f_1 *or* f_2 *is surjective. Then there is an exact sequence*:

$$U(B_1) \times U(B_2) \xrightarrow{\delta} U(C) \xrightarrow{\mu} \operatorname{Pic}(A) \xrightarrow{\lambda} \operatorname{Pic} B_1 \times \operatorname{Pic} B_2$$

where the maps are defined as follows:

(1) $\delta(b_1, b_2) = f_1(b_1)f_2(b_2^{-1})$, *where* b_1 *and* b_2 *are units in* B_1 *and* B_2 *respectively.*

(2) $\lambda(\text{class } M) = (\text{class } (M \otimes_A B_1), \text{ class } (M \otimes_A B_2))$, *where* M *is a projective* A*-module of rank one representing a class of* Pic A.

(3) $\mu(c) = \text{class } (M_c)$ *where* c *is a unit in* C.

The sequence is natural with respect to cartesian squares of rings satisfying the hypotheses.

COROLLARY 1.4. *Let R be a commutative ring, and suppose diagram* (1.1) *is a cartesian square of commutative R-algebras and R-algebra homomorphisms. Then, if S is a commutative R-algebra which is flat over R, the square*

$$\begin{array}{ccc} A \otimes S & \xrightarrow{h_2 \otimes id} & B_2 \otimes S \\ {\scriptstyle h_1 \otimes id}\big\downarrow & & \big\downarrow{\scriptstyle f_2 \otimes id} \\ B_1 \otimes S & \longrightarrow & C \otimes S \end{array}$$

is also cartesian. If in addition f_1 or f_2 is surjective then the diagram

$$\begin{array}{ccccccc} U(B_1) \times U(B_2) & \longrightarrow & U(C) & \longrightarrow & \operatorname{Pic} A & \longrightarrow & \operatorname{Pic} B_1 \times \operatorname{Pic} B_2 \\ \big\downarrow & & \big\downarrow & & \big\downarrow & & \big\downarrow \\ U(B_1 \otimes S) \times U(B_2 \otimes S) & \longrightarrow & U(C \otimes S) & \longrightarrow & \operatorname{Pic}(A \otimes S) & \longrightarrow & \operatorname{Pic}(B_1 \otimes S) \times \operatorname{Pic}(B_2 \otimes S) \end{array} \tag{1.5}$$

is commutative, where the rows are the exact sequences from Theorem 1.3, *and the vertical maps are the natural ones induced by the canonical R-algebra homomorphisms $A \to A \otimes S$, $B_1 \to B_1 \otimes S$, $B_2 \to B_2 \otimes S$, and $C \to C \otimes S$. Here $\otimes$ means $\otimes_R$.*

Proof. The right exactness of the tensor product implies that if $B_i \xrightarrow{f_i} C \to 0$ is exact, so is $B_i \otimes S \xrightarrow{f_i \otimes id} C \otimes S \to 0$. Hence by Theorem 1.3, we shall have proved Corollary 1.4 completely once the first part is proved.

Thus, by the definition of cartesian, what we must show is that the exactness of the sequence $0 \to A \xrightarrow{h_1 \times h_1} B_1 \times B_2 \xrightarrow{f_1 - f_2} C$, implies the exactness of

$$0 \to A \otimes S \xrightarrow{(h_1 \otimes id) \times (h_2 \otimes id)} (B_1 \otimes S) \times (B_2 \otimes S) \xrightarrow{(f_1 \otimes id) - (f_2 \otimes id)} C \otimes S.$$

But using the natural isomorphism $(B_1 \otimes S) \times (B_2 \otimes S) \cong (B_1 \times B_2) \otimes S$, the conclusion follows from the flatness of S.

REMARK 1.6. Suppose $B_1 = B_2 = B$ and $f_1 = f_2 = f$ in Corollary 1.4. Then, since $f_1(U(B_1)) \cdot f_2(U(B_2))^{-1} = f(U(B))$, diagram (1.5) can be replaced with

$$\begin{array}{ccccccc} U(B) & \longrightarrow & U(C) & \longrightarrow & \operatorname{Pic} A & \longrightarrow & \operatorname{Pic} B \times \operatorname{Pic} B \\ \big\downarrow & & \big\downarrow & & \big\downarrow & & \big\downarrow \\ U(B \otimes S) & \longrightarrow & U(C \otimes S) & \longrightarrow & \operatorname{Pic}(A \otimes S) & \longrightarrow & \operatorname{Pic}(B \otimes S) \times \operatorname{Pic}(B \otimes S) \end{array}$$

without destroying exactness (or commutativity).

Since μ in Theorem 1.3 is a group homomorphism, we can conclude that $M_{c_1} \otimes_A M_{c_2} \cong M_{c_1 c_2}$ when c_1 and c_2 are units of C. The next lemma, however, provides an explicit isomorphism.

LEMMA 1.7. *Let*

$$\begin{array}{ccc} A & \xrightarrow{h_2} & B \\ {\scriptstyle h_1}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow{f} & C \end{array}$$

be a cartesian square of commutative rings with f a surjection, and let c_1 and c_2 be units of C. Then $\sigma\colon M_{c_1} \otimes_A M_{c_2} \to M_{c_1 c_2}$, defined by $\sigma((x, y) \otimes (u, v)) = (xu, yv)$, on a generator $(x, y) \otimes_A (u, v)$ of $M_{c_1} \otimes M_{c_2}$, is an A-module isomorphism. The inverse of σ is given by $\tau\colon M_{c_1 c_2} \to M_{c_1} \otimes_A M_{c_2}$ defined by $\tau((s, t)) = (bs, t) \otimes (b', 1) + (s, b't) \otimes (1 - bb', 0)$, where b and b' are fixed elements of B with $f(b) = c_2$ and $f(b') = c_2^{-1}$.

Proof. By direct calculation it is easy to check that σ and τ are well defined, and $\sigma \circ \tau$ is the identity. The proof that $\tau \circ \sigma$ is the identity is only slightly harder, but does depend on the fact that the square is cartesian. For suppose (x, y) is in M_{c_1} and (u, v) is in M_{c_2}. Then $\tau \circ \sigma((x, y) \otimes (u, v)) = \tau(xu, yv) = (bxu, yv) \otimes (b', 1) + (xu, b'yv) \otimes (1 - bb', 0)$. But $f(v) = c_2 f(u) = f(bu)$, hence from the hypothesis that the square is cartesian, we obtain $v = h_2(a)$ and $bu = h_1(a)$ for an element a of A. Therefore, $(bxu, yv) \otimes (b', 1) = a \cdot (x, y) \otimes (b', 1) = (x, y) \otimes a \cdot (b', 1) = (x, y) \otimes (bub', v)$. For the same reason $(xu, b'yv) \otimes (1 - bb', 0) = (x, y) \otimes (u(1 - bb'), 0)$. Thus $\tau \circ \sigma((x, y) \otimes (u, v)) = (x, y) \otimes (bub', v) + (x, y) \otimes (u(1 - bb'), 0) = (x, y) \otimes (u, v)$, completing the proof.

We conclude the section with one more technical lemma. The sequence in Theorem 1.3 tells us that if M is a projective rank one A-module with $M \otimes_A B_i \cong B_i$ as B_i-modules, $i = 1, 2$, then $M \cong M_c$ for some c of C. Lemma 1.8 tells us how to actually produce this unit.

LEMMA 1.8. *Let diagram* (1.1) *be a cartesian square of commutative rings where either f_1 or f_2 is surjective. Further suppose that M is a projective A-module of rank one and ϕ_i is an isomorphism of $M \otimes_A B_i \to B_i$, for $i = 1, 2$. Then $M \cong M_c$ where c is the unit of C corresponding to the automorphism*:

$$C \cong B_1 \otimes_{B_1} C \xrightarrow{(\phi_1 \otimes id)^{-1}} M \otimes_A B_1 \otimes_{B_1} C \xrightarrow{r} M \otimes_A B_2 \otimes_{B_2} C \xrightarrow{\phi_2 \otimes id} B_2 \otimes_{B_2} C \cong C$$

where $\gamma\colon M \otimes_A B_1 \otimes_{B_1} C \xrightarrow{\sim} M \otimes_A B_2 \otimes_{B_2} C$ *is the isomorphism provided by the commutativity of the cartesian square,* i.e., $\gamma(m \otimes b_1 \otimes c) = m \otimes 1 \otimes f_1(b_1)c$ *where* m *is in* M, b_1 *is in* B_1, *and* c *is in* C.

Proof. By [13, Theorem 2.2, p. 20], M is isomorphic to the A-submodule,

$$\{(\sum m_{i_1} \otimes b_{i_1}, \sum m_{i_2} \otimes b_{i_2}) \text{ in } (M \otimes_A B_1) \times (M \otimes_A B_2) \mid \gamma(\sum m_{i_1} \otimes b_{i_1} \otimes 1_C) = \sum m_{i_2} \otimes b_{i_2} \otimes 1_C\}$$

of $(M \otimes B_1) \times (M \otimes B_2)$. Applying the A-module isomorphisms h_1 and h_2 to the first and second coordinates respectively, we obtain $M \cong \{(h_1(\sum m_{i_1} \otimes b_{i_1}), h_2(\sum m_{i_2} \otimes b_{i_2})) \mid \sum m_{i_j} \otimes b_{i_j}$ is in $M \otimes_A B_j$ for $j = 1, 2$, and $\gamma(\sum m_{i_1} \otimes b_{i_1} \otimes 1_C) = \sum m_{i_2} \otimes b_{i_2} \otimes 1_C\} = \{(b_1, b_2)$ in $B_1 \times B_2 \mid \gamma(h_1^{-1}(b_1) \otimes 1_C) = h_2^{-1}(b_2) \otimes 1_C\}$. Rewriting this we obtain

$$M \cong \{(b_1, b_2) \text{ in } B_1 \times B_2 \mid (h_2 \otimes id)\circ\gamma\circ(h_1^{-1} \otimes id)(b_1 \otimes 1_C) = b_2 \otimes 1_C\}\ .$$

But by definition the unit c corresponds to the automorphism

$$C \xrightarrow{\sim} B_1 \otimes_{B_1} C \xrightarrow{(h_2\otimes id)\circ\gamma\circ(h_1^{-1}\otimes id)} B_2 \otimes_{B_2} C \xrightarrow{\sim} C, \text{ thus } M \cong M_C\ .$$

2. $H^1(S/R, \text{Pic})$. Let R be an integral domain whose quotient field K has characteristic different from 2. Let S be an integral quadratic extension of R, that is $S \cong R[x]/(p(x))$ where $p(x) = x^2 + ax + b$ is a polynominal in $R[x]$ which is irreducible over K. Since $(p(x))$ is a prime ideal, S is an integral domain. We will fix a root ρ of $p(x)$ in S, noting that $S = R[\rho]$. Then $\bar\rho = -\rho - a$ is the other root of $p(x)$, which clearly lies in S. The only nontrivial R-automorphism of S is the one that takes ρ to $\bar\rho$. We denote this automorphism either by j, or simply by placing a bar over the appropriate symbol. We will write G for the group $\{id, j\}$ of R-automorphisms of S. The quotient ring $S/(\rho - \bar\rho)S$ will be denoted S', with $\pi\colon S \to S'$, the natural projection map.

The unlabeled $\otimes$ will be understood as $\otimes_R$. We will write $\alpha_1\colon S \otimes S \to S$ for the contraction mapping $\alpha_1(s \otimes t) = st$. $\alpha_2\colon S \otimes S \to S$ will denote the composition $\alpha_1 \circ (j \otimes id)$. It will not be unusual in what follows for a ring to be considered an algebra in several different ways. Therefore, if the ring B is to be considered as an algebra over a commutative ring A by $f\colon A \to B$, we will denote it by B_f.

In [14] Morris uses the Mayer-Vietoris sequence to describe Pic (S^2) in terms of $U(S)$ and $U(S')$. In this section we carry this technique a step further to describe $H^1(S/R, \text{Pic})$ in terms of $U(S)$, $U(S')$, $U(S' \otimes S)$, and $U(S \otimes S)$ in the case that Pic S is finite and (Pic $S)G = \{1\}$.

REMARK 2.1. Suppose R is the ring of integers in an algebraic number field K, with the class number of R equal to 1. As noted in [14, Remark, p. 625] the ring of integers S in a quadratic extension L of K is of the form $R[\rho]$ mentioned above. Since S is a Dedekind domain, $\operatorname{Pic} S$ is isomorphic to the ideal class group of S and is then finite by [16, Theorem 5-3-11, p. 207]. If I is an ideal of S, then $I \otimes_S S_j \cong j(I)$. Therefore, since every class of $\operatorname{Pic} S$ is represented by an ideal of S, j acts on $\operatorname{Pic} S$ by merely applying j to a representative ideal. By [12, Corollary 3, p. 21] for any ideal I of S, $I \cdot j(I) = PS$ for some ideal P of R, hence $I \cdot j(I)$ is principal. Thus in $\operatorname{Pic} S$, $\operatorname{class}(j(I)) = (\operatorname{class}(I))^{-1}$, and class (I) is of order 2 iff class (I) is in $(\operatorname{Pic} S)^G$. Hence, for this choice of S, the hypothesis $(\operatorname{Pic} S)^G = \{1\}$ is equivalent to the class number of S being odd.

We will use the notation S^n and ε_i as defined in §0.

LEMMA 2.2. *The square*

$$\begin{array}{ccc} S \otimes S & \xrightarrow{\alpha_2} & S \\ {\scriptstyle\alpha_1}\downarrow & & \downarrow{\scriptstyle\pi} \\ S & \xrightarrow{\pi} & S' \end{array}$$

is cartesian. Tensoring the square on the right with S over R induces the commutative diagram

$$\begin{array}{ccccccc} U(S) & \longrightarrow & U(S') & \longrightarrow & \operatorname{Pic} S^2 & \longrightarrow & \operatorname{Pic} S \times \operatorname{Pic} S \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ U(S^2) & \longrightarrow & U(S' \otimes S) & \longrightarrow & \operatorname{Pic} S^3 & \longrightarrow & \operatorname{Pic} S^2 \times \operatorname{Pic} S^2 \end{array}$$

with exact rows, described in Corollary 1.4 *and Remark* 1.6. *The vertical maps are the natural ones obtained from tensoring on the right with S, e.g.,* $\operatorname{Pic} S^2 \to \operatorname{Pic} S^3$ *by* $\operatorname{Pic}(\varepsilon_2)$.

Proof. That the square is cartesian is [14, Lemma 4.0, p. 625]. Then since S is a free and hence flat R-module, the second assertion follows from Corollary 1.4 and Remark 1.6.

REMARK 2.3. By Definition 1.2, the $S \otimes S$ module $M_1 = \{(s, t)$ in $S \times S \mid \pi(s) = \pi(t)\}$. We will write θ for the $S \otimes S$ module homomorphism $\theta: S \otimes S \to M_1$ defined by $\theta(s \otimes t) = (st, \bar{s}t)$. Since the square in Lemma 2.2 is cartesian, θ is an isomorphism. At times it will be more convenient to work with M_1 than $S \otimes S$, thus we note that θ induces a ring structure on M_1, under which θ becomes a ring homomorphism. An easy computation shows that this ring multiplication on M_1 is given by componentwise multiplication.

DEFINITION 2.4. Let M be an $S \otimes S$ module. We will write M^* for the set $\{m^* \mid m \in M\}$ made into an $S \otimes S$ module by: $m^* + n^* = (m + n)^*$ for m, n in M, and $x \cdot m^* = ((j \otimes id)(x) \cdot m)^*$ for x in $S \otimes S$ and m in M. For later use we note that $S^2_{j \otimes id} \otimes_{S^2} M$ is isomorphic to M^*, where the isomorphism takes $1 \otimes m$ to m^*, for m in M.

If A is a commutative ring and M is a projective A-module of rank one, we will denote its class in $\operatorname{Pic} A$ by $[M]$. If the ring A is not clear from context we will write $[M]_A$.

LEMMA 2.5. *If a is a unit of S', then the map $T\colon (M_a)^* \to M_{a^{-1}}$ defined by $T((s, t)^*) = (t, s)$ is an $S \otimes S$ module isomorphism. Consequently $[M_a^*] = [M_a]^{-1}$.*

Proof. If (s, t) is in M_a, $a\pi(s) = \pi(t)$, hence $a^{-1}\pi(t) = \pi(s)$ which implies (t, s) is in $M_{a^{-1}}$. Thus the codomain of T is as claimed. Since T has an obvious set theoretic inverse and is clearly additive, we only need show it is $S \otimes S$ linear. But if x is in $S \otimes S$:

$$\begin{aligned} T(x \cdot (s, t)^*) &= T((j \otimes id)(x) \cdot (s, t)^*) \\ &= T(\alpha_1 \circ (j \otimes id)(x) \cdot s,\ \alpha_2 \circ (j \otimes id)(x) \cdot t^*) \\ &= T((\alpha_2(x) \cdot s,\ \alpha_1(x) \cdot t)^*) = (\alpha_1(x) \cdot t,\ \alpha_2(x) \cdot s) \\ &= x \cdot (t, s) = x \cdot T((s, t)^*)\ . \end{aligned}$$

The final assertion follows from the first and Lemma 1.7.

If H is an abelian group, we will write $(H)_2$ for the subgroup of H consisting of those elements whose order divides 2.

REMARK 2.6. Recall that in Lemma 2.1 the maps $\lambda_1\colon \operatorname{Pic} S^2 \to \operatorname{Pic} S \times \operatorname{Pic} S$ and $\lambda_2\colon \operatorname{Pic} S^3 \to \operatorname{Pic} S^2 \times \operatorname{Pic} S^2$ are given by $\lambda_1([M]_{S^2}) = ((\operatorname{Pic} \alpha_1)([M]), (\operatorname{Pic} \alpha_2)([M]))$ and $\lambda_2([N]_{S^3}) = ((\operatorname{Pic} \alpha_1 \otimes id)([N]), (\operatorname{Pic} \alpha_2 \otimes id)([N]))$ by Theorem 1.3.

LEMMA 2.7. *Let $d^1 = (\operatorname{Pic} \varepsilon_0)(\operatorname{Pic} \varepsilon_1)^{-1}(\operatorname{Pic} \varepsilon_2)\colon \operatorname{Pic} S^2 \to \operatorname{Pic} S^3$ be the Amitsur 1-coboundary map for the complex $C(S/R, \operatorname{Pic})$ (defined in [5]). Then if we compose λ_2 with d^1, yielding a map $\operatorname{Pic} S^2 \to \operatorname{Pic} S^2 \times \operatorname{Pic} S^2$, it follows that $(\mu_1(U(S')))_2 = \operatorname{Ker} (\lambda_2 \circ d^1) \cap \mu_1(U(S'))$.*

Proof. Let $[M]$ in $\operatorname{Pic} S^2$ be in $\mu_1(U(S'))$. We must show that $\lambda_2 \circ d^1([M]) = 1$ iff $[M]$ has order 2 in $\operatorname{Pic} S^2$. Now,

$$\begin{aligned}\lambda_2\circ d^1([M]) &= \lambda_2(\mathrm{Pic}\ \varepsilon_0([M])\cdot\mathrm{Pic}\ \varepsilon_1([M]^{-1})\cdot\mathrm{Pic}\ \varepsilon_2([M]))\\ &= \lambda_2\circ\mathrm{Pic}\ \varepsilon_0([M])\cdot\lambda_2\circ\mathrm{Pic}\ \varepsilon_1([M]^{-1})\cdot\lambda_2\circ\mathrm{Pic}\ \varepsilon_2([M])\ ,\end{aligned}$$

since λ_2 is a group homomorphism. But in Lemma 2.2 $\mathrm{Pic}\,\varepsilon_2$ is the vertical map from $\mathrm{Pic}\,S^2 \to \mathrm{Pic}\,S^3$, hence $\lambda_2\circ\mathrm{Pic}\,\varepsilon_2\circ\mu_1$ is trivial by the commutativity and exactness of that diagram. Therefore, by Remark 2.6,

$$\begin{aligned}\lambda_2\circ d_1([M]) &= \lambda_2\circ\mathrm{Pic}\ \varepsilon_0([M])\cdot\lambda_2\circ\mathrm{Pic}\ \varepsilon_1([M]^{-1})\\ &= (\mathrm{Pic}\ ((\alpha_1\otimes id)\circ\varepsilon_0)([M])\cdot\mathrm{Pic}\ ((\alpha_1\otimes id)\circ\varepsilon_1)([M]^{-1})\ ,\\ &\qquad \mathrm{Pic}\ ((\alpha_2\otimes id)\circ\varepsilon_0)([M])\cdot\mathrm{Pic}\ ((\alpha_2\otimes id)\circ\varepsilon_1)([M]^{-1}))\ .\end{aligned}$$

But by direct computation, $(\alpha_1\otimes id)\circ\varepsilon_0 = (\alpha_1\otimes id)\circ\varepsilon_1 = (\alpha_2\otimes id)\circ\varepsilon_0 =$ identity, and $(\alpha_2\otimes id)\circ\varepsilon_1 = j\otimes id$, hence $\lambda_2\circ d^1([M]) = ([M]\cdot[M]^{-1}, [M][M^*]^{-1})$. Then by Lemma 2.5 $\lambda_2\circ d^1([M]) = (1, [M]^2)$, which is just what we were to have proved.

LEMMA 2.8. *If* $\mathrm{Pic}\,S$ *is finite and* $(\mathrm{Pic}\,S)^G = \{1\}$ *then* $H^1(S/R, \mathrm{Pic})$ *is isomorphic to* $\mu_1(U(S'))\cap\mathrm{Ker}\,d^1$.

Proof. Let $f\colon \mu_1(U(S'))\cap\mathrm{Ker}\,d^1 \to \mathrm{Ker}\,d^1/d^0(\mathrm{Pic}\,S) = H^1(S/R, \mathrm{Pic})$ by the restriction of the natural projection. We will show that f is bijective.

Consider the composite homomorphism $\lambda_1 d^0\colon \mathrm{Pic}\,S\to\mathrm{Pic}\,S^2\to\mathrm{Pic}\,S\times\mathrm{Pic}\,S$. If $[M]$ is in $\mathrm{Pic}\,S$, $\lambda_1 d^0([M]) = (\mathrm{Pic}(\alpha_1\circ\varepsilon_0)([M])\cdot\mathrm{Pic}(\alpha_1\circ\varepsilon_1)([M]^{-1}), \mathrm{Pic}\,(\alpha_2\circ\varepsilon_0)([M])\cdot\mathrm{Pic}\,(\alpha_2\circ\varepsilon_1)([M]^{-1}))$. But by direct computation $\alpha_1\circ\varepsilon_0 = \alpha_1\circ\varepsilon_1 = \alpha_2\circ\varepsilon_0 =$ identity and $\alpha_2\circ\varepsilon_1 = j$, thus $\lambda_1 d^0([M]) = ([M]\cdot[M]^{-1}, [M]\cdot\mathrm{Pic}\,j([M]^{-1})) = (1, [M]\cdot\mathrm{Pic}\,j([M]^{-1}))$. Thus for $[M]$ to be in $\mathrm{Ker}\,\lambda_1 d^0$ it must be in $(\mathrm{Pic}\,S)^G$. Hence, by the assumption $(\mathrm{Pic}\,S)^G = \{1\}$ we obtain that $\lambda_1 d^0$ is injective. Furthermore, if we denote by p_2 the map $\mathrm{Pic}\,S\times\mathrm{Pic}\,S\to\mathrm{Pic}\,S$ obtained by projecting onto the second factor, then $p_2\circ\lambda_1\circ d^0\colon \mathrm{Pic}\,S\to\mathrm{Pic}\,S$ is an injection by the explicit form of $\lambda_1\circ d^0$. Then since $\mathrm{Pic}\,S$ is finite, it follows that $p_2\circ\lambda_1\circ d^0$ is actually an isomorphism.

To prove that f is injective, we notice that $d^0(\mathrm{Pic}\,S)\subset\mathrm{Ker}\,d^1$ which implies $\mathrm{Ker}\,f = \mu_1(U(S'))\cap d^0(\mathrm{Pic}\,S)$. But then by Lemma 2.2 we obtain $\mu_1(U(S')) = \mathrm{Ker}\,\lambda_1$, hence

$$\mathrm{Ker}\,f = \lambda_1\cap d^0(\mathrm{Pic}\ S) = d^0\circ(\mathrm{Ker}\ (\lambda_1\circ d^0))\ .$$

Therefore, since we have proved $\lambda_1\circ d^0$ is injective, it follows that f is injective.

Finally, we will show that f is surjective. Let $[N]_{S^2}$ be any element of $\mathrm{Ker}\,d^1$. That is $\mathrm{Pic}\,\varepsilon_0([N])\cdot\mathrm{Pic}\,\varepsilon_1([N]^{-1})\cdot\mathrm{Pic}\,\varepsilon_2([N]) = 1$. We define $E\colon S^3\to S$ by $E(s\otimes t\otimes u) = stu$. Then since $\mathrm{Pic}\,E\colon \mathrm{Pic}\,S^3\to\mathrm{Pic}\,S$ is a group homomorphism and $\mathrm{Pic}\,(E\circ\varepsilon_i) = \mathrm{Pic}\,E\circ\mathrm{Pic}\,\varepsilon_i$, it follows that $\mathrm{Pic}\,(E\circ\varepsilon_0)([N])\cdot\mathrm{Pic}\,(E\circ\varepsilon_1)([N]^{-1})\cdot\mathrm{Pic}\,(E\circ\varepsilon_2)([N]) = 1$. But $E\circ\varepsilon_0 = E\circ\varepsilon_1 = E\circ\varepsilon_2 = \alpha_1$, thus $\mathrm{Pic}\,\alpha_1([N]) = 1$. Therefore, since $\lambda_1([N]) = (\mathrm{Pic}\,\alpha_1([N]), \mathrm{Pic}\,\alpha_2([N]))$ by Remark 2.6, it follows that $\lambda_1([N]) = (1, [Q])$ for some $[Q]$ in $\mathrm{Pic}\,S$. But $p_2\circ\lambda_1\circ d^0$ is an isomorphism, hence $[Q] = p_2\circ\lambda_1\circ d^0([M])$ for some $[M]$ in $\mathrm{Pic}\,S$, so $\lambda_1([N]) = \lambda_1 d^0([M])$. This implies that $[N]\cdot(d^0([M]))^{-1}$ is in $\mathrm{Ker}\,\lambda_1 = \mu_1(U(S'))$. But $[N]$ and $[N](d^0([M]))^{-1}$ are in the same class of $H^1(S/R, \mathrm{Pic})$, thus the class of $[N]$ is in the image of f. Since $[N]$ was arbitrary, f is surjective.

COROLLARY 2.9. *There is a unique group homomorphism* $(d^1)'$ *which makes the diagram*

$$\begin{tikzcd} & & (\mu_1(U(S')))_2 \arrow[dl, dashed, "(d^1)'"'] \arrow[d, "d^1"] & \\ 0 \arrow[r] & \dfrac{U(S'\otimes S)}{\mathrm{im}\,U(S\otimes S)} \arrow[r, "\mu_2'"] & \mathrm{Pic}\,S^3 \arrow[r, "\lambda_2"] & \mathrm{Pic}\,S^2 \end{tikzcd}$$

commute, where μ_2' *is the injection obtained by factoring out the kernel of* μ_2.

If $\mathrm{Pic}\,S$ *is finite and* $(\mathrm{Pic}\,S)^G = \{1\}$ *then*

$$H^1(S/R, \mathrm{Pic}) \cong \mathrm{Kernel}\left(\frac{U(S')}{\mathrm{im}\,U(S)}\right)_2 \xrightarrow{(d^1)'\circ\mu_1'} \frac{U(S'\otimes S)}{\mathrm{im}\,U(S\otimes S)}$$

where μ_1' *is the restriction to* $(U(S')/\mathrm{im}\,U(S))_2$ *of the injection obtained by factoring* $U(S')$ *by the kernel of* μ_1.

Proof. Since $\lambda_2 d^1(\mu_1(U(S'))_2) = \{1\}$ by Lemma 2.7, and $\mathrm{im}\,\mu_2'$ is the kernel of λ_2, the first assertion follows by the universal mapping property of kernels. By Lemma 2.8 we know that $H^1(S/R, \mathrm{Pic})$ is isomorphic to $\mu_1(U(S'))\cap\mathrm{Ker}\,d^1$. But certainly

$$\mu_1(U(S'))\cap\mathrm{Ker}\,d^1 = (\mu_1(U(S'))\cap\mathrm{Ker}\,(\lambda_2\circ d^1))\cap\mathrm{Ker}\,d^1\ ,$$

hence $\mu_1(U(S'))\cap\mathrm{Ker}\,d^1 = (\mu_1(U(S')))_2\cap\mathrm{Ker}\,d^1$ by Lemma 2.7. Thus $H^1(S/R, \mathrm{Pic})$ is isomorphic to

$$\begin{aligned}&\mathrm{Kernel}\,((\mu_1(U(S')))_2 \xrightarrow{d^1} \mathrm{Pic}\,S^3)\\ &\quad = \mathrm{Kernel}\,(\mu_1(U(S')))_2 \xrightarrow{(d^1)'} \frac{U(S'\otimes S)}{\mathrm{im}\,U(S\otimes S)}\ .\end{aligned}$$

The final assertion of the corollary now follows since μ_1 induces an isomorphism of $U(S')/\mathrm{im}\,U(S)$ to $\mu_1(U(S'))$.

In [14] Morris proves that $\mathrm{Pic}\,S^2$ vanishes iff both $\mathrm{Pic}\,S$ and $U(S')/\mathrm{im}\,U(S)$ are trivial. Therefore, when S is the ring of integers in a quadratic field extension of $\boldsymbol{Q}$, he can conclude $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ is trivial for the six quadratic extensions S for which $\mathrm{Pic}\, S$ and $U(S')/\mathrm{im}\, U(S)$ are trivial [14, Theorem 4.5]. By Corollary 2.9 and Remark 2.1, we can extend the conclusion of the vanishing of $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ to the cases where $\mathrm{Pic}\, S$ and $U(S')/\mathrm{im}\, U(S)$ have an odd number of elements. However, to compute $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ without this hypothesis on $U(S')/\mathrm{im}\,(U(S))$, we will have to describe $(d^1)' \circ \mu_1'$ more explicitly.

LEMMA 2.10. *Let a be a unit of S' such that $\pi(t) = a$ and $\pi(s) = a^2$, where t is in S and s is a unit in S. Let N be the S^3 module $(M_a \otimes_{S^2} S^3) \otimes_{S^3} (M_{a^{-1}} \otimes_{S^2} S^3)$. Then there exist S^2-module isomorphisms $\phi_i \colon N \otimes_{S^3} S^2_{\alpha_i \otimes id} \to S^2$ for $i = 1, 2$ such that:*

(i) $\phi_1^{-1}(1 \otimes 1) = n \otimes (1 \otimes 1)$, *where*

$$\begin{aligned} n = {} & ((s^{-1}t, 1) \otimes (1 \otimes 1 \otimes 1)) \otimes ((t, 1) \otimes (1 \otimes 1 \otimes 1)) \\ & + ((1, t) \otimes (1 \otimes 1 \otimes 1)) \otimes ((1 - s^{-1}t^2, 0) \otimes (1 \otimes 1 \otimes 1)) \,. \end{aligned}$$

(ii) $\phi_2(n \otimes (1 \otimes 1)) = \theta^{-1}((t, t(2 - s^{-1}t^2)))$ *where $\theta \colon S^2 \to M_1$ is the isomorphism described in Remark* 2.3.

Proof. (i) Consider the following string of isomorphisms:

$$\begin{array}{c} N \otimes_{S^3} S^2_{\alpha_1 \otimes id} \\ \Vert \\ ((M_a \otimes_{S^2} S^3_{\varepsilon_0}) \otimes_{S^3} (M_{a^{-1}} \otimes_{S^2} S^3_{\varepsilon_1})) \otimes_{S^3} S^2_{\alpha_1 \otimes id} \\ \downarrow{\scriptstyle f_1} \\ ((M_a \otimes_{S^2} S^3_{\varepsilon_0}) \otimes_{S^3} S^2_{\alpha_1 \otimes id}) \otimes_{S^2} ((M_{a^{-1}} \otimes_{S^2} S^3_{\varepsilon_1}) \otimes_{S^3} S^2_{\alpha_1 \otimes id}) \\ \downarrow{\scriptstyle f_2} \\ (M_a \otimes_{S^2} S^2_{id}) \otimes_{S^2} (M_{a^{-1}} \otimes_{S^2} S^2_{id}) \\ \downarrow{\scriptstyle f_3} \\ M_a \otimes_{S^2} M_{a^{-1}} \\ \downarrow{\scriptstyle f_4} \\ M_1 \\ \downarrow{\scriptstyle \theta^{-1}} \\ S^2 \end{array}$$

where the isomorphisms are described as follows:

(1) Suppose A is a commutative ring and B is a commutative A-algebra. Then if P and Q are A modules, the map $(P \otimes_A Q) \otimes_A B \to$

$(P \otimes_A B) \otimes_B (Q \otimes_A B)$ which takes $(p \otimes q) \otimes b$ to $(p \otimes b) \otimes (q \otimes 1)$ is an isomorphism. The isomorphism f_1 is one of this type applicable to the given situation.

(2) Suppose A is a commutative ring, $A \xrightarrow{\beta} B$ is a commutative A-algebra, and $B \xrightarrow{\gamma} C$ is a commutative B-algebra. Then if P is an A-module, the map $(P \otimes_A B_\beta) \otimes_B C_\gamma \to P \otimes_A C_{\gamma\beta}$ which takes $(p \otimes b) \otimes c$ to $p \otimes \gamma(b)c$ is an isomorphism. The map f_2 is induced by two isomorphisms of this type, one from the observation $\gamma\beta = (\alpha_1 \otimes id) \circ \varepsilon_0 =$ identity when $P = M_a$, $B = S^3$, and $C = S^2$, the other from the observation $\gamma\beta = (\alpha_1 \otimes id) \circ (\varepsilon_1) =$ identity when $P = M_{a^{-1}}$, $B = S^3$, and $C = S^2$.

(3) If P is a module over the commutative ring A, then the map $P \otimes_A A \to P$ where $p \otimes a$ is taken to $a \cdot p$ is an isomorphism. The map f_3 is induced by two isomorphisms of this type.

(4) f_4 is the isomorphism σ of Lemma 1.7.

Let $\phi_1 = \theta^{-1} \circ f_4 \circ f_3 \circ f_2 \circ f_1$. We wish to compute

$$\phi_1^{-1}(1 \otimes 1) = f_1^{-1} \circ f_2^{-1} \circ f_3^{-1} \circ f_4^{-1} \circ \theta(1 \otimes 1)\,.$$

First $\theta(1 \otimes 1) = (\alpha_2(1 \otimes 1), \alpha_2(1 \otimes 1)) = (1, 1)$. Then since $\pi(s^{-1}t) = a^{-1}$ and $\pi(t) = a$, by Lemma 1.7, we have $f_4^{-1}(1, 1) = \tau(1, 1) = (s^{-1}t, 1) \otimes (t, 1) + (1, t) \otimes (1 - s^{-1}t^2, 0)$. That $\phi_1^{-1}(1 \otimes 1) = n \otimes 1$ now follows by checking that under the composition of the canonical isomorphisms f_1, f_2, f_3, one obtains $f_3 \circ f_2 \circ f_1(n \otimes 1) = (s^{-1}t, 1) \otimes (t, 1) + (1, t) \otimes (1 - s^{-1}t^2, 0)$.

(ii) Consider the string of isomorphisms:

$$\begin{array}{c}
N \otimes_{S^3} S^2_{\alpha_2} \otimes id \\
\| \\
((M_a \otimes_{S^2} S^3_{\varepsilon_0}) \otimes_{S^3} (M_a \otimes_{S^2} S^3_{\varepsilon_1})) \otimes_{S^3} S^2_{\alpha_2 \otimes id} \\
\downarrow g_1 \\
((M_a \otimes_{S^2} S^3_{\varepsilon_0}) \otimes_{S^3} S^2_{\alpha_2 \otimes id}) \otimes_{S^2} ((M_a \otimes_{S^2} S^3_{\varepsilon_1}) \otimes_{S^3} S^2_{\alpha_2 \otimes id}) \\
\downarrow g_2 \\
(M_a \otimes_{S_2} S^2_{id}) \otimes_{S^2} (M_{a^{-1}} \otimes_{S^2} S^2_{j \otimes id}) \\
\downarrow g_3 \\
M_a \otimes_{S^2} (M_{a^{-1}})^* \\
\downarrow g_4 \\
M_a \otimes M_a \\
\downarrow g_5 \\
M_{a^2} \\
\downarrow g_6 \\
M_1 \\
\downarrow \theta^{-1} \\
S^2
\end{array}$$

where the isomorphisms are described as follows:

(1) g_1 corresponds to f_1 in part (i).

(2) g_2 corresponds to f_2 in part (i), except here the compositions are $(\alpha_2 \otimes id) \circ \varepsilon_0 =$ identity and $(\alpha_2 \otimes id) \circ \varepsilon_1 = j \otimes id$.

(3) g_3 is induced by the isomorphisms: $M_a \otimes_{S^2} S^2_{id} \to M_a$ described in part (i), and $M_{a^{-1}} \otimes_{S^2} S^2_{j \otimes 1} \to (M_{a^{-1}})^*$ described in Definition 2.3.

(4) g_4 is induced by the isomorphism $T: (M_{a^{-1}})^* \to M_a$ defined in Lemma 2.4.

(5) g_5 is the isomorphism σ of Lemma 1.7.

(6) Let $g_6: M_{a^2} \to M_1$ be defined by $g_6((u, v)) = (su, v)$ for (u, v) in M_{a^2}. This is well defined since, by the definition of M_{a^2}, (u, v) in M_{a^2} implies $a^2\pi(u) = \pi(v)$, hence $\pi(su) = \pi(v)$ or (su, v) is in M_1. That g_6 is an isomorphism follows from the fact that s is a unit of S, since we can define an inverse of g_6 by sending (x, y) in M_1 to $(s^{-1}x, y)$.

Now define $\phi_2 = \theta \circ g_6 \circ g_5 \circ g_4 \circ g_3 \circ g_2 \circ g_1$. We wish to compute $\phi_2(n \otimes (1 \otimes 1))$. By inspecting g_1 and g_2 we see that $g_2 \circ g_1(n \otimes (1 \otimes 1)) = ((s^{-1}t, 1) \otimes (1 \otimes 1)) \otimes ((t, 1) \otimes (1 \otimes 1)) + ((1, t) \otimes (1 \otimes 1)) \otimes ((1 - s^{-1}t^2, 0) \otimes (1 \otimes 1))$, hence

$$g_3 \circ g_2 \circ g_1(n \otimes (1 \otimes 1)) = (s^{-1}t, 1) \otimes (t, 1)^* + (1, t) \otimes (1 - s^{-1}t^2, 0)^* .$$

Now applying g_4 we obtain $g_4 \circ g_3 \circ g_2 \circ g_1(n \otimes (1 \otimes 1)) = (s^{-1}t, 1) \otimes (1, t) + (1, t) \otimes (0, 1 - s^{-1}t^2)$. Then since g_5 is the σ of Lemma 1.1, $g_5 \circ g_4 \circ g_3 \circ g_2 \circ g_1(n \otimes (1 \otimes 1)) = (s^{-1}t, t) + (0, t(1 - s^{-1}t^2)) = (s^{-1}t, t(2 - s^{-1}t^2))$. Finally, $\phi_2(n \otimes (1 \otimes 1)) = \theta^{-1}g_6((s^{-1}t, t(2 - s^{-1}t^2)) = \theta^{-1}((t, (2 - s^{-1}t^2)))$.

COROLLARY 2.11. *Let a be a unit in S' representing a class* (a) *in $(U(S')/\mathrm{im}\, U(S))_2$. Then there exist elements s and t of S with $\pi(s) = a^2$, $\pi(t) = a$ and s a unit of S. In the notation of Corollary* 2.9. $(d^1)' \circ \mu_1'((a)) =$ class $((a \otimes 1) \cdot (\pi \otimes id)\theta^{-1}((t, t(2 - s^{-1}t^2))))$.

Proof. That elements s and t exist satisfying the first assertion follows from the fact that (a) is of order 2 in $U(S')/\mathrm{im}\, U(S)$ and π is surjective.

Now let $N = (M_a \otimes_{S^2} S^3_{\varepsilon_0}) \otimes_{S^3} (M_{a^{-1}} \otimes_{S^2} S^3_{\varepsilon_1})$. Recall that

$$\mu_1': U(S')/\mathrm{im}\, U(S) \longrightarrow \mathrm{Pic}\, S^2$$

by taking the class of a unit u of S' to $[M_u]$ in $\mathrm{Pic}\, S^2$. Then

$$(d_1)' \circ \mu_1'((a)) = d^1([M_a]) = [N] \cdot \mathrm{Pic}\, \varepsilon_2([M_a]) .$$

But then $(d^1)' \circ \mu_1'((a)) =$ class (b) where b is a unit of $S' \otimes S$ with $[M_b]_{S^3} = [N] \cdot [\mathrm{Pic}\, \varepsilon_2([M_a])]$. Therefore, if we can find units b_1 and b_2 of $S' \otimes S$ with $[M_{b_1}]_{S^3} = [N]$ and $[M_{b_2}] = \mathrm{Pic}\, \varepsilon_2([M_a])$, then by Lemma 1.1 we can choose $b = b_1 \cdot b_2$.

First we find b_2. By the definition of μ_1, $\mathrm{Pic}\, \varepsilon_2([\mathrm{M}_a]) = \mathrm{Pic}\, \varepsilon_2 \circ \mu_1(a)$. But the map $\mathrm{Pic}\, S^2 \to \mathrm{Pic}\, S^3$ in Lemma 2.2 is $\mathrm{Pic}\, \varepsilon_2$, while the map

$U(S') \to U(S' \otimes S)$ is the one that takes a unit u of S' to $u \otimes 1$. Therefore, by the commutativity of that diagram

$$\operatorname{Pic} \varepsilon_2([M_a]) = \mu_2(a \otimes 1) = [M_{a\otimes 1}]_{S^3} .$$

Thus we can choose $b_2 = a \otimes 1$.

Next we find b_1 by using Lemma 1.8 as applied to the square in Lemma 2.2. Recall, that by 1.8 we can choose b_1 to be the image of $1 \otimes 1$ under the composition

$$S' \otimes S \xrightarrow{D^{-1}} S^2 \otimes_{S^2} (S' \otimes S) \xrightarrow{(\phi_1 \otimes id)^{-1}} (N \otimes_{S^3} S^2_{\alpha_1 \otimes id}) \otimes_{S^2} (S' \otimes S) \xrightarrow{\gamma}$$
$$(N \otimes_{S^3} S^2_{\alpha_2 \otimes id}) \otimes_{S^2} (S \otimes S') \xrightarrow{\phi_2 \otimes id} S^2 \otimes_{S^2} (S' \otimes S) \xrightarrow{D} S' \otimes S ,$$

where γ is the natural isomorphism obtained from the commutativity of the cartesian square and D is the obvious contraction of $S^2 \otimes_{S^2} (S' \otimes S)$ $S' \otimes S$. Now if we choose the ϕ_1 and ϕ_2 as in Lemma 2.8 then $D \circ (\phi_2 \otimes id) \circ \gamma \circ (\phi_1 \otimes id)^{-1} \cdot D^{-1}(1 \otimes 1) = D \circ (\phi_2 \otimes id) \circ \gamma \circ (\phi_1 \otimes id)^{-1}((1 \otimes 1) \otimes (1 \otimes 1)) = D \circ (\phi_2 \otimes id) \cdot \gamma((n \otimes (1 \otimes 1)) \otimes (1 \otimes 1)) = D \circ (\phi_2 \otimes id))(n \otimes (1 \otimes 1)) \otimes (1 \otimes 1)) = D(\phi_2(n \otimes (1 \otimes 1)) \otimes (1 \otimes 1))$ where n is in Lemma 2.10. But by that lemma, $\phi_2(n \otimes (1 \otimes 1)) = \theta^{-1}(t, t(2 - s^{-1}t^2))$, hence we may choose $b_1 = D(\theta^{-1}((t, t(2 - s^{-1}t^2))) \otimes (1 \otimes 1)) = \pi \otimes id \circ \theta^{-1}((t, t(2 - s^{-1}t^2)))$.

Dealing with the group $U(S' \otimes S)/\operatorname{im} U(S \otimes S)$ is inconvenient, since it is even difficult to tell when two elements of $U(S' \otimes S)$ are equal. Therefore, we now produce a different description of this quotient group. By the definition of S' the sequence

$$0 \longrightarrow (\rho - \bar{\rho})S \longrightarrow S \xrightarrow{\pi} S' \longrightarrow 0$$

is exact. Since S is a free R-module, it then follows that the sequence

$$0 \longrightarrow (\rho - \bar{\rho})S \otimes S \longrightarrow S \otimes S \xrightarrow{\pi \otimes id} S' \otimes S \longrightarrow 0$$

is exact. If we let $J = \theta((\rho - \bar{\rho})S \otimes S)$ we get a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\rho - \bar{\rho})S \otimes S & \longrightarrow & S \otimes S & \longrightarrow & S' \otimes S & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta^*} & & \\ 0 & \longrightarrow & J & \longrightarrow & M_1 & \longrightarrow & M_1/J & \longrightarrow & 0 \end{array} \tag{2.12}$$

where the last vertical map θ^* is defined by commutativity, and is necessarily an isomorphism. By Remark 2.3 M_1 can be considered a ring and θ a ring homomorphism, thus this last square induces an isomorphism

$$\theta' : \frac{U(S' \otimes S)}{\text{im } U(S \otimes S)} \longrightarrow \frac{U(M_1/J)}{\text{im } U(M_1)} .$$

We will write d^* for the composition

$$\theta' \circ (d^1)' \circ \mu_1' : \left(\frac{U(S')}{\text{im } U(S)}\right)_2 \longrightarrow \frac{U(M_1/J)}{\text{im } U(M_1)} .$$

THEOREM 2.13. *Suppose* Pic S *is finite and* (Pic $S)^G = \{1\}$. *Then*

$$H^1(S/R, \text{Pic}) \cong \text{Ker}: \left(\frac{U(S')}{\text{im } U(S)}\right)_2 \xrightarrow{d^*} \frac{U(M_1/J)}{\text{im } U(M_1)} .$$

If a is a unit in S' representing class (a) *in* $(U(S')/\text{im } U(S))_2$, *and* $\pi(s) = a^2$, $\pi(t) = a$ *for t an element in S and s a unit in S, then* $d^*((a)) = \text{class}\,((t^2, t\bar{t}(2 - s^{-1}t^2)))$.

Proof. By Corollary 2.9 and Corollary 2.11, the only thing to show is that

$$\frac{U(S' \otimes S)}{\text{im } U(S^2)} \longrightarrow \frac{U(M_1/J)}{\text{im } U(M_1)}$$

takes class $((a \otimes 1)\cdot(\pi \otimes id))\circ\theta^{-1}((t, t(2-s^{-1}t^2)))$ to class $((t^2, t\bar{t}(2-s^{-1}t^2)))$. But $a \otimes 1 = (\pi \otimes id)(t \otimes 1) = (\pi \otimes id)\circ\theta^{-1}((t, \bar{t}))$, hence class $((a \otimes 1)\cdot(\pi \otimes id)\circ\theta^{-1}((t, t(2 - s^{-1}t^2))) = \text{class}\,(\pi \otimes id)\circ\theta^{-1}((t^2, t\bar{t}(2 - s^{-1}t^2)))$. Then conclusion now follows from the defining diagram (2.12) of θ^*.

We conclude this section with a lemma helpful in detecting the kernel of d^*.

LEMMA 2.14. *Let (s, t) be an element of M_1, then (s, t) is in the zero class of M_1/J iff* $s \equiv t \equiv 0 \pmod{(\rho - \bar{\rho})S}$ *and* $s + t \equiv 0 \pmod{(\rho - \bar{\rho})^2 S}$.

Proof. What we must show is that (s, t) is in J iff the two congruences hold. But $J = \theta((\rho - \bar{\rho})S \otimes S) = \theta(\rho - \bar{\rho} \otimes 1)M_1 = (\rho - \bar{\rho}, \bar{\rho} - \rho)M_1$, therefore, (s, t) is in J iff $s = a(\rho - \bar{\rho})$ and $t = b(\bar{\rho} - \rho)$ for element a, b in S with $\pi(a) = \pi(b)$. This last condition is equivalent to $a \equiv b \pmod{(\rho - \bar{\rho})S}$.

First, suppose (s, t) is in J, hence there are elements a and b as above. Then, clearly, $s \equiv t \equiv 0 \pmod{(\rho - \bar{\rho})S}$. Furthermore, $s + t = (a - b)(\rho - \bar{\rho})$ which implies $s + t \equiv 0 \pmod{(\rho - \bar{\rho})^2 S}$ since $a - b \equiv 0 \pmod{(\rho - \bar{\rho})S}$.

Finally, suppose $s \equiv t \equiv 0 \pmod{(\rho - \bar{\rho})S}$ and $s + t \equiv 0 \pmod{(\rho - \bar{\rho})^2 S}$. Then by the first congruence $s = a(\rho - \bar{\rho})$ and $t = b(\bar{\rho} - \rho)$ for some

a and b in S. To conclude the proof we only have to show that $a \equiv b \pmod{(\rho-\bar{\rho})S}$. But $s+t=(a-b)(\rho-\bar{\rho})$, hence $(a-b)(\rho-\bar{\rho}) = c = (\rho-\bar{\rho})^2$ for some c in S. Then, since S is an integral domain, it follows that $(a-b)=c(\rho-\bar{\rho})$, or $a \equiv b \pmod{(\rho-\bar{\rho})S}$.

3. $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$. Let $\boldsymbol{Q}(\sqrt{d})$ be a quadratic extension of $\boldsymbol{Q}$, and let S be the ring of integers in $\boldsymbol{Q}(\sqrt{d})$. By Remark 2.1, S satisfies the hypothesis in Theorem 2.13 exactly when the class number of S is odd. In this section, under that hypothesis, we compute $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ by using Theorem 2.13 and several number theoretic facts about S.

First we state the number theoretic facts that we will assume in our computations. We will always assume that d is a square free integer not equal to 0 or 1.

LEMMA 3.1 [16, Theorem 6-1-1, p. 234]. *If S is the ring of integers in $\boldsymbol{Q}(\sqrt{d})$ then $S=\boldsymbol{Z}[\rho]$ where:*

(1) $\rho=\sqrt{d}$ *if* $d \not\equiv 1 \pmod 4$.

(2) $\rho=(1+\sqrt{d})/2$ *if* $d \equiv 1 \pmod 4$.

LEMMA 3.2 [16, Proposition 6-3-1, p. 238]. *Let S be the ring of integers in $\boldsymbol{Q}(\sqrt{d})$, then:*

(1) *if $d>0$, then every unit of S can be written uniquely as $\pm\varepsilon^i$, where ε is the fundamental unit of S,* i.e., *the smallest unit of S greater than* 1.

(2) *if $d<0$ but not equal to -1 or -3, then ± 1 are the only units of S.*

(3) *if $d=-1$, then ± 1, $\pm i$ are the only units of S.*

(4) *if $d=-3$, then ± 1, $\pm\alpha$, $\pm\alpha^2$ are the only units of S, where* $\alpha=(\pm 1+\sqrt{-3})/2$.

LEMMA 3.3 [10, p. 432]. *If S is the ring of integers in $\boldsymbol{Q}(\sqrt{d})$ then the class number of S is odd iff d falls into one of the following cases:*

(1) *$d=pq$ where p and q are distinct primes with $p, q \equiv 3$* $\pmod 4$.

(2) *$d=-p$ where p is a prime with* $p \equiv 3 \pmod 4$.

(3) *$d=p$ where p is a prime with* $p \equiv 3 \pmod 4$.

(4) *$d=-1, 2$ or -2.*

(5) *$d=p$ where p is a prime with* $p \equiv 1 \pmod 4$.

(6) *$d=2p$ where p is a prime with* $p \equiv 3 \pmod 4$.

LEMMA 3.4 [14, Lemmas 4.3 and 4.4, p. 626]. *Let S be the ring of integers in $\boldsymbol{Q}(\sqrt{d})$.*

(1) *If* $d \equiv 1 \pmod 4$, *then* $S' = S/(\rho - \bar{\rho})S$ *is isomorphic to* $\boldsymbol{Z}/d\boldsymbol{Z}$ *under the isomorphism which takes the class of* $a + b\rho$ *in* S' *to the class of* $a - ((d-1)/2)b$ *in* $\boldsymbol{Z}/d\boldsymbol{Z}$, *where* a *and* b *are integers.*

(2) *If* $d \not\equiv 1 \pmod 4$, *then* $S' = S/(\rho - \bar{\rho})S$ *is isomorphic to* $\boldsymbol{Z}/2d\boldsymbol{Z} \oplus \boldsymbol{Z}/2\boldsymbol{Z}(\sqrt{d}) = \{\tilde{a} + \hat{b}\sqrt{d} \mid a, b \text{ in } \boldsymbol{Z}\}$ *where* $\sim$ *and* $\wedge$ *denote reduction* mod $2d$ *and* 2 *respectively, and the multiplication is given by*: $(\tilde{a} + \hat{b}\sqrt{d})(\tilde{e} + \hat{f}\sqrt{d}) = \widetilde{ae + bfd} + \widehat{af + be}\sqrt{d}$. *The isomorphism of* S' *to* $\boldsymbol{Z}/2d\boldsymbol{Z} \oplus \boldsymbol{Z}/2\boldsymbol{Z}(\sqrt{d})$ *is defined by taking the class of* $a + b\rho$ *in* S' *to* $\tilde{a} + \hat{b}\sqrt{d}$.

Our first step will be to study the image of $U(S)$ in $U(S')$. *If* s is an element of S we will use the notation $N(s)$ for $s\bar{s}$, the norm of S. Then, since N is multiplicative, an element s in S is a unit iff $N(s)$ is a unit of $\boldsymbol{Z}$, that is iff $N(s) = \pm 1$.

LEMMA 3.5. *Let* S *be the ring of integers in* $\boldsymbol{Q}(\sqrt{d})$, *where* $d > 0$. *Then the image of the fundamental unit* ε *of* S *is not equal to* ± 1 *in* S'.

Proof. Suppose $\pi(\varepsilon) = \pm 1$. If in addition $N(\varepsilon) = -1$, then $1 = (\pi(\varepsilon))^2 = \pi(\varepsilon^2) = \pi(\varepsilon\bar{\varepsilon}) = -1$ in S', contradicting Lemma 3.4. Thus we may assume $N(\varepsilon) = 1$.

We first suppose that $d \equiv 1 \pmod 4$. Then by Lemma 3.1(2) we can write $\varepsilon = ((a/2) + (b)/2)\sqrt{d} = (a-b)/2 + b\rho$ where a and b are integers. By Lemma 3.4(1), our assumption that $\pi(\varepsilon) = \pm 1$ becomes $(a-b)/2 - ((d-1)/2)b = \pm 1 + da$ for some integer s, or equivalently:

(1) $a - 2c = d(b + 2s)$ where $c = \pm 1$.

We have also assumed that $N(\varepsilon) = 1$, or

(2) $a^2 - b^2 d = 4$.

Let $x = \sqrt{a + 2c}$, $y = b/(\sqrt{a + 2c})$ and $\varepsilon' = (x/2) + (y/2)\sqrt{d}$. By direct calculation and equation (2), it is easy to check that $(\varepsilon')^2 = \varepsilon$. Thus, once we have checked that ε' is in S, we will have a contradiction of Lemma 3.2 (1). Note that since S is integrally closed and $(\varepsilon')^2 = \varepsilon$, it will suffice to show that x any y are integers.

Let $r = b + 2s$, an integer which is positive by (1). From equation (1) we obtain $a = dr + 2c$. Substituting this expression for a into equation (2) and simplifying yields $b^2 = r(rd + 4c)$. Now, let $r = r_1 2^n$ where r_1 is an integer prime to 2. Then $b^2 = r_1(2^n(rd + 4c))$ implies that r_1 and $2^n(rd + 4c)$ are both squares, since they are relatively prime. We now show r is also a square.

If n is even then $r = r_1 2^n$ is a square as claimed, hence we assume that n is odd. But, if n is 3 or greater, 2^{n+2} and $2^{n-2}r_1 d + c$

are relatively prime, 2^{n+2} is not a square, yet the product $2^n(rd+4c)$ is a square. Thus, $n=1$ is the only remaining possibility. Since both r_1 and d are odd we obtain that r_1d+2c is odd, therefore $4r_1(r_1d+2c)$ is divisible by 4 but not 8. But

$$b^2 = r(rd+4c) = 4r_1(r_1d+2c) ,$$

hence b is divisible by 2 but not by 4. Then, by equation (2) a is divisible by 2, in fact $(a/2)^2 - d(b/2)^2 = 1$. Since $(b/2)$ is odd it is congruent to 1 or 3 mod 4, hence $(b/2)^2$ is congruent to 1 mod 4. Therefore, $(a/2)^2 = d(b/2)^2 + 1 \equiv 2 \pmod 4$. But this is a contradiction, since 2 is not a square mod 4. Thus n cannot be odd, and r is a square.

By equation (2) $a^2-4=b^2d=a^2-4c^2$, therefore $a+2c=(b^2d)/(a-2c)$. But by equation (1) $a-2c=d(b+2s)=dr$, hence $a+2c=b^2d/dr=b^2/r$. Therefore, since r is a square, $a+2c$ is a square and $x=\sqrt{a+2c}$ is an integer. Furthermore, $\sqrt{a+2c}=b/\sqrt{r}$ which yields that $y=b(\sqrt{a+2c})=\sqrt{r}$ is also an integer. This is the required contradiction.

Finally, consider the case when $d \not\equiv 1 \pmod 4$. Again, $\varepsilon = a/2 + (b/2)\sqrt{d}$, this time with a and b even. From Lemma 3.4(2) we obtain $a/2 \equiv \pm 1 \pmod{2d}$ and $b/2 \equiv 0 \pmod 2$, which again makes equation (1) valid, but not s is even. The proof that x and y are integers now proceeds just as before, with the simplication that $r=b+2s$ is divisible by at least 4, thus eliminating the $n=1$ case above.

COROLLARY 3.6. *Let S be the ring of integers in $\boldsymbol{Q}(\sqrt{d})$. Then the order of the image of $U(S)$ is $U(S')$ is:*

(1) 4, *if* $d>0$.

(2) 2, *if* $d<0$.

Proof. (1) Suppose $d>0$. Since $N(\varepsilon)=\pm 1$, it follows that $\pi(\varepsilon)^2=\pi(\varepsilon^2)=\pi(\varepsilon\bar{\varepsilon})=\pm 1$. But this implies that $\pi(\varepsilon)^i$ is $\pm\pi(\varepsilon)$ if i is odd, or ± 1 if i is even. Therefore, by Lemma 3.2(1), ± 1, $\pm\pi(\varepsilon)$ are the elements in the image of $U(S)$, and by Lemma 3.5 they are distinct elements.

(2) Suppose d is not equal to -1 or -3. Then by Lemma 3.2(2) the only units of S are ± 1. But since $1 \neq -1$ in S' by Lemma 3.4, $\pi(U(S))$ has 2 elements. The $d=-1$ or -3 cases can be easily deduced directly from Lemmas 3.2 and 3.4.

We now compute $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$, where S is the ring of integers in a quadratic extension of $\boldsymbol{Q}$, with odd class number. The computation will be broken into the cases of Lemma 3.3.

LEMMA 3.7. *Let S be the ring of integers in $\boldsymbol{Q}(\sqrt{d})$, where $d = pq$, $d = -p$, or $d = p$ for distinct primes p, q with $p \equiv q \equiv 3 \pmod 4$. Then $(U(S')/\mathrm{im}\, U(S))_2$ is trivial, which implies $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ is trivial by Theorem* 2.13.

Proof. Let x be an element of $U(S')$ which represents a class of $(U(S')/\mathrm{im}\, U(S))_2$. Then x^2 is in $\pi(U(S))$, which by Corollary 3.6 makes the order of x a power of 2. Thus to complete the proof, it will suffice to show that in each case the number of elements in $U(S')$ with order a power of 2, is equal to the order of $\pi(U(S))$.

Suppose $d = pq$. Then by Lemma 3.4(1), $S' \cong \boldsymbol{Z}/(pq)\boldsymbol{Z}$, hence $U(S') \cong U(\boldsymbol{Z}/(pq)\boldsymbol{Z}) \cong U(\boldsymbol{Z}/p\boldsymbol{Z}) \times U(\boldsymbol{Z}/q\boldsymbol{Z})$. But since $U(\boldsymbol{Z}/p\boldsymbol{Z})$ and $U(\boldsymbol{Z}/q\boldsymbol{Z})$ are cyclic groups with $p-1$ and $q-1$ elements, and $p \equiv q \equiv 3 \pmod 4$, each of these groups have only 2 elements with order a power of 2. Therefore, $U(S')$ has only 4 elements with order a power of 2, which by Corollary 3.6 is the number of elements in $\pi(U(S))$.

Suppose $d = -p$. Then, by Lemma 3.4(1), $U(S') \cong U(\boldsymbol{Z}/p\boldsymbol{Z})$, a cyclic group with $p-1$ elements. Then since $p \equiv 3 \pmod 4$, $U(S')$ has only two elements with order a power of 2. Again by Corollary 3.6 these are precisely the elements of $\pi(U(S))$.

Finally, suppose $d = p$. Then, by Lemma 3.4(2) $S' \cong \boldsymbol{Z}/2p\boldsymbol{Z} \oplus \boldsymbol{Z}/2\boldsymbol{Z}\sqrt{p}$. But if $y = \tilde{a} + \hat{b}\sqrt{p}$ is in the latter ring, $y^2 = \widetilde{a^2 + b^2p}$. Therefore, x is a unit iff $a^2 + b^2p$ is a unit of $\boldsymbol{Z}/2p\boldsymbol{Z}$. From this it is not hard to show that $U(S')$ has axactly $2(p-1)$ units. But $p \equiv 3 \pmod 4$, thus $U(S')$ has only 4 elements whose order is a power of 2, which by Corollary 3.6 completes the proof.

LEMMA 3.8. *Let S be the ring of integers in $\boldsymbol{Q}(\sqrt{d})$, where d is -1, 2, or -2. Then $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ is trivial.*

Proof. The cases $d = -1$ and $d = 2$ are dealt with in [14, Theorem 4.5, p. 627]. In case $d = -2$, it is easy to see by inspection that $(U(S')/\mathrm{im}\, U(S))_2$ has only one nontrivial class, namely the class represented by $1 + \sqrt{2}$. However, by direct calculation it is not hard to check that this class is not in kernel of d^*.

The next lemma provides an example of the nonvanishing of $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$.

LEMMA 3.9. *Let S be the ring of integers in $\boldsymbol{Q}(\sqrt{d})$ where $d = p$, and p is a prime with $p \equiv 1 \pmod 4$. Then $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ is trivial or has 2 elements as $p \equiv 5 \pmod 8$ or $p \equiv 1 \pmod 8$ respectively.*

Proof. By Lemma 3.4(1), $U(S') \cong U(Z/pZ)$, a cyclic group of order $p-1$. Thus, since by Corollary 3.6(2) $\operatorname{im}(U(S))$ has order 4, the group $U(S')/\operatorname{im}(U(S))$ is a cyclic group of order $(p-1)/4$. Therefore, $(U(S')/\operatorname{im}(U(S)))_2$ is trivial or has 2 elements as $p \equiv 5 \pmod 8$ or $p \equiv 1 \pmod 8$ respectively. Thus, by Theorem 2.13, $H^1(S/Z, \mathrm{Pic})$ is trivial if $p \equiv 5 \pmod 8$, and has at most 2 elements if $p \equiv 1 \pmod 8$.

The $p \equiv 5 \pmod 8$ case being resolved, we now assume $p \equiv 1 \pmod 8$. Let n be an integer such that $n^4 \equiv -1 \pmod p$. By Lemma 3.4(1) and the congruence defining n, we see that $\pi(n)$ is an element of $U(S')$ of order 8, which makes $((\pi(n)))$ the only nontrivial element of $(U(S')/\operatorname{im} U(S))_2$. Thus to complete the proof we must show that $d^*((\pi(n))) = 1$, where d^* is defined in Theorem 2.13.

In the notation of Theorem 2.13, we pick $t = n$, and let s be any unit of S with $\pi(s) = (\pi(n))^2$. By Lemma 3.1(2) we can write $s = a + b\rho$ where a and b are integers and $\rho = (1 + \sqrt{p})/2$. Applying Lemma 3.4(1) to the equation $\pi(s) = \pi(n))^2$, yields $a - ((p-1)/2)b \equiv n^2 \pmod p$. We will write x for the integer $a - ((p-1)/2)b$.

Since $\pi(s) = (\pi(n))^2$, it follows that $\pi(s)$ is of order 4 in $U(S')$. Then if $N(s) = 1$, we must have $1 = \pi(s\bar{s}) = \pi(s)^2$ which is a contradiction. Therefore, $N(s) = -1$ which yields $s^{-1} = -\bar{s}$, or $s^{-1} = -a - b\bar{\rho}$. Hence, $t\bar{t}(2 - s^{-1}t^2) = n^2(2 + (a + b\bar{\rho})n^2) = 2n^2 + an^4 + bn^4\bar{\rho}$. But $n^4 \equiv -1 \pmod p$ and $p = (\rho - \bar{\rho})^2$, thus

$$t\bar{t}(2 - s^{-1}t^2) \equiv 2n^2 + -a - b\bar{\rho} \pmod{(\rho - \bar{\rho})^2 S} .$$

Then substituting $\bar{\rho} = 1 - \rho$, we obtain

$$t\bar{t}(2 - s^{-1}t^2) \equiv 2n^2 - a - b + b\rho \pmod{(\rho - \bar{\rho})^2 S} .$$

Recall though that from the last paragraph $a - ((p-1)/2)b \equiv n^2 \pmod p$, hence $2n^2 \equiv 2a + b \pmod p$. This then yields $t\bar{t}(2 - s^{-1}t^2) \equiv (2a + b) - a - b + b\rho \equiv a + b\rho \equiv s \pmod{(\rho - \bar{\rho})^2 S}$.

By direct computation one easily verifies that $s = a + b\rho = x + b\rho(\rho - \bar{\rho})$. Therefore $s^p = x^p + px^{p-1}b\rho(\rho - \bar{\rho}) + (\rho - \bar{\rho})^2 y$, where y is some element of S. But then since

$$p = (\rho - \bar{\rho})^2 , \quad s^p \equiv x^p \pmod{(\rho - \bar{\rho})^2 S} .$$

Now, since $x^p \equiv x \pmod p$, it follows that $s^p \equiv x \pmod{(\rho - \bar{\rho})^2 S}$. Finally, since $x \equiv n^2 \pmod p$, $s^p \equiv n^2 \pmod{(\rho - \bar{\rho})^2 S}$.

In the last two paragraphs we have established that $t^2 = n^2 \equiv s^p \pmod{(\rho - \bar{\rho})^2 S}$ and $t\bar{t}(2 - s^{-1}t^2) \equiv s \pmod{(\rho - \bar{\rho})^2 S}$. Since by Theorem 2.13, $(t^2, t\bar{t}(2 - s^{-1}t^2))$ is in M_1, we must have

$$t^2 \equiv t\bar{t}(2 - s^{-1}t^2) \pmod{(\rho - \bar{\rho})S}$$

which by the above congruences yields $s^p \equiv s \pmod{(\rho - \bar{\rho})S}$. Therefore, (s^p, s) is in M_1, and since s is a unit, (s^p, s) is actually in $U(M_1)$. To complete the proof we show that $d^*(\pi((n)))$ is trivial by showing $(t^2, t\bar{t}(2 - s^{-1}t^2)) \equiv (s^p, s) \pmod{J}$. But by Lemma 2.14 this will hold iff $t^2 \equiv s^p \pmod{(\rho - \bar{\rho})S}$, $t\bar{t}(2 - s^{-1}t^2) \equiv s \pmod{(\rho - \bar{\rho})S}$, and $t^2 + t\bar{t}(2 - s^{-1}t^2) \equiv s^p + s \pmod{(\rho - \bar{\rho})^2 S}$. However, these last three congruence follow immediately from the first two congruences in this paragraph.

We have studied all the cases of Lemma 3.3 except the one where S is the ring of integers in $\boldsymbol{Q}(\sqrt{2p})$, where p is a prime with $p \equiv 3 \pmod 4$. For the next four lemmas we assume p and S satisfy these hypotheses, and proceed to establish the vanishing of $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ in this case.

LEMMA 3.10. *If $m + n\sqrt{2p}$ is a unit of S where m and n are integers, then $N(m + n\sqrt{2p}) = 1$, n is even, and $m^2 \equiv 1 \pmod{8p}$. The unit $\pi(m + n\sqrt{2p})$ is of order at most 2 in $U(S')$.*

Proof. By [16, Exercise 6-3-4, p. 240] $N(\varepsilon) = 1$, where ε is the fundamental unit of S. But then since $m + n\sqrt{2p} = \pm\varepsilon^i$, the multiplicativity of the norm yields $N(m + n\sqrt{2p}) = N(\pm\varepsilon^i) = N(\pm 1)N(\varepsilon)^i = 1$. This immediately implies our last assertion, since $(\pi(m + n\sqrt{2p}))^2 = \pi(m + n\sqrt{2p})\cdot\pi(j(m + n\sqrt{2p})) = \pi(N(m + n\sqrt{2p})) = 1$. Furthermore, since $N(m + n\sqrt{2p}) = m^2 - 2pn^2$, we obtain $m^2 - 2pn^2 = 1$. Therefore, since $p \equiv 3 \pmod 4$ we obtain, $m^2 + 2n^2 \equiv 1 \pmod 4$. If n is odd then $n^2 \equiv 1 \pmod 4$, hence $m^2 \equiv -1 \pmod 4$. But -1 is not a square mod 4, thus n is even. This yields that $1 \equiv m^2 - 2pn^2 \equiv m \pmod{8p}$.

LEMMA 3.11. *Let $t = x + y\sqrt{2p}$, where x and y are integers, be an element of S. Suppose $\pi(t)^2 = \pi(s)$ for some unit s of S, with $s = a + b\sqrt{2p}$. Then:*

(1) *$a \equiv x^2 + 2py^2 \pmod{4p}$.*

(2) *If y is even then $\pi(t)$ is in $\pi(U(S))$.*

(3) *If y is odd then $\pi(t)^2 \neq \pm 1$.*

Proof. (1) We have

$$\begin{aligned}\pi(a + b\sqrt{2p}) = \pi(s) = \pi(t)^2 = \pi(t^2) &= \pi((x + y\sqrt{2p})^2) \\ &= (x^2 + 2py^2 + 2xy\sqrt{2p}) .\end{aligned}$$

Therefore, by Lemma 3.4(2), we obtain the required $a \equiv x^2 + 2py^2 \pmod{4p}$.

(2): If y is even, then by (1) we obtain $a \equiv x^2 \pmod{4p}$. But by Lemma 3.10 $a^2 \equiv 1 \pmod{8p}$, hence $x^4 \equiv 1 \pmod{4p}$. The equation $z^4 \equiv 1 \pmod 4$ has only two solutions. Furthermore, $z^4 \equiv 1 \pmod p$

has only two solutions mod p, since the order $p-1$ of $U(Z/pZ)$ is divisible by 2 but not $4\,(p \equiv 3 \pmod 4)$. Therefore, $z^4 \equiv 1 \pmod{4p}$ has exactly four solutions. Now if $\varepsilon = m + n\sqrt{2p}$ is the fundamental unit of S, Lemma 3.10 yields that $m^2 \equiv 1 \equiv m^4 \pmod{4p}$. But by Lemma 3.5 we know that $\pi(\varepsilon) \neq \pm 1$, hence Lemma 3.4(2) then implies that $m \not\equiv \pm 1 \pmod{4p}$. Therefore, ± 1, $\pm m$ are all the solutions mod $4p$ to $z^4 \equiv 1 \pmod{4p}$; hence $x \equiv \pm 1$ or $\pm m \pmod{4p}$. Furthermore, we have $y \equiv 0 \equiv n \pmod 2$ by our hypothesis and Lemma 3.10. Lemma 3.4(2) then implies that $\pi(t) = \pi(x + y\sqrt{2p}) = \pm\pi(\varepsilon)$ or $\pm\pi(1)$. In any case $\pi(t)$ is in $\pi(U(S))$.

(3): If y is odd, by (1) we obtain $a \equiv x^2 + 2p \pmod{4p}$. Therefore, $a^2 \equiv (x^2+2p)^2 \equiv x^4 \pmod{4p}$, and by Lemma 3.1 $1 \equiv a^2 \equiv x^4 \pmod{4p}$. As in part (2) by counting the solutions to the equation $z^4 \equiv 1 \pmod{4p}$, we see that $x \equiv \pm 1$ or $\pm m \pmod{4p}$ where $\varepsilon = m + n\sqrt{2p}$ is the fundamental unit. But, since $m^2 \equiv 1 \pmod{4p}$ by Lemma 3.10, we obtain $x^2 \equiv 1 \pmod{4p}$ in either case. Then $a \equiv x^2 + 2p \pmod{4p}$ implies $a \equiv 1 + 2p \pmod{4p}$, hence $\pi(s) = \pi(a + b\sqrt{2p}) \neq \pm 1$ by Lemma 3.4(2).

LEMMMA 3.12. *Let $t = x + y\sqrt{2p}$ be an element of S, where x is an integer and y is an odd integer. Suppose $\pi(t)^2 = \pi(s)$ for some unit s of S, with $s = a + b\sqrt{2p}$. Then:*

(1) $x^2 + 2py^2 \equiv a + kp \pmod{8p}$, *where k is 0 or 4.*

(2) *If $w_1 = t^2$ and $w_2 = t\bar{t}(2 - s^{-1}t^2)$, then*
$w_1 + w_2 \equiv 2a + (k-4)p + b\sqrt{2p} \pmod{(\rho - \bar{\rho})^2 S}$.

Proof. (1) follows immediately from Lemma 3.11(1).

(2): As pointed out in the proof of Lemma 3.10, the norm of any unit of S is 1. In particular $s\bar{s} = 1$, hence $s^{-1} = \bar{s} = a - b\sqrt{2p}$. Then by substituting $t = x + y\sqrt{2p}$, $\bar{t} = x - y\sqrt{2p}$, and $s^{-1} = a - b\sqrt{2p}$ into the defining equations of w_1 and w_2 we obtain $w_1 = r_1 + r_2\sqrt{2p}$ and $w_2 = r_3 + r_4\sqrt{2p}$ where $r_1 = x^2 + 2py^2$, $r_2 = 2xy$, $r_3 = (x^2 - 2py^2)\cdot[2 + 4bxyp - a(x^2 + 2py^2)]$, and $r_4 = (x^2 - 2py^2)[b(x^2 + 2py^2) - 2axy]$. By part (1) we know that $x^2 + 2py^2 \equiv a + kp \pmod{8p}$ where $k = 0$ or 4, hence it follows that $x^2 - 2py^2 \equiv a + (k+4)p \pmod{8p}$ since y is odd. Therefore, $r_4 \equiv (a + (k+4)p)[b(a + kp) - 2axy] \equiv (a + (k+4)p)\cdot[b(a+kp) - 2(a + (k+4)p)axy] \pmod{8p}$. But because $k = 0$ or 4 we see that $2(k+4)p \equiv 0 \pmod{8p}$, and since b is even by Lemma 3.10, we also obtain $bkp \equiv b(k+4)p \equiv 0 \pmod{8p}$. This yields $r_4 \equiv a^2b - 2a^2xy \pmod{8p}$. But by Lemma 3.10, we know that $a^2 \equiv 1 \pmod{8p}$, hence it follows that $r_4 \equiv b - 2xy \pmod{8p}$. Similarly, $r_3 = (x^2 - 2py^2)\cdot[2 + 4bxyp - a(x^2 + 2py^2)] \equiv (x^2 - 2py^2)[2 - a(x^2 + 2py^2)] \equiv (a + (k+4)p)\cdot[2 - a(a+kp)] \equiv 2(a + (k+4)p) - a^2(a+kp) - a(a+kp)(k+4)p \equiv 2a - a^2(a+kp) - a^2(k+4)p - akp\,(k+4)p \equiv$

$2a - (a + kp) - (k + 4)p \equiv a - 2kp - 4p \equiv a - 4p \pmod{8p}$. Then, since $(\rho - \bar{\rho})^2 = (\sqrt{2p} - (-\sqrt{2p}))^2 = 8p$, we obtain $w_1 + w_2 = (r_1 + r_3) + (r_2 + r_4)\sqrt{2p} \equiv (x^2 + 2py^2) + (a - 4p) + ((2xy) + (b - 2xy))\sqrt{2p} \equiv (a + kp) + (a - 4p) + b\sqrt{2p} \equiv 2a + (k - 4)p + b\sqrt{2p} \pmod{(\rho - \bar{\rho})^2 S}$.

LEMMA 3.13. *Let u_1 and u_2 be units of S with (u_1, u_2) in M_1. Suppose $u_1 = (-1)^i\varepsilon^r$ and $u_2 = (-1)^j\varepsilon^q$ where $\varepsilon = m + n\sqrt{2p}$ is the fundamental unit of S, and r and q are nonnegative integers. Then $r \equiv q \pmod 2$, and*

$$u_1 + u_2 \equiv (-1)^i(2m^r + (r + q)m^{r-1}n\sqrt{2p}) \bmod ((\rho - \bar{\rho})^2 S) .$$

Proof. Since (u_1, u_2) is in M_1, we obtain that $\pi(u_1) = \pi(u_2)$ from the definition of M_1. Thus $(-1)^i\pi(\varepsilon)^r = (-1)^j\pi(\varepsilon)^q$, or $\pi(\varepsilon)^{r-q} = (-1)^{i-j}$. But by Lemma 3.5 we know that $\pi(\varepsilon) \neq \pm 1$, and by Lemma 3.10 we know that $\pi(\varepsilon)^2 = 1$, hence $r \equiv q \pmod 2$ and $i \equiv j \pmod 2$.

By the binomial expansion of $\varepsilon^r = (m + n\sqrt{2p})^r$, we obtain $\varepsilon^r = m^r + rm^{r-1}n\sqrt{2p} + 2n^2pg$ where g is some element of S. But, by Lemma 3.10 n is even, thus $\varepsilon^r \equiv m^r + rm^{r-1}n\sqrt{2p} \pmod{(8pS)}$. Similarly, $\varepsilon^q \equiv m^q + qm^{q-1}n\sqrt{2p} \pmod{8pS}$). By Lemma 3.10 we have that $m^2 \equiv 1 \pmod{8p}$, therefore, since $r \equiv q \pmod 2$, it follows that $\varepsilon^q \equiv m^r + qm^{r-1}n\sqrt{2p} \pmod{8pS}$. Then $u_1 + u_2 = (-1)^i\varepsilon^r + (-1)^j\varepsilon^q$, and since $i \equiv j \pmod 2$ this is

$$(-1)^i(\varepsilon^r + \varepsilon^q) \equiv (-1)^i(2m^r + (r + q)m^{r-1}n\sqrt{2p}) \pmod{(8pS)} .$$

Since $(\rho - \bar{\rho})^2 = 8p$, the required congruence follows.

LEMMA 3.14. *Let S be the ring of integers in $Q(\sqrt{d})$, where $d = 2p$ and p is a prime with $p \equiv 3 \pmod 4$. Then $H^1(S/Z, \mathrm{Pic})$ is trivial.*

Proof. Let z be a unit of $U(S')$ which represents a class of $(U(S')/\pi(U(S))_2)$. By Theorem 2.13, we must show that if $d^*((z))$ is trivial, then z actually lies in $\pi(U(S))$. Since z is in S' we can write $z = \pi(t)$ where $t = x + y\sqrt{2p}$ is in S, and since z^2 is in $\pi(U(S))$ we can write $z^2 = \pi(s)$ where $s = a + b\sqrt{2p}$ is a unit of S. Then if we let $w_1 = t^2$ and $w_2 = t\bar{t}(2 - s^{-1}t^2)$, by Theorem 2.13, we have $d^*((z)) = \text{class}((w_1, w_2))$ where we mean the class of (w_1, w_2) in $U(M_1/J)/\text{im } U(M_1)$. Therefore, what we must show is that if (u_1, u_2) is in M_1, where u_1, u_2 are units of S, and $(u_1, u_2) \equiv (w_1, w_2) \pmod J$ then $z = \pi(t)$ is in $\pi(U(S))$. Thus we now assume the hypotheses of the last sentence.

By Lemma 3.11(2), we see that we are done if y is even, hence we assume y is odd. Since s is a unit of S, Lemma 3.2(1) yields that $s = c\varepsilon^l$ where $c = \pm 1$ and l is an integer. Then $\pi(s) = c(\pi(\varepsilon))^l$ which by Lemma 3.11(3) yields that $\pi(\varepsilon)^l \neq \pm 1$. But by Lemma 3.10 $\pi(\varepsilon)^2 = 1$, hence l is odd. Therefore, $\pi(s) = c(\pi(\varepsilon))^l = c\pi(s) = \pi(c\varepsilon)$. Thus, since s was chosen to be any unit of S with $\pi(s) = z = \pi(t)^2$, we may assume $s = c\varepsilon$ without loss of generality.

Since $S/(\rho - \bar{\rho})^2 S = S/8pS$ is isomorphic to $\boldsymbol{Z}/8p\boldsymbol{Z} \oplus \boldsymbol{Z}/8p\boldsymbol{Z}(\sqrt{2p})$, we know that $S/(\rho - \bar{\rho})^2 S$ is a finite ring. Therefore,

$$\varepsilon^n \equiv 1 \,(\mathrm{mod}\,(\rho - \bar{\rho})^2 S)$$

for some positive integer n. But then by Lemma 2.14 $(\varepsilon^{nf}, \varepsilon^{nf}) \equiv (1, 1) \,(\mathrm{mod}\, J)$ for any integer f. It then follows that $(w_1, w_2) \equiv (u_1, u_2) \equiv (u_1\varepsilon^{nf}, u_2\varepsilon^{nf}) \,(\mathrm{mod}\, J)$. Therefore, since f can be taken to be a large positive integer, we can assume without loss of generality that $u_1 = (-1)^i\varepsilon^r$ and $u_2 = (-1)^j\varepsilon^q$ where r and q are positive integers.

Since $(u_1, u_2) \equiv (w_1, w_2) \,(\mathrm{mod}\, J)$, Lemma 2.14 at least implies $u_1 \equiv w_1 \,(\mathrm{mod}\,(\rho - \bar{\rho})S)$. But $w_1 = t^2 \equiv s \,(\mathrm{mod}\,(\rho - \bar{\rho})S)$, hence

$$(-1)^i\varepsilon^r \equiv n_1 \equiv s \equiv c\varepsilon \,(\mathrm{mod}\,(\rho - \bar{\rho})S) ,$$

or since $c = \pm 1$, we have $(-1)^i c\varepsilon^{r-1} \equiv 1 \,(\mathrm{mod}\,(\rho - \bar{\rho})S)$. Then since $\pi(\varepsilon)^2 = 1$ and $\pi(\varepsilon) \neq \pm 1$ by Lemma 3.5, we must have that r is odd and $(-1)^i c = 1$.

Since $\varepsilon = cs = c(a + b\sqrt{2p})$, Lemma 3.13 implies

$$\begin{aligned} u_1 + u_2 &\equiv (-1)^i(2(ca)^r + (r + q)(ca)^{r-1}(cb)\sqrt{2p}) \\ &\equiv (-1)^i c^r(2a^r + (r + q)a^{r-1}b\sqrt{2p}) \,(\mathrm{mod}\,(\rho - \bar{\rho})^2 S) . \end{aligned}$$

But, since r is odd, $a^2 \equiv 1 \,(\mathrm{mod}\, 8p)$ by Lemma 3.10, and $(\rho - \bar{\rho})^2 = 8p$, it follows that $u_1 + u_2 \equiv (-1)^i c^r(2a + (r + q)b\sqrt{2p}) \,(\mathrm{mod}\,(\rho - \bar{\rho})^2 S)$. Finally, since $c = \pm 1$ and r is odd, we have $(-1)^i c^r = (-1)^i c = 1$, thus $u_1 + u_2 \equiv (2a + (r + q)b\sqrt{2p}) \,(\mathrm{mod}\,(\rho - \bar{\rho})^2 S)$.

By Lemma 2.14, $(u_1, u_2) \equiv (w_1, w_2) \,(\mathrm{mod}\, J)$ implies $u_1 + u_2 \equiv w_1 + w_2 \,(\mathrm{mod}\,(\rho - \bar{\rho})^2 S)$. Putting the congruence of the last paragraph together with Lemma 3.12(2), we obtain $2a + (r + q)b\sqrt{2p} \equiv (2a + (k - 4)p) + b\sqrt{2p} \,(\mathrm{mod}\,(\rho - \bar{\rho})^2 S)$, where $k = 0$ or 4. But, since $(\rho - \bar{\rho})^2 = 8p$, the last congruence is equivalent to the two congruences: $2a \equiv 2a + (k - 4)p \,(\mathrm{mod}\, 8p)$, and $(r + q)b \equiv b \,(\mathrm{mod}\, 8p)$. The first of these latter congruences implies $k = 4$. By the second $b(r + q - 1) \equiv 0 \,(\mathrm{mod}\, 8p)$, which yields $b \equiv 0 \,(\mathrm{mod}\, 8)$ since Lemma 3.13 forces $r + q - 1$ to be odd.

By Lemma 3.13(1), we obtain $x^2 + 2py^2 \equiv a + kp \equiv a + 4p \,(\mathrm{mod}\, 8p)$. Then $p \equiv 3 \,(\mathrm{mod}\, 4)$ implies $2p \equiv 6 \,(\mathrm{mod}\, 8)$ and $4p \equiv 4 \,(\mathrm{mod}\, 8)$, hence $x^2 + 6y^2 \equiv a + 4 \,(\mathrm{mod}\, 8)$. But we have assumed y is odd, therefore $y^2 = 1 \,(\mathrm{mod}\, 8)$. Thus $x^2 + 6 \equiv a + 4 \,(\mathrm{mod}\, 8)$, or $x^2 \equiv a - 2 \,(\mathrm{mod}\, 8)$. Now, Lemma 3.10 yields that $N(a + b\sqrt{2p}) = a^2 - 2bp^2 = 1$, and since we now know that $b \equiv 0 \pmod 8$, this implies $a^2 \equiv 1 \pmod{16}$. But then since $3^2 \not\equiv 1 \pmod{16}$ and $5^2 \not\equiv 1 \pmod{16}$ we have $a \equiv \pm 1 \pmod 8$. Therefore, $x^2 \equiv a - 2 \equiv -1$ or $-3 \pmod 8$. This is a contradiction since neither -1 nor -3 is a square mod 8.

Since the assumption that y was odd led to contradiction, the proof is complete.

THEOREM 3.15. *Let S be the ring of integers in $\boldsymbol{Q}\sqrt{d})$. Further suppose that the class number of S is odd. Then $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ is trivial unless d is prime and congruent to* 1 mod 8. *In this latter case $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ has two elements.*

Proof. This is just Lemma 3.3 together with Lemmas 3.7, 3.8, 3.9, and 3.14.

4. **$H^2(S/R, U)$ for some cyclic extensions.** Let R be an integrally closed integral domain with quotient field K, and let L be a Galois field extension of K with group G. Now suppose S is an integral extension of R in L which is mapped to itself by G. In this section we show that $H^2(S/R, U)$ vanishes in a number of special cases in which G is cyclic, by considering a homomorphism $H^2(S/R, U) \to H^2(G, U(S))$. The result is applied to the case where R is the ring of rational integers, and S is the ring of integers in certain quadratic, cubic, and cyclotomic number fields. A similar result for cubic fields can already be found in [6], and several of the quadratic cases can be found in [7] and [14].

The homomorphism $H^2(S/R, U) \to H^2(G, U(S))$ that we use to compare the cohomology groups is described in [4, Theorem 5.4 and Lemma 5.1]. Of course, in that paper, S is a Galois extension of R with group G and the homomorphism is an isomorphism. However, the map is always defined and we now recall the definition.

If H is a group and X is a set, we will write $E^n(H, X)$ for the set of functions of n variables defined on H with values in X. Now suppose B is a commutative algebra over a commutative ring A, H is a group of A-algebra automorphisms of B, and F is an additive functor from the category of A-algebras to the category of groups. Then it is easily verified that the map $h_n\colon B^{n+1} \to E^n(H, B)$ defined on the generators $b_0 \otimes \cdots \otimes b_n$ of B^{n+1} by

$$(h_n(b_0 \otimes \cdots \otimes b_n))(\sigma_1, \cdots, \sigma_n) = b_0\sigma_1(b_1)\sigma_1\sigma_2(b_2) \cdots \sigma_1\sigma_2 \cdots \sigma_n(b_n)\ ,$$

is an A-algebra homomorphism. Applying the functor F we obtain a group homomorphism $F(h_n)\colon F(B^{n+1}) \to F(E^n(H, B))$, which when composed with the natural isomorphism $\phi\colon F(E^n(H, B)) \to E^n(H, F(B))$

[4, 5.3, p. 16] yields a group homomorphism $\phi \circ F(h_n): F(B^{n+1}) \to E^n(H, F(B))$. By the same computation as in [4], we find that the maps $\{\phi \circ F(h_n)\}$ commute with the coboundary maps of Amitsur and group cohomology, i.e., the diagram

$$\begin{array}{ccc} F(B^{n+1}) & \longrightarrow & F(B^{n+2}) \\ \downarrow & & \downarrow \\ E^n(H, F(B)) & \longrightarrow & E^{n+1}(H, F(B)) \end{array} \tag{4.1}$$

commutes for each n, where the horizontal maps are the coboundary homomorphisms. Thus $\phi \circ F(h_n)$ induces a group mapping

$$h^*_{n,F}: H^n(B/A, F) \to H^n(H, F(B)) .$$

REMARK 4.2. By [4, Lemma 5.1], the mapping $h_n: L^{n+1} \to E^n(G, L)$ is an isomorphism since L is Galois over K. Therefore, if S is flat over R we at least know that $h_n: S^{n+1} \to E^n(G, S)$ is injective. Then if F is a left exact functor, as the functor U is, it follows that $h_{n,F}: F(S^{n+1}) \to E^n(G, F(S))$ is also injective. We also note explicitly that the map $h^*_{2,U}: H^2(S/R, U) \to H^2(G, U(S))$ takes the class of a unit $\sum s_i \otimes t_i \otimes u_i$ of S^3 which represents an Amitsur 2-cocycle, to the class of the 2-cocycle $f: G \times G \to U(S)$ defined by

$$f(\sigma_1, \sigma_2) = \sum s_i \sigma_1(t_i) \sigma_1 \sigma_2(u_i) .$$

We will write I for the ideal of S generated by the set $\{\sigma(x) - \tau(x) \mid \sigma, \tau \text{ in } G, x \text{ in } S\}$.

LEMMA 4.3. *Suppose that R is integrally closed and the Galois group G of L/K is cyclic. Then the homomorphism $h^*_2: H^2(S/R, U) \to H^2(G, U(S))$ is trivial if either:*

(1) *$U(R) = N(U(S))$ where N is the norm mapping from L to K.*

(2) *The natural mapping $U(S) \to U(S/I)$ is injective when restricted to $U(R)$.*

Proof. Suppose H is any finite cyclic group with generator σ, and of order m. Then if M is an H-module, it is well known that $H^n(H, M)$ is isomorphic to $M^H/N(M)$ when n is even and where N is the norm mapping. In fact when n is 2 it is easy to write down an isomorphism defined explicitly on 2-cocycles represented by functions mapping $H \times H \to M$. We define $g: H^2(H, M) \to M^H/N(M)$ by $g(\text{class}(f)) = \text{class}(\prod_{i=1}^m f(\sigma^i, \sigma))$, where $f: K \times K \to M$ is a cocycle (cf. [11, Theorem 4.3]).

Now, to show that the image of $h^*_2: H^2(S/R, U) \to H^2(G, U(S))$ is trivial it will suffice to show that the image of the composite $H^2(S/R, U) \to H^2(G, U(S)) \to U(S)^G/N(U(S))$ is trivial. Of course if hypothesis (1) holds this is immediate, since R integrally closed implies $U(S)^G = U(R)$. Therefore, suppose hypothesis (2) holds. Let $w = \sum s_i \otimes t_i \otimes u_i$ be a unit in S^3 which is an Amitsur 2-cocycle. Then we see that the composition

$$H^2(S/R, U) \longrightarrow H^2(G, U(S)) \longrightarrow \frac{U(S)^G}{N(U(S))}$$

takes the class of w to class $(\prod_{j=1}^m f(\sigma^j, \sigma))$ where $h_2(w) = f$, σ is a generator of G, and m is the order of G. But by the definition of h_2, we have $f(\sigma^j, \sigma) = \sum_i s_i\sigma^j(t_i)\sigma^{j+1}(u_i)$, hence the class of w is taken to the class $xN(U(S))$ in $U(R)/N(U(S))$, where $x = \prod_{j=1}^m \sum s_i\sigma^j(t_i)\sigma^{j+1}(u_i)$. But clearly from the definition of the ideal I, we see that $s_i\sigma^j(t_i)\sigma^{j+1}(u_i) \equiv s_it_iu_i \equiv \sigma^j(s_it_iu_i) \pmod I$. Thus if we write y for the unit $\sum s_it_iu_i$ of S obtained by contracting w, we obtain

$$\sum_i s_i\sigma^j(t_i)\sigma^{j+1}(u_i) \equiv \sigma^j\left(\sum s_it_iu_i\right) \equiv \sigma^j(y) \pmod I .$$

Therefore, $x \equiv \prod_{j=1}^m \sigma^j(y) \equiv N(y) \pmod I$. But both x and $N(y)$ are units in R, hence hypothesis (2) implies $x = N(y)$ making the image of w trivial.

The next proposition at least partially fills in the connection between Amitsur and Galois cohomology provided by h_2^*.

For any Dedekind domain A, we let $D(A)$ donote its group of fractional ideals.

PROPOSITION 4.4. *Let R be a Dedekind domain with quotient field K, and L be a Galois extension of K with group G. Further, suppose that S is the integral closure of R in L. Then S is also Dedekind* [18, Theorem 19, p. 281], *and there is a commutative diagram*

$$(4.5)\qquad \begin{array}{ccccccc} & & 0 & & & & \\ & & \downarrow & & & & \\ & 0 \longrightarrow & H^0(S/R, \mathrm{Pic})/\mathrm{im}\,\mathrm{Pic}\,R & \xrightarrow{\gamma} & H^2(S/R, U) & \xrightarrow{\alpha} & \mathrm{Br}(S/R) \\ & & \downarrow{\scriptstyle h_0'} & & \downarrow{\scriptstyle h_2^*} & & \\ D(S)^G/\mathrm{im}\,D(R) & \longrightarrow & (\mathrm{Pic}\,S)^G/\mathrm{im}\,\mathrm{Pic}\,R & \xrightarrow{\gamma'} & H^2(G, U(S)) & \longrightarrow & H^2(G, U(L)) \end{array}$$

with exact rows.

Proof. The top row is obtained from part of the seven term exact sequence [5, Theorem 7.6], and the bottom exact sequence is from [15, Theorem, p. 873]. The vertical map h_0' is induced by

$$h_{0,\mathrm{Pic}}^*: H^0(S/R, \mathrm{Pic}) \longrightarrow H^0(G, \mathrm{Pic}\, S) = (\mathrm{Pic}\, S)^G .$$

Actually, since there are no coboundaries in dimension 0, $H^0(S/R, \mathrm{Pic})$ is a subgroup of $\mathrm{Pic}\, S$ (in fact $(\mathrm{Pic}\, S)^G$), and h_0' can be identified with the natural injection.

The only thing left to prove is the commutativity of the diagram. We recall from [15] that the map γ' is induced by a composition $(\mathrm{Pic}\, S)^G = H^0(G, U(S)) \to H^1(G, U(L)/U(S)) \to H^2(G, U(S))$, where the first map is the connecting homomorphism in degree 0 obtained from $0 \to U(L)/U(S) \to D(S) \to \mathrm{Pic}\,(S) \to 0$, and the second is the connecting homomorphism in degree 1 obtained from

$$0 \longrightarrow U(S) \longrightarrow U(L) \longrightarrow U(L)/U(S) \longrightarrow 0 .$$

From this it is not difficult to write down an explicit formula for γ'. Furthermore, an explicit formula for γ is given in [9, (A. 18–3), p. 155]. Thus the commutativity of the diagram can be verified by direct computation, a computation we omit.

LEMMA 4.6. *Let R be a Dedekind domain with quotient field K, and let S be the integral closure of R in a Galois field extension L of K with group G, so that S is also Dedekind. If both of the maps $h_2^*: H^2(S/R, U) \to H^2(G, U(S))$ and $D(S)^G \to (\mathrm{Pic}\, S)G/\mathrm{im}\, \mathrm{Pic}\, R$ are trivial, then $H^2(S/R, U) = 0$.*

Proof. Consider diagram (4.5). By the triviality of $D(S)^G \to (\mathrm{Pic}\, S)^G/\mathrm{im}\, \mathrm{Pic}\, R$, γ' is injective. Thus $\gamma' \circ h_0' = h_2^* \circ \gamma$ is injective, and since h_2^* is trivial the conclusion will follow if γ is surjective, or equivalently α is trivial.

Let $\alpha': H^2(L/K, U) \to \mathrm{Br}\,(L/K)$ be the map corresponding to α obtained when [5, Theorem 7.6] is applied to L/K. By [7, Theorem 1.3, p. 241] we know that the sequence of [5, Theorem 7.6] is natural in both variables. Therefore, the inclusion mapping $R \to K$ induces a commutative diagram

$$\begin{array}{ccc} H^2(S/R,\ U) & \xrightarrow{\alpha} & \mathrm{Br}\,(S/R) \\ \big\downarrow & & \big\downarrow \\ H^2(L/K,\ U) & \xrightarrow{\alpha'} & \mathrm{Br}\,(L/K)\ . \end{array} \tag{4.7}$$

But since R is Dedekind $\mathrm{Br}\,(R) \to \mathrm{Br}\,(K)$ is injective by [1, Theorem 7.2], which makes $\mathrm{Br}\,(S/R) \to \mathrm{Br}\,(L/K)$ injective. Thus to show α is trivial it will suffice to show that the map $H^2(S/R, U) \to H^2(L/K, U)$ is trivial.

Let $h_2^K\colon L^3 \to E^2(G, L)$ be the map of the same form as $h_2\colon S^3 \to E^2(G, S)$, but here applied to L/K. By [4, Theorem 5.4, p. 17], since L is Galois over K, h_2^K induces an isomorphism

$$(h_2^K)^*\colon H^2(L/K, U) \longrightarrow H^2(G, U(L)) .$$

Therefore, we will have α is trivial once we have shown that

$$H^2(S/R, U) \longrightarrow H^2(L/K, U) \xrightarrow{(h_2^K)^*} H^2(G, U(L))$$

is trivial. However, this composition also factors as $H^2(S/R, U) \xrightarrow{h_2^*} H^2(G, U(S)) \to H^2(G, U(L))$, which is trivial since h_2^* is.

LEMMA 4.8. *Let ρ be a primitive p^n root of unity, where p is any prime number. Suppose $L = \boldsymbol{Q}(\rho)$ and K is a subfield of L. Then since L is Galois over $\boldsymbol{Q}$, it follows that L is Galois over K, say with group G.*

If R and S are the ring of integers in K and L respectively, then the image of $D(S)^G \to (\mathrm{Pic}\, S)^G/\mathrm{im}\,\mathrm{Pic}\, R$ is trivial.

Proof. Let M be any fractional ideal of $D(S)^G$. Since we are mapping into $(\mathrm{Pic}\, S)^G$, we can assume M is integral without loss of generality. Let $M = \prod_{i,j} Q_{ij}^{r_{ij}}$ be the prime factorization of M indexed so that $Q_{ij} \cap R = Q_{ij'} \cap R$ is the same prime Q_i of R. Now let $M_i = \prod_j Q_{ij}^{r_{ij}}$, and let σ be in G. Since σ must map one prime lying over Q_i to another prime lying over Q_i and $\sigma(M) = M$, it follows that $\sigma(M_i) = M_i$ by the uniqueness of factorization into prime ideals. Therefore, each M_i is in $D(S)^G$, and without loss of generality we may assume the primes of M all lie over a given prime of R.

With this reduction we now write the prime factorization of M as $M = \prod Q_j^{r_j}$ with each $Q_j \cap R$ equal to the prime ideal Q of R. Since G acts transitively on the primes of S, ([18, Theorem 22, p. 289]) M in $D(S)^G$ implies that all r_j must equal a given nonnegative integer r, and each prime lying over Q must be a Q_j. Now since L is Galois over $\boldsymbol{Q}$ and consequently over K, by [12, Corollary 2, p. 21] $QS = \prod Q_j^e$ where e is the ramification index of Q in S. If $e = 1$ then $M = (\prod Q_j)^r = Q^r S$, so that the image of M is trivial in

$$(\mathrm{Pic}\, S)^G/\mathrm{im}\,\mathrm{Pic}\, R .$$

Thus we may assume Q ramifies in S.

Since $Q \cap \boldsymbol{Z}$ is a prime ideal in $\boldsymbol{Z}$, we must have $Q \cap \boldsymbol{Z} = (q)$ for some prime number q. But since Q ramifies in S, certainly q will ramify in S. Then by [16, 7-4-1, p. 262] $q = p$ and the only prime in S lying over p is the principal prime ideal $(1 - \rho)S$. Therefore,

$M = (1 - \rho)^r S$ and its image is again trivial in $(\mathrm{Pic}\, S)^G/\mathrm{im}\ \mathrm{Pic}\ R$.

THEOREM 4.9. *Let ρ be a primitive p^n root of unity, where p is an odd prime number. Suppose $L = \boldsymbol{Q}(\rho)$, K is a subfield of L, and R and S are the rings of integers in K and L respectively. If the only units of R are ± 1, then $H^2(S/R, U)$ is trivial.*

Proof. By Lemmas 4.6 and 4.8, it will suffice to show that the image of $H^2(S/R, U) \xrightarrow{h_2^*} H^2(G, U(S))$ is trivial, where G is the Galois group L over K. By [16, 7-1-2, p. 257] the Galois group of $L/\boldsymbol{Q}$ is cyclic, thus certainly G is cyclic. Therefore, by Lemma 4.3 it will suffice to verify that the composite $U(R) \to U(S) \to U(S/I)$ is an injection where I is the ideal of S generated by $\{\sigma(x) - \tau(x) \mid \sigma, \tau$ are in G, and x is in $S\}$. Since by hypothesis $U(R) = \{\pm 1\}$, we need only show that 2 is not in I.

By [16, p. 264], $S = \boldsymbol{Z}[\rho]$, thus I is generated by $\{\sigma(\rho^k) - \tau(\rho^k) \mid k$ is a positive integer, and σ, τ are in $G\}$. But $\sigma(\rho)^k$ and $\tau(\rho^k)$ are also p^n roots of 1, thus $\sigma(\rho^k) - \tau(\rho^k) = \rho^l - \rho^m$ where l and m are positive integers. Then since $\rho^l - o^m = \rho^m(\rho^{l-m} - 1) = -\rho^l(\rho^{m-l} - 1)$, we see that $\rho^l - \rho^m$ is divisible by $(\rho - 1)$ no matter which of l and m is the greatest. Thus I is contained in the prime ideal $(\rho - 1)S$. Therefore, if 2 is in I then 2 is in $(\rho - 1)S \cap \boldsymbol{Z} = p\boldsymbol{Z}$. But we assumed p was an odd prime. Hence 2 is not in I, completing the proof.

REMARK 4.10. One reason for calculating $H^2(S/R, U)$ is that knowledge of that group together with [5, Theorem 7.6] should reveal information about $\mathrm{Br}\,(S/R)$. Theorem 4.9 applied to the case $K = \boldsymbol{Q}$ immediately implies that $H^2(S/\boldsymbol{Z}, U)$ vanishes. Therefore, by [5, Theorem 7.6] there is an exact sequence $0 \to \mathrm{Br}\,(S/\boldsymbol{Z}) \to H^1(S/\boldsymbol{Z}, \mathrm{Pic}) \to H^3(S/\boldsymbol{Z}, U)$. However, $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ has proved difficult to compute, and we have no result corresponding to Theorem 3.15 in the cyclotomic case.

The number rings R that satisfy Theorem 4.9 can be found explicitly. By the Dirichlet Units Theorem, for $U(R)$ to be finite, $r + s - 1 = 0$ where r is the number of real embeddings of K and s is the number of conjugate pairs of complex embeddings. Thus, either $r = 1$ and $s = 0$, or $r = 0$ and $s = 1$. But if n is the dimension of K over Q, then $n = r + 2s$, thus K is either Q or an imaginary quadratic number field. But if $K = \boldsymbol{Q}(\sqrt{-d})$ for d a positive square free integer, then by [16, 7-4-4, p. 263] K will be contained in L iff d divides p^n and satisfies $d \equiv 3 \pmod 4$. Therefore, the only choices for K are $\boldsymbol{Q}$ and $\boldsymbol{Q}(\sqrt{-p})$, with $p \equiv 3 \pmod 4$. But for the units of R to be exactly ± 1, [16, 6-3-1, p. 238] leaves exactly $\boldsymbol{Q}$ and $\boldsymbol{Q}(\sqrt{-p})$ with $p \equiv 3 \pmod 4$ and $p \neq 3$.

Although Lemma 4.8 was applicable to the p^n roots of unity for any prime p, Theorem 4.9 required that p be odd. There were two reasons for this. First, the 2^n roots of unity are not a cyclic extension of $\boldsymbol{Q}$ when $n > 2$. Second, the map $U(\boldsymbol{Z}) \to U(S) \to U(S/I)$ is not an injection since $2 = (1 - \rho)^{2^{n-1}}$.

However, the vanishing of $H^2(S/\boldsymbol{Z}, U)$ for S the ring of integers in the field of 2^n roots of unity can be deduced from the fact that $\mathrm{Br}(\boldsymbol{Z}) = 0$ ([8]). For by Lemmas 4.6 and 4.8, it will suffice to show that $H^2(S/\boldsymbol{Z}, U) \xrightarrow{h_2^*} H^2(G, U(S))$ is trivial. But by diagram (4.5) the kernel of $H^2(G, U(S)) \to H^2(G, U(L))$ is just the image of

$$\gamma' : (\mathrm{Pic}\, S)^G/\mathrm{im}\,\mathrm{Pic}\,\boldsymbol{Z} \longrightarrow H^2(G, U(S)) .$$

By [16, Satz C, p. 244] the class number of S is odd, yet $H^2(G, U(S))$ has exponent 2^{n-1} since this is the order of G. Therefore, the image of γ' is trivial and $H^2(G, U(S)) \to H^2(G, U(L))$ is an injection. Thus it will suffice to show that $H^2(S/\boldsymbol{Z}, U) \xrightarrow{h_2^*} H^2(G, U(S)) \to H^2(G, U(L))$ is trivial. But this composite is the same as

$$H^2(S/\boldsymbol{Z}, U) \longrightarrow H^2(L/\boldsymbol{Q}, U) \xrightarrow{(h_2^Q)^*} H^2(G, U(L)) ,$$

and since $(h_2^Q)^*$ is an isomorphism it will suffice to show

$$H^2(S/\boldsymbol{Z}, U) \longrightarrow H^2(L/\boldsymbol{Q}, U)$$

is trivial. This, however, follows from diagram (4.7) since α' is an isomorphism ([4, Corollary 5.5, p. 17]) and $\mathrm{Br}(S/\boldsymbol{Z}) = 0$.

We now prepare to establish the vanishing of $H^2(S/R, U)$ for some extensions of degree 3. Our method requires some explicit calculations with 2-cocycles over groups of order 3. The next lemma rewrites the coboundary equations in dimension 2 in a form more convenient for our purposes. The proof is by reversible substitution which we omit.

LEMMA 4.11. *Let $G = \{id, \sigma, \sigma^2\}$ be a group of order 3 and M a G-module. Let $h: G \times G \to M$ be a function with $h(id, id) = 0$. Then h is a coboundary iff there is a function f: $G \to M$ such that:*

(1) $0 = f(0) = h(0, 0) = h(0, 1) = h(0, 2) = h(1, 0) = h(2, 0)$

(2) $f(1) = h(1, 2) - \sigma(f(2))$

(3) $h(1, 1) = -N(f(2)) + h(1, 2) + \sigma(h(1, 2))$

(4) $h(2, 1) = \sigma^2(h(1, 2))$

(5) $h(2, 2) = N(f(2)) - h(1, 2)$

where N is the norm mapping and we have written $h(i, j)$ for $h(\sigma^i, \sigma^j)$ and $f(i)$ for $f(\sigma^i)$.

LEMMA 4.12. *Let R be an integral domain with quotient field*

K, and suppose $U(R)$ is a torsion group with no 3 torsion. Suppose further that L is a Galois extension of K of degree 3 with Galois group G, and S, the integral closure of R in L, is flat over R. Then the map $h_2^*\colon H^2(S/R, U) \to H^2(G, U(S))$ is an injection.

Proof. Let $w = \sum x_i \otimes y_i \otimes z_i$ be an Amitsur 2-cocycle in $U(S^3)$. We must show that if $h_2(w)$ in $E^2(G, U(S))$ is a 2-coboundary, then w is an Amitsur 2-coboundary. Recall, that by the definition of h_2, if (τ, μ) is in G^2 then $h_2(w)(\tau, \mu) = \sum x_i \tau(y_i)\tau\mu(z_i)$. Now, let

$$s = \sum x_i y_i z_i = h_2(w)(id, id) ,$$

a unit of S. Then $s \otimes 1$ is in $U(S^2)$, and

$$(1 \otimes s \otimes 1)(s \otimes 1 \otimes 1)^{-1} \cdot (s \otimes 1 \otimes 1) = 1 \otimes s \otimes 1$$

is a coboundary in $U(S^3)$. Then if we let $w' = w/(1 \otimes s \otimes 1)$, w' is in the same class as w in $H^2(S/R, U)$, but $h_2(w')(id, id) = s/s = 1$. Therefore., without loss of generality we may assume $h_2(w)(id, id) = 1$.

Let σ be a generator of the Galois group G, so that $G = \{id, \sigma, \sigma^2\}$. To simplify notation we will write $h(i, j)$ instead of $h_2(w)(\sigma^i, \sigma^j)$, where $i, j = 0, 1, 2$. Now assume $h_2(w)$ is a coboundary. Then by Lemma 4.11 there is a function $f\colon G \to U(S)$ satisfying equations (1)-(5) of that lemma with h replaced by $h_2(w)$.

Consider diagram (4.1), specialized to the functor U with $n = 1$. The horizontal maps are the Amitsur and group cohomology coboundaries, while the vertical maps are just the restrictions of h_1 and h_2. Since h_2 is injective by Remark 4.2, to show that w is an Amitsur coboundary, it will suffice to find a unit t of S^2 such that $h_1(t)$ is taken to $h_2(w)$ by the group coboundary operator. Specifically then, we must find a unit t of S^2 such that the equations (1)-(5) of Lemma 4.11 hold with $h_1(t)$ in place of f. But since those equations do hold for f, we see that it is sufficient to find t such that:

$$\begin{aligned} &h_1(t)(0) = 1,\ h_1(t)(1) = h(1, 2)\sigma(h_1(t)(2))^{-1} , \quad \text{and} \\ &N(h_1(t)(2)) = N(f(2)) , \end{aligned} \tag{4.13}$$

where we have written $h_1(t)(i)$ for $h_1(t)(\sigma^i)$.

If we apply the norm N to equation (3) of Lemma 4.11, we obtain

$$\begin{aligned} N(h(1, 1)) &= N(N(f(2)))^{-1} \cdot N(h(1, 2))N(\sigma(h(1, 2)) \\ &= N(f(2))^{-3}N(\sigma^2(h(1, 2))^2 . \end{aligned}$$

If we let $a = \sigma^2(h(1, 2))^2 \cdot h(1, 1)^{-1}$, then we can rewrite the last equation as $N(f(2))^3 = N(a)$. But $N(a)$ is in $U(R)$, hence it must have order n which is prime to 3. Thus we can write

$$1 = 3k + nm \text{ for some integers } k \text{ and } m\,. \tag{4.14}$$

Then $N(a) = N(a)^{3k+nm} = N(a)^{3k} = N(a^k)^3$. But then $N(f(2))^3 = N(a) = N(a^k)^3$, therefore $N(f(2)) = N(a^k)$ since $U(R)$ has no 3 torsion. But then to satisfy equations (4.13) it will suffice to find a unit t of S^2 such that:

$$\begin{aligned} &h_1(t)(0) = 1,\ h_1(t)(2) = a^k\,, \quad \text{and} \\ &h_1(t)(1) = h(1, 2)\sigma(a^k)^{-1}\,. \end{aligned} \tag{4.15}$$

Now recall that $w = \sum x_i \otimes y_i \otimes t_i$ and let $t_1 = \sum x_i\sigma^2(z_i) \otimes \sigma^2(y_i)$, $t_2 = \sum \sigma^2(x_i)\sigma(z_i) \otimes \sigma^2(y_i)$, $t_3 = \sum x_i\sigma(y_i) \otimes \sigma^2(z_i)$, $t_4 = \sum x_i\sigma^2(z_i) \otimes \sigma(y_i)$, $t_5 = \sum \sigma^2(x_i)y_i \otimes z_i$, and $t_6 = \sum \sigma(x_i)z_i \otimes \sigma(y_i)$. Each of the t_i is a unit of S^2 since each is the image of w under an obvious algebra homomorphism of S^3 to S^2. Using the definitions of h_1 and the t_i together with Lemma 4.11(1) (where applicable), it is not difficult to explicitly compute the $h_1(t_i)(j)$. For example, $h_1(t_2)(2) = \sum \sigma^2(x_i)\sigma(z_i)\sigma(y_i) = \sigma^2(\sum x_i\sigma^2(z_i)\sigma^2(y_i)) = \sigma^2(h(2, 0)) = 1$ and $h_1(t_1)(2) = \sum x_i\sigma^2(z_i)\sigma(y_i) = h(1, 1)$. Systematically computing all the $h_1(t_i)(j)$ we obtain

$$\begin{cases} 1 = h_1(t_1)(0) = h_1(t_1)(1) = h_1(t_2)(0) = h_1(t_2)(2) = h_1(t_3)(1) \\ \quad = h_1(t_3)(2) = h_1(t_4)(1) = h_1(t_4)(2) = h_1(t_5)(0) = h_1(t_6)(0) \\ \quad = h_1(t_6)(2) \\ h(1, 1) = h_1(t_1)(2) = h_1(t_3)(0) = h_1(t_4)(0) \\ \sigma^2(h(1, 1)) = h_1(t_2)(1) = h_2(t_5)(2) \\ h(1, 2) = h_1(t_3)(1) \\ \sigma^2(h(1, 2)) = h_1(t_5)(2) \\ \sigma(h(1, 1)) = h_1(t_6)(1)\,. \end{cases} \tag{4.16}$$

Now let $t = t_1^{-k} t_2^{-2k} t_3^{(-2k+1)} t_4^{(2k-1)} t_5^{2k} t_6^{k}$, where k is the integer chosen in equation (4.14). Then using the above table, we obtain:

$$\begin{aligned} h_1(t)(0) &= 1 \cdot 1 \cdot h(1, 1)^{(-2k+1)} \cdot h(1, 1)^{(2k-1)} \cdot 1 \cdot 1 = 1 \\ h_1(t)(1) &= 1 \cdot \sigma^2(h(1, 1))^{-2k} \cdot h(1, 2)^{-2k+1} \cdot 1 \cdot \sigma^2(h(1, 1))^{2k} \cdot \sigma(h(1, 1))^k \\ &= h(1, 2)^{-2k+1}\sigma(h(1, 1))^k \\ h_1(t)(2) &= h(1, 1)^{-k} \cdot 1 \cdot 1 \cdot 1 \cdot \sigma^2(h(1, 2)^{2k}) \cdot 1 = h(1, 1)^{-k}\sigma^2(h(1, 2))^{2k}\,. \end{aligned} \tag{4.17}$$

But substituting the definition $a = \sigma^2(h(1, 2))^2h(1, 1)^{-1}$ into equations (4.15) we obtain:

$$\begin{aligned} h_1(t)(0) &= 1 \\ h_1(t)(1) &= h(1, 2)\sigma(\sigma^2(h(1, 2)^2h(1, 1)^{-1})^{-k}) \\ &= h(1, 2)^{-2k+1}\sigma(h(1, 1))^k \\ h_1(t)(2) &= (\sigma^2(h(1, 2)^2h(1, 1)^{-1})^k) = h(1, 1)^{-k}\sigma^2(h(1, 2))^{2k}\,. \end{aligned} \tag{4.18}$$

Since equations (4.17) and (4.18) agree, we have found a unit t in S^2 meeting the necessary requirements.

THEOREM 4.19 (cf. [6, Theorem 4.1]). *Let R be an integrally closed integral domain with quotient field K, and suppose $U(R)$ is a torsion group with no 3 torsion. Suppose further that L is a Galois extension of K of degree 3, and S, the integral closure of R in L, is flat over R. Then $H^2(S/R, U) = 0$.*

Proof. By Lemma 4.12, it will suffice to show that the image of $H^2(S/R, U) \xrightarrow{h_2^*} H^2(G, U(S))$ is trivial. This, however, follows from Lemma 4.3 once we show that $N(U(S)) = U(R)$. But every element of $U(R)/U(R)^3$ simultaneously has order 3 and order prime to 3, therefore, $U(R) = U(R)^3$. This establishes $N(U(R)) = U(R)$, hence certainly $N(U(S)) = U(R)$.

REMARK 4.20. Again it is easy to determine the number rings R whose units satisfy the hypotheses of Theorem 4.19. For $U(R)$ to be torsion, as in Remark 4.10, the Dirichlet Unit Theorem implies that $K = \boldsymbol{Q}$ or $\boldsymbol{Q}(\sqrt{-d})$ for d a square free positive integer. By [16, 6-3-1, p. 238] the requirement that $U(R)$ has no 3 torsion further eliminates exactly $\boldsymbol{Q}(\sqrt{-3})$. Thus, if we require that R be a number ring, Theorem 4.19 coincides with [6, Theorem 4.1].

Actually, Dobbs has noted that [6, Theorem 3.2] which establishes the vanishing of $H^1(S/R, UK/U)$, with a little work implies our Theorem 4.1. It is interesting that this apparently different approach also requires the normality of L over K. Of course when L is not normal over K, the group G of K-automorphisms of L is trivial, and our approach of considering $H^2(S/R, U) \rightarrow H^2(G, U(S))$ is hopeless. However, in [6], Dobbs has been able to show that $H^2(S/R, U)$ vanishes in several specific cubic nonnormal cases, by using inflation to the normal closure together with known information about class numbers.

We now compute $H^2(S/R, U)$ in the following setting. Let R be an integrally closed integral domain whose quotient field K has characteristic different from 2. Let L be a quadratic field extension of K with Galois group $G = \{\sigma, id\}$. We further suppose that ρ is an element of L which is integral over R, and S is the subring of L for which $\{1, \rho\}$ is a basis over R.

In the following lemma we revive the notation $M_1, \theta, \alpha_1, \alpha_2, \pi, S'$ of § 2.

LEMMA 4.21. *Let r be an element of R. S^3 contains an element w satisfying:*

$$(4.22)\qquad \begin{aligned}&h_2(w)(id,\, id) = h_2(w)(id,\, \sigma) = h_2(w)(\sigma,\, id) = 1 \quad \textit{and}\\ &h_2(w)(\sigma,\, \sigma) = r\ ,\end{aligned}$$

iff $1 - r$ *is in* $(\rho - \bar{\rho})^2 R$, *where for any element* s *of* S *we write* $\sigma(s) = \bar{s}$.

Proof. Recall that by Corollary 1.4 and Lemma 2.2 the square

$$\begin{array}{ccc} S \otimes S \otimes S & \xrightarrow{\alpha_2 \otimes id} & S \otimes S \\ \Big\downarrow{\scriptstyle \alpha_1 \otimes id} & & \Big\downarrow{\scriptstyle \pi \otimes id} \\ S \otimes S & \xrightarrow{\pi \otimes id} & S' \otimes S \end{array}$$

is cartesian. Furthermore, by Remark 2.3, $\theta: S \otimes S \to M_1$ defined by $\theta(s \otimes t) = (st, \bar{s}t)$ is an isomorphism.

Now, let $w = \sum x_i \otimes y_i \otimes z_i$ be an element of S^3. Then

$$\begin{aligned}\theta \circ (\alpha_1 \otimes id)(w) &= \theta\,(\textstyle\sum x_i y_i \otimes z_i) = \sum\,(x_i y_i z_i,\, \sum \bar{x}_i \bar{y}_i z_i)\\ &= (h_2(w)(id,\, id),\, \sigma(h_2(w)(id,\, \sigma)))\ ,\end{aligned}$$

and

$$\begin{aligned}\theta \circ (\alpha_2 \otimes id)(w) &= \theta\,(\textstyle\sum \bar{x}_i y_i \otimes z_i) = (\sum \bar{x}_i \bar{y}_i z_i,\, \sum x_i \bar{y}_i z_i)\\ &= (\sigma(h_2(w)(\sigma,\, id)),\, h_2(w)(\sigma,\, \sigma))\ .\end{aligned}$$

Therefore, S^3 has an element w satisfying (4.22) iff it has an element w with $\theta \circ (\alpha_1 \otimes id)(w) = (1, 1)$ and $\theta \circ (\alpha_2 \otimes id)(w) = (1, r)$. That is iff there are elements z_1, z_2 of S^2 with $\theta(z_1) = (1, 1)$, $\theta(z_2) = (1, r)$, $(\alpha_1 \otimes id)(w) = z_1$, and $(\alpha_2 \otimes id)(w) = z_2$. But then since the diagram above is cartesian, an element w in S^3 satisfying (4.22) will exist iff there are elements z_1, z_2 of S^2 with $\theta(z_1) = (1, 1)$, $\theta(z_2) = (1, r)$ and $(\pi \otimes id)(z_1) = (\pi \otimes id)(z_2)$.

We now refer to diagram (2.12) of § 2. By that diagram $(\pi \otimes id)(z_1) = (\pi \otimes id)(z_2)$ iff $\theta(z_1) \equiv \theta(z_2) \pmod{J}$. Thus an element w satisfying (4.22) exists iff $(1, 1)$ and $(1, r)$ are in M_1 and $(1, 1) \equiv (1, r) \pmod{J}$. Then by Lemma 2.14 this is equivalent to $1 - r$ being an element of $(\rho - \bar{\rho})^2 S$. But $1 - r$ and $(\rho - \bar{\rho})^2$ are in R and R is integrally closed, thus $1 - r$ is in $(\rho - \bar{\rho})^2 S$ iff it is in $(\rho - \bar{\rho})^2 R$, completing the proof.

LEMMA 4.23. *Let* r *be in* $U(R)$, *and* w *be an element of* $U(S^3)$ *satisfying* (4.22). *Then* w *is Amitsur coboundary iff there is an element* a *of* $U(S)$ *with* $N(a) = r$ *and* $a \equiv 1 \pmod{(\rho - \bar{\rho})S}$.

Proof. As mentioned in the proof of Lemma 4.12, we know that w is a coboundary iff there is an element f of $h_1(U(S^2))$ which is taken to $h_2(w)$ by the group coboundary operator. But by equation (4.22) and the formula for the group coboundary operator, this occurs iff $(\sigma^i(f(\sigma^j))\cdot f(\sigma^i))/f(\sigma^{i+j})=1$ if i or j is not 1, and $(\sigma(f(\sigma))\cdot f(\sigma))/f(id)=r$. Simplifying, this is the same as $f(id) = 1$ and $N(f(\sigma)) = r$.

We now know that w is a coboundary iff there is an element z of $U(S^2)$ with $h_1(z)(id) = 1$ and $N(h_1(z)(\sigma)) = r$. But since

$$\theta(z) = (h_1(z)(id), \sigma(h_1(z)(\sigma))) ,$$

and $\theta: S \otimes S \to M_1$ is an isomorphism, this is the same as the existence of a unit $(1, a)$ of M_1 with $N(a) = r$. That is, w is a coboundary iff there exists a unit a of S with $a \equiv 1 \pmod{(\rho - \bar{\rho})S}$ and $N(a) = r$.

THEOREM 4.24. *Suppose R is an integrally closed integral domain whose quotient field K has characteristic different from 2, and L is a quadratic field extension of K. If ρ is an element of L which is integral over R, and S is the subring of R with R-basis $\{1, \rho\}$, then $H^2(S/R, U) \cong A/N(B)$, where $A = \{a \in U(R) \mid a \equiv 1 \pmod{(\rho - \bar{\rho})^2R}\}$ and $B = \{b \in U(S) \mid b \equiv 1 \pmod{(\rho - \bar{\rho})S}\}$.*

Proof. If a is in A we will write $f_a: G \times G \to S$ for the map defined by $f_a(id, id) = f_a(id, \sigma) = f_a(\sigma, id) = 1$ and $f_a(\sigma, \sigma) = a$. By Lemma 4.21 there is a w in S^3 with $h_2(w) = f_a$. Since h_2 is injective (Remark 4.2), w is unique and we write $g: A \to S^3$ for the mapping which takes a to w. Since $f_a \cdot f_{a'} = f_{aa'}$ and h_2 is multiplicative, it follows that g is a group homomorphism with $g(A)$ contained in $U(S^3)$. Furthermore, by an easy computation, f_a is a 2-cocycle, which by the injectivity of h_3, forces $g(a)$ to be an Amitsur 2-cocycle. Thus g induces a homomorphism $g^*: A \to H^2(S/R, U)$, which by Lemma 4.23 has kernel $N(B)$.

To complete the proof we must show that g^* is surjective, so let w be an arbitrary Amitsur 2-cocycle in $U(S^3)$. As demonstrated in Lemma 4.13, we can without loss of generality assume $h_2(w)(id, id)=1$.

Since $h_2(w)$ must be a cocycle of $E^2(G, U(S))$, we obtain

$$\frac{\sigma^i(h_2(w)(\sigma^j, \sigma^k))}{h_2(w)(\sigma^{i+j}, \sigma^k)} \cdot \frac{h_2(w)(\sigma^i, \sigma^{j+k})}{h_2(w)(\sigma^i, \sigma^j)} = 1$$

for $i, j, k = 0, 1$. When $i = 0, j = 0, k = 1$ we obtain $h_2(w)(id, \sigma) = h_2(id, id) = 1$. When $i = 1, j = 1, k = 0$ we obtain $\sigma(h_2(w)(\sigma, id)) = h_2(w)(id, \sigma) = 1$. Finally, when $i = j = k = 1$, we obtain $\sigma(h_2(w)(\sigma, \sigma)) = h_2(w)(\sigma, \sigma)$. Therefore, $h_2(w)(\sigma, \sigma)$ is in $U(S) \cap K = U(R)$. Thus we have $h_2(w)(id, \sigma) = h_2(w)(\sigma, id) = h_2(w)(id, id) = 1$ and $h_2(w)(\sigma, \sigma) = a$, for some a in $U(R)$. But then Lemma 4.21 yields that a is in A, hence class $(w) = g^*(a)$, completing the proof.

COROLLARY 4.25. *Let R be an integrally closed domain whose quotient field K has characteristic different from 2, and suppose 2 is not in $U(R)$. Let $S = R(\sqrt{d})$ where d is an element of R.*

(1) *If $U(R)$ is a torsion group, then $H^2(S/R, U)$ is trivial.*

(2) *If $U(R)$ is a finitely generated group of rank n, then $H^2(S/R, U) \subseteqq (Z/2Z)^n$.*

Proof. (1): In the notation of Theorem 4.24, $H^2(S/R, U) \cong A/N(B)$. Let x be an element of A of order p^r, where p is a prime and $r > 0$. If p is odd then $N(x^{(1-p^r)/2}) = x$, making x trivial in $A/N(B)$. On the other hand, suppose $p = 2$. Since x is in A, $x \equiv 1 \pmod{(\rho - \bar{\rho})^2 R}$ or $1 - x = 4dy$ for some y in R. But, letting $t = 1 + x + x^2 + \cdots + x^{(2^{r-1}-1)}$, we obtain $(1 - x^{2^{r-1}}) = (1 - x)t = 4dyt$. Then, since $x^{2^{r-1}} = -1$, $2 = 4dyt$ or $1 = 2dyt$. This is a contradiction, since we assumed 2 was not a unit. Thus $A/N(B)$ contains no non-trivial elements of prime order. Since A was torsion, this implies $A/N(B) = 0$.

(2): Since $A \subseteqq U(R)$ we can decompose A as $T \times F$ where T is a torsion group and F is free abelian group of rank $\leqq n$. The proof of (1) shows that $T \subseteqq N(B)$, hence $H^2(S/R, U) \cong F \cdot N(B)/N(B)$. Thus $H^2(S/R, U)$ is generated by n or fewer elements. But $F^2 \subseteqq A^2 \subseteqq N(B)$ implies $2H^2(S/R, U) = 0$, yielding the conclusion.

REMARK 4.26. If R is the ring of integers in an algebraic number field K, which has r real embeddings and s conjugate pairs of complex embeddings, then the last corollary implies

$$H^2(S/R, U) \subseteqq (Z/2Z)^{r+s-1}.$$

In particular, $H^2(S/R, U)$ vanishes if R is Z or the ring of integers in an imaginary quadratic number field.

We note that if $U(R) = \{\pm 1\}$ and K has characteristic different from 3, 4.25(1) applies. In that case this result compares closely to [7, Proposition 1.9].

THEOREM 4.27. *If S is the ring of integers in $Q(\sqrt{d})$, then $H^2(S/Z, U)$ is trivial* (cf. [14] Theorems 3.0 and 3.2, [7] Remark 1.10(b)).

Suppose in addition the class number of S is odd. Then if $d \not\equiv 1 \pmod 8$, $\mathrm{Br}(S/Z) = 0$. If $d \equiv 1 \pmod 8$, $\mathrm{Br}(S/Z)$ has at most 2 elements.

Proof. The second assertion follows from the first, Theorem 3.15 and [5, Theorem 7.6].

If $d \not\equiv 1 \pmod 4$, by Lemma 3.1 $S = R(\sqrt{d})$ and $H^2(S/Z, U)$

vanishes by Corollary 4.25. If $d \equiv 1 \pmod 4$, then by Lemma 3.1, $S = R[\rho]$ where $\rho = (1 + \sqrt{d})/2$. By Theorem 4.24, $H^2(S/R, U) \cong A/N(B)$, and $A \subsetneqq \{\pm 1\}$. However, for -1 to be in A, $2 = 1 - (-1)$ must be in $(\rho - \bar{\rho})^2 R = dR$. This implies $d = 2, -2$ or -1, none of which is congruent to $1 \pmod 4$.

REMARK 4.28. The last theorem and [5, Theorem 7.6] yields that the sequence $0 \rightarrow \mathrm{Br}(S/\boldsymbol{Z}) \rightarrow H^1(S/\boldsymbol{Z}, \mathrm{Pic}) \rightarrow H^3(S/\boldsymbol{Z}, U)$ is exact where S is the ring of integers in any quadratic extension field of $\boldsymbol{Q}$. However, by Theorem 3.15, $H^1(S/\boldsymbol{Z}, \mathrm{Pic})$ does not always vanish even when the class number of S is odd. Therefore, any further attempt along these lines to prove $\mathrm{Br}(S/\boldsymbol{Z})$ is trivial must show that

$$H^1(S/\boldsymbol{Z}, \mathrm{Pic}) \rightarrow H^3(S/\boldsymbol{Z}, U)$$

is injective, and the simple calculation of the groups themselves will not suffice.

REFERENCES

1. M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc., **97** (1960), 367-409.
2. H. Bass, *Algebraic K-theory*, Benjamin, 1968.
3. N. Bourbaki, *Elements de Mathematique*, Algebra Commutative, Ch. 2, Hermann, Paris, 1961.
4. S. U. Chase, D. K. Harrison, and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Amer. Math. Soc. Memoir, No. **52** (1965), 1-19.
5. S. U. Chase and A. Rosenberg, *Amitsur cohomology and the Brauer group*, Amer. Math. Soc. Memoir, No. **52** (1965), 20-64.
6. D. Dobbs, *Amitsur cohomology of cubic extensions of algebraic integers*, Israel J. Math., **14**, (1973), 213-220.
7. ———, *On inflation and torsion of Amitsur cohomology*, Canad. J. Math., **24** (1972), 239-260.
8. R. M. Fossum, *The Noetherian Different of Projective Orders*, Thesis, University of Michigan, 1963.
9. G. Garfinkel, *Amitsur Cohomology and an Exact Sequence Involving Pic and the Brauer Group*, Ph. D. thesis, Cornell University, Ithaca, (1968).
10. H. Hasse, *Zahlentheorie*, Akademie-Verlag, 1949.
11. G. Hochschild, *Local class field theory*, Annals of Math., **51** (1950), 339.
12. S. Lang, *Algebraic Numbers*, Addison-Wesley, 1965.
13. J. Milnor, *Introduction to algebraic K-theory*, Annals of Math. Studies, **72** (1971).
14. R. A. Morris, *On the Brauer group of Z*, Pacific J. Math., **39** (1971), 619-630.
15. D. Rim, *An exact sequence in Galois cohomology*, Proc. Amer. Math. Soc., **16** (1965), 837-840.
16. E. Wess, *Algebraic Number Theory*, McGraw-Hill, 1963.
17. H. Weber, *Theorie der Abel'schen Zahlkorper*, Acta Math., **8** (1886).
18. O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1, D. van Nostrand, 1958.

Received August 10, 1973 and in revised form October 22, 1974.

EMORY UNIVERSITY