[3] N.G. De Bruijn, *On the number of positive integers* $\leqslant x$ *and free of prime factors* $> y$, Koninkl. Nederl. Akademie Van Wetenschappen, Series A, 54 (1951), 49–60.
[4] J.M. De Koninck et A. Ivić, *The distribution of the average prime divisor of an integer*, Arch. Math. 43 (1984), 37–43.
[5] J.M. De Koninck et R. Sitaramachandrarao, *Sums involving the largest prime divisor of an integer*, Acta Arith. 48 (1987), 1–8.
[6] P. Erdős, A. Ivić et C. Pomerance, *On sums involving reciprocals of the largest prime factor of an integer*, Glasnik Matematicki 2 (1986), 27–44.
[7] A. Hildebrand, *On the number of positive integers* $\leqslant x$ *and free of prime factors* $> y$, J. Number Theory 22 (1986), 289–307.
[8] J. Karamata, *Sur un mode de croissance régulière des fonctions*, Mathematica (Cluj) 4 (1930), 38–53.
[9] G.J. Rieger, *On two arithmetic sums*, Notices of A.M.S., 74t-A-177.
[10] E. Seneta, *Regularly varying functions*, LNM 508, Springer-Verlag, Berlin, Heidelberg, New York 1976.

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ LAVAL
Québec, G1K 7P4
Canada

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ DU QUÉBEC
Chicoutimi, G7H 2B1
Canada

Reçu le 2.1.1987
et dans la forme modifiée 14.7.1987 (1696)

ACTA ARITHMETICA
LII (1989)

On the 2-Sylow subgroup of the Hilbert kernel of K_2 of number fields

by

ALAN CANDIOTTI (Madison, N.J.) and KENNETH KRAMER (Flushing, N.Y.)

1. Introduction. Let F be a number field. For each non-complex completion F_v of F, let m_v be the order of the group of roots of unity $\mu_v = \mu(F_v)$. Let λ_v: $F_v^* \times F_v^* \to \mu_v$ denote the Hilbert norm residue symbol ([11], Remark 15.10), as well as the corresponding map from $K_2 F$ to μ_v. By convention, we take λ_v and μ_v to be trivial at complex places. For non-Archimedean v, let q_v be the exact power of the residue characteristic dividing m_v and let k_v be the residue field. The tame symbol λ_v^{tame}: $K_2 F \to k_v^*$ is obtained from $\lambda_v^{q_v}$ by reducing modulo v.

Let S be a finite set of places of F including the Archimedean ones and those above the rational prime p. If O_S is the ring of S-integers of F, we may define $K_2 O_S$ as the kernel of all tame symbols on $K_2 F$ at places outside S. Assume that F contains the qth roots of unity μ_q, where q is a power of p. Let A_S be the ideal class group of F modulo the subgroup generated by classes of ideals over S. By [12], Theorem 6.2, A_S is related to the tame kernel by an exact sequence of the form

$$(1) \qquad 0 \to A_S/(A_S)^q \to K_2 O_S/(K_2 O_S)^q \to \prod_{\substack{v \in S - \{v_0\} \\ v \text{ not complex}}} \mu_q \to 0.$$

Let $R_2 F$ be the kernel of all Hilbert symbols. In Section 2 we give an analogous idelic interpretation of $R_2 F/(R_2 F)^q$.

Suppose instead that F is a totally real number field with ring of integers 0. Let $K_2 O$ be the kernel of all tame symbols. According to a conjecture of Birch and Tate, the order of $K_2 O$ is $w_F |\zeta_F(-1)|$, where ζ_F is the Dedekind zeta-function of F and

$$w_F = 4 \prod_{[E:F]=2} \{(1/2)|\mu(E)|\}$$

with the product being taken over quadratic extensions E of F. When F is an abelian extension of $\boldsymbol{Q}$ the Birch–Tate formula is correct at least up to multiplication by powers of 2. This is a deep theorem, depending on work of Coates [4], Greenberg [8] and Mazur and Wiles [10].

Various authors ([2], [7], [13]) have verified certain cases of the 2-primary part of the Birch–Tate conjecture. Perhaps the most general is a result of Kolster [9] showing that it holds whenever the 2-Sylow subgroup of $K_2 O$ is elementary abelian. In particular, this includes certain fields F which are not abelian over $\mathbf{Q}$. Kolster relates $K_2 O$ to a certain "relative ideal class group" for the extension $E = F(i)$ and uses the zeta-function computation of Brown [3].

In Section 3 we apply methods similar to Kolster's to study $R_2 F$ in terms of a slightly different "relative idele group" denoted $I(E/F)$. In Theorem 3.1, we give general conditions under which $R_2 F$ has the same number of direct summands of order exactly 2^n as $I(E/F)$. These conditions hold if, for example, $n < \operatorname{ord}_2 |\mu(E)|$ and there is one prime over 2 in E. It would be interesting to know more about $I(E/F)$. For example, using [5], it can be shown that $I(E/F)$ is finite if and only if Gross's 2-adic regulator R_E does not vanish. We are happy to acknowledge here the helpful comments of Leslie Federer about this equivalence.

In Section 4 we show that for real quadratic fields $F = \mathbf{Q}(\sqrt{D})$, the relative idele group $I(E/F)$ is easily described in terms of the ideal class group $A_S(K)$ of $K = \mathbf{Q}(\sqrt{-D})$.

In Section 5, results of Urbanowicz [13] on the exact power of 2 dividing $w_F \zeta_F(-1)$, when this power is small, then permit us to verify the 2-primary part of the Birch–Tate conjecture for infinite families of real quadratic fields such that $K_2 O[2]$ is not necessarily elementary abelian. In particular, we complete the verification of the conjectures in [13].

Notation: We let $|G|$ be the order of the finite abelian group G. We denote the p-Sylow subgroup of G by $G[p]$ and the kernel of multiplication by p on G by ${}_pG$.

2. An idelic interpretation of the wild kernel. Let F be a number field which contains a primitive p-power root of unity ζ_q. Let $m = |\mu(F)|$ and $m_v = |\mu(F_v)|$. Let J denote idele group of F, consisting of valuation vectors (a_v) such that $a_v \in F_v^*$ and a_v is in the local units U_v of F_v^* for all but finitely many v. Denote the principal ideles by $\mathbf{F}$. Throughout this section, we fix S_0 to consist of the complex places of F and a place v_0 such that m_{v_0}/m is not divisible by p.

PROPOSITION 2.1. *Let* $\eta = \prod_{v \in S_0} F_v^* \times \prod_{v \notin S_0} \eta_v$ *where*

$$\eta_v = \{x \in F_v^* \mid \lambda_v \{\zeta_q, x\} = 1\} = \{x \in F_v^* \mid x \text{ is a norm from } F_v(\zeta_{qm_v})\}.$$

If v is prime to p, then $\eta_v = U_v F_v^{*q}$. For each $\alpha = (a_v) \in J$ there exist elements $t(\alpha)$ in $K_2 F$ such that $\lambda_v \{t(\alpha)\} = \lambda_v \{\zeta_q, a_v\}$ for all $v \notin S_0$. There is an isomorphism Ψ: $J/(\eta \mathbf{F}) \to R_2 F/(R_2 F)^q$ given by $\Psi(\alpha \cdot \eta \mathbf{F}) = t(\alpha)^q (R_2 F)^q$.

Proof. We construct the following commutative diagram, in which the vertical arrows are surjective.

$$\begin{array}{ccccccccc} & & & & \mu_q \otimes F^* & \to & \mu_q \otimes J & & \\ & & & & \downarrow & & \downarrow \beta & & \\ 0 & \to & {}_q(R_2 F) & \to & {}_q(K_2 F) & \to & \prod_{v \notin S_0} \mu_q & \xrightarrow{\delta} & R_2 F/(R_2 F)^q \to 0. \end{array}$$

By Moore's theorem ([11], Theorem 16.1), there is an exact sequence

$$0 \to \operatorname{Ker} h \to K_2 F \xrightarrow{h} \prod_{v \notin S_0} \mu_v \to 0$$

in which the map h is given by Hilbert symbols. Since m_{v_0}/m is prime to p, the reciprocity law forces $\operatorname{Ker} h$ and $R_2 F$ to have the same p-Sylow subgroup. It follows from [12], Proposition 4.3, that $R_2 F \subset (K_2 F)^q$. By the snake lemma for multiplication by q in Moore's exact sequence, the bottom row of our diagram is exact.

The first vertical arrow sends $\zeta \otimes f \in \mu_q \otimes F^*$ to $\{\zeta, f\}$ and is surjective by [12], Theorem 6.1. The second vertical arrow β sends $\zeta \otimes (a_v) \in \mu_q \otimes J$ to $(\lambda_v(\zeta, a_v))$. Since λ_v gives a perfect self-pairing of $F_v^*/(F_v^*)^{m_v}$, the map $\lambda_v \{\zeta_q, \ \}$: $F_v^* \to \mu_q$ is surjective and its kernel is η_v for $v \notin S_0$. Since $J^q \subset \eta$ we clearly have an isomorphism $J/\eta \cong (\mu_q \otimes J)/\operatorname{Ker} \beta$. Letting Ψ be induced by $\delta \circ \beta$, we see that Ψ is an isomorphism.

Finally, for v prime to p, $F_v(\zeta_{qm_v})$ is an unramified extension of F_v of degree q. Therefore $\eta_v = U_v F_v^{*q}$ by local class field theory.

COROLLARY 2.2. *Let L be the abelian extension of F corresponding to $J/(\eta \mathbf{F})$. Then $L = F(\varkappa^{1/q})$, where $\varkappa = \{f \in F^* \mid f \in \mu_v F_v^{*q}$ for $v \neq v_0$ and $f \in F_{v_0}^{*q}\}$.*

Proof. Let $(\ , \ )_v$ be the q-power norm residue symbol $\lambda_v^{m_v/q}$, which provides a perfect self-pairing of F_v^*/F_v^{*q}. Choose a generator ζ_v for μ_v such that $\zeta_v^{m_v/q} = \zeta_q$. Then $\lambda_v \{\zeta_q, Y\} = (\zeta_v, Y)_v$ and it is easy to see from the definition of η_v in Proposition 2.1 that the orthogonal complement of η_v/F_v^{*q} under the pairing $(\ , \ )_v$ is $(\mu_v F_v^{*q})/F_v^{*q}$.

From Kummer theory and class field theory, we have the perfect pairing

$$\langle \ , \ \rangle_F \colon J/(J^q \mathbf{F}) \times F^*/F^{*q} \to \mu_q$$

given by $\langle \ , \ \rangle_F = \prod_v (\ , \ )_v$. The orthogonal complement of $(\eta \mathbf{F})/(J^q \mathbf{F})$ in the pairing $\langle \ , \ \rangle_F$ clearly is $\varkappa/F^{*q}$. Kummer generators for the extension L are therefore given by the elements of $\varkappa$.

Remark 2.3. Let $\eta^0 = \prod \eta_v$ and $E = F(\zeta_q^{1/q})$. The argument above shows that Kummer generators for the extension of F with Galois group

$J/(\eta^0 F)$ are given by

$$\{f \in F^* \mid f \in \mu_v F_v^{*q} \text{ for all } v\}.$$

Since m_{v_0}/m is prime to p, this extension is LE. Since v_0 splits completely in L but not at all in E, we have $L \cap E = F$.

3. The wild kernel and a relative idele group. We now specialize to the case in which F is a totally real field and $p = 2$. Let $E = F(i)$. Let S_F be the set of places of F over 2 and ∞. Denote by S_F^+ (resp. S_F^-) the set of primes v of F dividing 2 such that v is split (resp., not split) in E. Let S_E (resp., $S_E^{\pm}$) be the primes of E over S_F (resp., $S_F^{\pm}$). Let $\mu_\infty = \varinjlim \mu_{2^n}$ and let

$$\mathcal{M}_w = \begin{cases} E_w^* & \text{if } w \in S_E^- \text{ or } w \mid \infty, \\ \{x \in E_w^* \mid x \text{ is a norm from } E_w(\mu_\infty)\} & \text{if } w \in S_E^+. \end{cases}$$

Let $\mathcal{M} = \prod_{w \in S_E} \mathcal{M}_w \times \prod_{w \notin S_E} U_w$. We define the "relative idele group" to be $I(E/F) = J_E/\overline{\mathcal{M} J_F E}$, where the bar denotes closure in the idele topology. The main result of this section is Theorem 3.1 below, relating the wild kernel and the relative idele group.

$I(E/F)$ is related to the S-ideal class groups of E and F as follows. Let ι: $A_S(F) \to A_S(E)$ be the map induced by lifting ideals. Then

$$A_S(E)/\iota\{A_S(F)\} \cong J_E/(J_{S_E} J_F E), \quad \text{where} \quad J_{S_E} = \prod_{w \in S_E} E_w^* \times \prod_{w \notin S_E} U_w.$$

Suppose that $S_F^+ = \{v_1, \ldots, v_n\}$ and let w_j and w_j' denote the primes over v_j in E. Then by local class field theory, $E_{w_j}^*/\mathcal{M}_{w_j} \cong \operatorname{Gal}(E_{w_j}(\mu_\infty)/E_{w_j}) \cong \mathbf{Z}_2$. Furthermore, there is an exact sequence of the form

$$\prod_{j=1}^{n} E_{w_j}^*/\mathcal{M}_{w_j} \to I(E/F) \to A_S(E)/\iota\{A_S(F)\} \to 0. \tag{2}$$

To see this, let $(z_w) \in J_E$ represent an element of $I(E/F) = J_E/\overline{\mathcal{M} J_F E}$ which becomes trivial in $J_E/(J_{S_E} J_F E)$. Correcting by an element of $\mathcal{M}$, we may assume that $z_w = 1$ for $w \notin S_E^+$. Correcting by an element lifted from $F_{v_j}^*$, we may further assume that $z_{w_j'} = 1$ for $j = 1, \ldots, n$ as desired. In Section 4 we will show that $I(E/F)$ is finite when F is a real quadratic field.

Let $\mathcal{D} = \{s \in {}_2(K_2 F) \mid \lambda_v(s) = 1 \text{ for all } v \notin S_F^-\}$ and let $\lambda = \prod_{v \in S_F^-} \lambda_v$: $K_2 F \to \prod_{v \in S_F^-} \mu_v$. Since $|\mu_v|$ is exactly divisible by 2 for all $v \in S_F^-$, reciprocity implies that $\lambda(\mathcal{D})$ is contained in the hyperplane $H_0 = \{(a_v) \in \prod_{v \in S_F^-} \{\pm 1\} \mid \prod_{v \in S_F^-} a_v = 1\}$. We say that all possible signatures occur over S_F^- if $\lambda(\mathcal{D}) = H_0$. This is trivially the case if for example there is one prime over 2 in E.

THEOREM 3.1. *Let F be a totally real field and let $E = F(i)$. Let $I(E/F) = J_E/\overline{\mathcal{M} J_F E}$. Suppose that E contains a primitive root of unity ζ_{2r} of 2-power order $2r$. Suppose further that all possible signatures occur over S_F^-. Then there is an isomorphism*

$$\Phi: {}_rI(E/F)/{}_{2r}I(E/F)^2 \to {}_r(R_2 F)/{}_{2r}(R_2 F)^2.$$

In particular, $I(E/F)$ and $R_2 F$ have the same number of direct summands of each order dividing r.

In what follows, we will use some elementary facts from class field theory which we collect here for reference. (See [6], § 2.)

Genus theory: Suppose that $\operatorname{Gal}(F_2/F_1) = \langle g \rangle$ is a finite cyclic group. Let J_j be the idele group of F_j, and let H_j be a profinite abelian extension of F_j. Suppose that $\operatorname{Gal}(H_j/F_j) \cong J_j/X_j$ in the isomorphism of class field theory. Let N: $J_2 \to J_1$ be the norm. Then:

(i) H_2 is Galois over F_1 if and only if $X_2^g = X_2$. If so, the commutator subgroup of $\operatorname{Gal}(H_2/F_1)$ is $\operatorname{Gal}(H_2/F_2)^{1-g}$, where g acts by conjugation.

(ii) Suppose H_2 is Galois over F_1. Let H_2^{ab} be the maximal subfield of H_2 abelian over F_1. Then the normic subgroup of J_1 corresponding to H_2^{ab} is $N(X_2)F_1$.

(iii) $H_2 \supset H_1$ if and only if $N(X_2) \subset X_1$. If so, we have the exact sequences below, in which the vertical arrows are isomorphisms and the map $\tilde{N}$ induced by norm corresponds to restriction on Galois groups.

$$\begin{array}{ccccccccc} 0 \to & N^{-1}(X_1)/X_2 & \to & J_2/X_2 & \xrightarrow{\tilde{N}} & J_1/X_1 & \to & J_1/\{X_1 N(J_2)\} & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & \operatorname{Gal}(H_2/H_1 F_2) & \to & \operatorname{Gal}(H_2/F_2) & \xrightarrow{\text{res}} & \operatorname{Gal}(H_1/F_1) & \to & \operatorname{Gal}(H_1 \cap F_2/F_1) & \to 0. \end{array}$$

Before proceeding to the proof of Theorem 3.1, we need the following lemmas. Fix a choice of prime v_0 not split in E and let L be the abelian extension of F corresponding to the normic subgroup ηF of J_F as in Corollary 2.2 with $q = 2$. Let M be the profinite abelian extension of E such that $\operatorname{Gal}(M/E) \cong J_E/\overline{\mathcal{M} J_F E} = I(E/F)$.

LEMMA 3.2. *Let $(\mathcal{M} J_F)_v$ be the semi-local component of $\mathcal{M} J_F$ over the prime v of F and let N_v: $\prod_{w \mid v} E_w^* \to F_v^*$ be the semi-local norm. Then $N_v(\mathcal{M} J_F)_v = \eta_v$. The norm $N_{E/F}$: $J_E \to J_F$ induces an isomorphism $\tilde{N}_{E/F}$: $J_E/(\mathcal{M} J_F J_E^2 E) \to J_F/(\eta F)$.*

We have $L \subset M$ and $L \cap E = F$. In fact, LE is the maximal abelian extension of F contained in M and the maximal elementary 2-extension of E contained in M.

The groups $I(E/F)$ and $R_2 F$ have the same 2-rank.

Proof. By definition, $\eta_v = \{x \in F_v^* \mid x \text{ is a norm from } F_v(\zeta_{2m_v})\}$. Suppose first that $v \in S_F^+$. Let $X = \{x \in F_v^* \mid x \text{ is a norm from } F_v(\mu_\infty)\}$. It follows from local class field theory and the fact that $F_v(\mu_\infty)$ is cyclic over F_v, that $\eta_v = X \cdot F_v^{*2}$, which clearly equals $N_v(\mathcal{M}J_F)_v$. Suppose next that v is archimedean or $v \in S_F^-$. Then $|\mu_v|$ is exactly divisible by 2. Let w lie over v in E. Since $F_v(\zeta_{2m_v})^* = F_v(i)^* = E_w^* = \mathcal{M}_w$ we have $\eta_v = N_v(E_w^*) = N_v(\mathcal{M}J_F)_v$. Finally, for $v \notin S_F$, the group of local norms of units is all of U_v. Hence $N_v(\mathcal{M}J_F)_v = U_v F_v^{*2} = \eta_v$ as desired. In the notation of Remark 2.3, $N_{E/F}(\mathcal{M}J_F) = \eta^0 = \prod_v \eta_v$ and $\operatorname{Gal}(LE/F) \cong J_F/\eta^0 F$.

By genus theory (i), M is Galois over F. Let M^{ab} be the maximal subfield of M abelian over F. Then

$$\operatorname{Gal}(M^{ab}/F) \cong J_F/\{N_{E/F}(\mathcal{M}J_F)F\} = J_F/(\eta^0 F) \cong \operatorname{Gal}(LE/F).$$

Hence $M^{ab} = LE$. Furthermore

$$\operatorname{Gal}(M^{ab}/E) \cong J_E/(\mathcal{M}J_F J_E^{1-\sigma} E).$$

But $J_E^{1-\sigma} J_F = J_E^2 J_F$. Therefore M^{ab} also is the maximal elementary 2-extension of E contained in M. By Remark 2.3, we have $L \cap E = F$. Hence $\tilde{N}_{E/F}$ is an isomorphism by genus theory (iii). It follows from this isomorphism and Proposition 2.1 that $I(E/F)$ and $R_2 F$ have the same 2-rank.

The next two lemmas are minor modifications of results of [9] in which we pay more attention to wild symbols for places over 2. For each prime v of F, let $(J_E)_v = \prod_{w|v} E_w^*$. If $z = (z_w) \in J_E$ we use boldface $\mathbf{z}_v \in (J_E)_v$ to denote the projection of z on $(J_E)_v$. If there are 2 primes w and w' over v in E and $e \in E^*$, we denote the element $(\{e, z_w\}, \{e, z_{w'}\}) \in K_2 E_w \times K_2 E_{w'}$ by $\{e, \mathbf{z}_v\}$.

Lemma 3.3. *Suppose that $\zeta_{2r} \in E$, where $r \geqslant 2$ is a power of 2. Let $b \in E^*$ and suppose that the principal idele $(b) \in (z_w)^r \mathcal{M}J_F$. Then*

$$\lambda_v \operatorname{Tr}\{\zeta_{2r}, b\} = \lambda_v\{-1, N_v \mathbf{z}_v\}$$

for each prime $v \notin S_F^-$.

Proof. Let $\operatorname{Tr}_v\colon \prod_{w|v} K_2 E_w \to K_2 F_v$ be the semi-local transfer map. In our context $[E:F] = 2$, so that the semi-local transfer is the usual transfer if v does not split in E, and is the product otherwise. By [1], Proposition 2, we have commutative diagram

$$\begin{array}{ccccc} K_2 E & \to & \prod_{w|v} K_2 E_w & \to & \prod_{w|v} \mu_w \\ \operatorname{Tr}\downarrow & & \downarrow \operatorname{Tr}_v & & \downarrow \theta \\ K_2 F & \to & K_2 F_v & \overrightarrow{\lambda_v} & \mu_v \end{array} \qquad (3)$$

in which $\theta_w(\zeta_w) = \zeta_w^{m_w/m_v}$ and $\theta = \prod_{w|v} \theta_w$.

Consider the principal idele

$$(b) = (z_w)^r (x_w)(a_v) \quad \text{with } (x_w) \in \mathcal{M} \text{ and } (a_v) \in J_F.$$

In the embedding of b to $\mathbf{b} \in (J_E)_v$ we have $\mathbf{b} = \mathbf{z}_v^r \mathbf{x}_v \mathbf{a}_v$. Using the fact that $N_{E/F}(\zeta_{2r}) = 1$, it is easy to see that $\operatorname{Tr}_v\{\zeta_{2r}, \mathbf{a}_v\} = 1$. It follows from the definition of $\mathcal{M}$ that $\lambda_w\{\zeta_{2r}, x_w\} = 1$ for all $w \notin S_E^-$. Hence $\lambda_v \operatorname{Tr}_v\{\zeta_{2r}, \mathbf{x}_v\} = 1$ for all $v \notin S_F^-$. Hence, for $v \notin S_F^-$, we have

$$\lambda_v \operatorname{Tr}\{\zeta_{2r}, b\} = \lambda_v \operatorname{Tr}_v\{\zeta_{2r}, \mathbf{b}\} = \lambda_v \operatorname{Tr}_v\{\zeta_{2r}, \mathbf{z}_v^r \mathbf{x}_v \mathbf{a}_v\}$$
$$= \lambda_v \operatorname{Tr}_v\{-1, \mathbf{z}_v\} = \lambda_v\{-1, N_v \mathbf{z}_v\}$$

as claimed.

Lemma 3.4. *Suppose that r is a power of 2 and that $\zeta_{2r} \in E$. Then every element of ${}_r(R_2 F)$ has the form $\operatorname{Tr}_{E/F}\{\zeta_r, b\}$ for some $b \in E^* \cap (J_E^r \mathcal{M}J_F)$.*

Proof. We use induction on the power of 2 in r. There is nothing to prove if $r = 1$. Suppose $r \geqslant 2$. Let $\Delta(r) = E^* \cap (J_E^r \mathcal{M}J_F)$. Given $s \in {}_r(R_2 F)$ we can by induction hypothesis find $b_1 \in \Delta(r/2)$ such that $s^2 = \operatorname{Tr}\{\zeta_{r/2}, b_1\}$. Then $s = \{-1, f\} \cdot \operatorname{Tr}\{\zeta_r, b_1\}$ for some $f \in F^*$. Since s is in $R_2 F$ and $\operatorname{Tr}\{\zeta_r, b_1\} = \operatorname{Tr}\{\zeta_{2r}, b_1\}^2 \in (K_2 F)^2$ all quadratic norm-residue symbols vanish on $\{-1, f\}$. Hence f is a global norm. Write $f = Ne$ for some $e \in E^*$. Then $\{-1, f\} = \operatorname{Tr}\{-1, e\} = \operatorname{Tr}\{\zeta_r, e^{r/2}\}$. Hence $s = \operatorname{Tr}\{\zeta_r, b\}$ with $b = b_1 e^{r/2}$. Clearly b is still in $\Delta(r/2)$, so that the principal idele (b) is an element of $(z_w)^{r/2} \mathcal{M}J_F$ for some $(z_w) \in J_E$.

For primes $w \in S_E^-$, b trivially is in $\mathcal{M}_w = E_w^*$. Suppose that $v \notin S_F^-$. Then $1 = \lambda_v(s) = \lambda_v \operatorname{Tr}\{\zeta_r, b\} = \lambda_v\{-1, N_v \mathbf{z}_v\}$, with the last equality by Lemma 3.3. It follows that $N_v \mathbf{z}_v \in \eta_v$. By Lemma 3.2, there exists $\mathbf{y}_v \in (\mathcal{M}J_F)_v$ such that $N_v \mathbf{y}_v = N_v \mathbf{z}_v$. Then by Hilbert's Theorem 90, $\mathbf{z}_v/\mathbf{y}_v \in (J_E)_v^{1-\sigma} \subset (J_E)_v^2 F_v^*$. Therefore $(z_w) \in J_E^2 \mathcal{M}J_F$. Hence $b \in \Delta(r)$, completing the induction.

Proof of Theorem 3.1. We also denote by $\tilde{N}$ the map ${}_r I(E/F) \to J_F/(\eta F)$ induced by norm. By Lemma 3.2 and Proposition 2.1, the composition $\Phi = \Psi \circ \tilde{N}\colon {}_r I(E/F) \to R_2 F/(R_2 F)^2$ is well-defined, and

$$\operatorname{Ker} \Phi = {}_{2r} I(E/F)^2.$$

Next we show that Image $\Phi = {}_r(R_2 F)/{}_{2r}(R_2 F)^2$. Suppose that $(z_w) \in J_E$ represents an element of ${}_r I(E/F)$. Then there exists $b \in E^*$ such that $(b) \in (z_w)^r \mathcal{M} J_F$. Let $N_{E/F}(z_w) = (a_v)$. By Lemma 3.3, we have $\lambda_v \operatorname{Tr}\{\zeta_{2r}, b\} = \lambda_v \{-1, a_v\}$ for all $v \notin S_F^-$. Using the assumption that all possible signatures occur over S_F^-, we can adjust $\operatorname{Tr}\{\zeta_{2r}, b\}$ by an element $\{-1, f\}$ in $K_2 F$ so that

$$\lambda_v(\{-1, f\} \cdot \operatorname{Tr}\{\zeta_{2r}, b\}) = \lambda_v\{-1, a_v\} \quad \text{for all } v.$$

In the notation of Proposition 2.1, we may choose

$$t(a_v) = \{-1, f\} \cdot \operatorname{Tr}\{\zeta_{2r}, b\}.$$

Then

$$\Phi(z_w) = \Psi \circ N(z_w) = \Psi(a_v) = t(a_v)^2 = \operatorname{Tr}\{\zeta_r, b\} \in {}_r(R_2 F) \pmod{{}_{2r}(R_2 F)^2}.$$

By Lemma 3.4, the map Φ is onto ${}_r(R_2 F)/{}_{2r}(R_2 F)^2$. This completes the proof.

4. Quadratic fields. Throughout this section $F = \boldsymbol{Q}(\sqrt{D})$ is a real quadratic field with square-free D. Let $K = \boldsymbol{Q}(\sqrt{-D})$ and $E = F(i)$. Let σ generate $\operatorname{Gal}(E/F)$ and let τ generate $\operatorname{Gal}(E/K)$. Let $I(E/F) = J_E/\overline{\mathcal{M} J_F E} \cong \operatorname{Gal}(M/E)$ be the relative idele group described in Section 3. By class field theory, the S-ideal class group $A_S(K)$ is isomorphic to $\operatorname{Gal}(H/K)$, where H is the maximal unramified abelian extension of K split over S_K. Our first step is to identify the relative S-ideal class group $A_S(E)/\iota\{A_S(F)\} \cong J_E/(J_{S_E} J_F \boldsymbol{E})$ of exact sequence (2) in terms of $A_S(K) \cong J_K/(J_{S_K} \boldsymbol{K})$.

Lemma 4.1. *The following sequence is exact*

$$0 \to J_E/(J_{S_E} J_F \boldsymbol{E}) \xrightarrow{\tilde{N}_{E/K}} J_K/(J_{S_K} \boldsymbol{K}) \to \operatorname{Gal}(H \cap E/K) \to 0.$$

Proof. For clarity, we make explicit the inclusion maps such as $i_F^E\colon J_F \to J_E$. Let $\boldsymbol{U}_{\boldsymbol{Q}}$ denote the subgroup of $J_{\boldsymbol{Q}}$ whose components are units at non-archimedean places and arbitrary at archimedean places. Since $\boldsymbol{Q}$ has class number 1, we have $J_{\boldsymbol{Q}} = \boldsymbol{U}_{\boldsymbol{Q}} \boldsymbol{Q}$. Hence

$$N_{E/K}\{i_F^E(J_F)\} = i_{\boldsymbol{Q}}^K\{N_{F/\boldsymbol{Q}}(J_F)\} \subset i_{\boldsymbol{Q}}^K(J_{\boldsymbol{Q}}) = i_{\boldsymbol{Q}}^K(\boldsymbol{U}_{\boldsymbol{Q}} \boldsymbol{Q}). \tag{4}$$

It follows that the map $\tilde{N}_{E/K}\colon J_E/(J_{S_F} J_F \boldsymbol{E}) \to J_K/(J_{S_K} \boldsymbol{K})$ induced by the norm is well-defined. Furthermore, $\operatorname{coker} \tilde{N}_{E/K} \cong \operatorname{Gal}(H \cap E/K)$ by genus theory (iii). Since $C = \boldsymbol{Q}(i)$ also has class number 1, we have

$$J_E^{1+\sigma\tau} = i_C^E(N_{E/C} J_E) \subset i_C^E(J_C) = i_C^E(\boldsymbol{U}_C \boldsymbol{C}). \tag{5}$$

Clearly σ acts by inversion on $J_E/(J_{S_E} J_F \boldsymbol{E})$. Hence $J_E^{1-\tau} \subset J_{S_E} J_F \boldsymbol{E}$.

To determine the kernel of $\tilde{N}_{E/K}$, suppose that $N_{E/K}(z_w) = (a_\varrho k) \in J_{S_K} \boldsymbol{K}$. Because E over K is unramified outside 2 and $a_\varrho \in U_\varrho$ for $\varrho \notin S_K$, the global element k is a norm from the completions of E everywhere locally except possibly over 2. If there is one prime over 2 in K, then by reciprocity k is a norm from E. If there are 2 primes over 2 in K, then we may replace k by $\pm k$ as necessary to insure that k is a norm from E locally at one of the completions of K over 2. Then k is a global norm from E again by reciprocity. Clearly then $(a_\varrho) \in N_{E/K}(J_{S_E})$. It follows from Hilbert's Theorem 90 that $N_{E/K}^{-1}(J_{S_K} \boldsymbol{K}) \subset J_{S_E} \boldsymbol{E} J_E^{1-\tau} \subset J_{SE} J_F \boldsymbol{E}$. Hence $\tilde{N}_{E/K}$ is injective, as desired.

We are now ready to relate $I(E/F)$ to $A_S(K)$ depending on the factorization of 2 in F.

Corollary 4.2. *If $D \not\equiv \pm 1 \pmod 8$, then $I(E/F) \cong A_S(K)$.*

Proof. Use exact sequence (2) and Lemma 4.1, noting that $H \cap E = K$ and S_F^+ is empty.

Corollary 4.3. *If $D \equiv 1 \pmod 8$, then there is an exact sequence*

$$0 \to I(E/F) \to A_S(K) \to \operatorname{Gal}(E/K) \to 0$$

which splits if and only if all possible signatures occur over S_F^-.

Proof. Exactness follows from (2) and Lemma 4.1. The sequence splits if and only if the induced map $N_0\colon J_E/(J_{S_E} J_F J_E^2 \boldsymbol{E}) \to J_K/(J_{S_K} J_K^2 \boldsymbol{K})$ is injective. Suppose $z \in J_E$ represents an element of the kernel of N_0. Then $N_{E/K} z \in a^2 J_{S_K} \boldsymbol{K}$ for some $a \in J_K$. Hence $N_{E/K}(za^{-1}) \in J_{S_K} \boldsymbol{K}$. It follows from the injectivity of $\tilde{N}_{E/K}$ in Lemma 4.1 that $za^{-1} \in J_{S_E} J_F \boldsymbol{E}$. Hence

$$\operatorname{Ker} N_0 = \{i_K^E(J_K) J_{S_E} J_F J_E^2 \boldsymbol{E}\}/(J_{S_E} J_F J_E^2 \boldsymbol{E}).$$

From the isomorphism $\tilde{N}_{E/F}$ of Lemma 3.2, noting that $\mathcal{M} = J_{S_E}$, we see that $\operatorname{Ker} N_0$ is trivial if and only if $N_{E/F}\{i_K^E(J_K)\} \subset \eta \boldsymbol{F}$. Furthermore, $N_{E/F}\{i_K^E(J_K)\} = i_{\boldsymbol{Q}}^F\{N_{K/\boldsymbol{Q}}(J_K)\}$.

From Kummer theory and class field theory we have the perfect pairing

$$\langle\,,\rangle_{\boldsymbol{Q}}\colon J_{\boldsymbol{Q}}/\{N_{K/\boldsymbol{Q}}(J_K)\, \boldsymbol{Q}\} \times \{\text{Subgroup of } \boldsymbol{Q}^*/\boldsymbol{Q}^{*2} \text{ generated by } -D\} \to \mu_2$$

given by the product of quadratic norm-residue symbols for all rational primes including ∞. Since $J_{\boldsymbol{Q}} = \boldsymbol{U}_{\boldsymbol{Q}} \boldsymbol{Q}$ it is easy to see that

$$N_{K/\boldsymbol{Q}}(J_K)\, \boldsymbol{Q} = X \boldsymbol{Q}, \quad \text{where } X = \{(x_p) \in \boldsymbol{U}_{\boldsymbol{Q}} \mid \langle (x_p), -D \rangle_{\boldsymbol{Q}} = 1\}.$$

Fix a rational prime l dividing D and consider the idele $\alpha = (\alpha_p) \in \boldsymbol{U}_{\boldsymbol{Q}}$ whose entries are 1, except for $a_2 = -1$ and $a_l \in U_l - U_l^2$. Given an idele $x \in X$, we can multiply by suitable powers of α or the principal idele (-1) to obtain an idele $x' = (x'_p) = (-1)^a \alpha^b x$ for which $x'_\infty > 0$ and x'_2 is a norm from $\boldsymbol{Q}_2(i)^*$. Hence $i_{\boldsymbol{Q}}^F(x') \in \eta$. It follows that $i_{\boldsymbol{Q}}^F\{N_{K/\boldsymbol{Q}}(J_K)\} \subset \eta \boldsymbol{F} \Leftrightarrow i_{\boldsymbol{Q}}^F(\alpha) \in \eta \boldsymbol{F} \Leftrightarrow$ there exists an element $f \in F^*$ such that

$$\lambda_v\{-1,f\} = \begin{cases} 1, & v \nmid 2, \\ -1, & v \mid 2. \end{cases}$$

Hence the sequence splits if and only if all possible signatures occur over S_F^-.

PROPOSITION 4.4. *Suppose that $D \equiv -1 \pmod 8$. Let π and π' be the primes over 2 in K. Let $U_2 = \{u \in \mathbf{Z}_2 \mid u \equiv 1 \pmod 4\}$. Let $U_{\{\pi'\}} = \{k \in K^* \mid k$ is a unit outside $\pi'\}$. Denote the closure of its image in $K_\pi \cong \mathbf{Q}_2$ by $\bar{U}_{\{\pi'\}}$. Then there is a split exact sequence*

$$0 \to U_2/\bar{U}^2_{\{\pi'\}} \to I(E/F) \to A_S(K) \to 0.$$

Proof. Let v and v' denote the primes of E over π and π'. The semi-local component of $\mathcal{M}J_F$ over 2 is $\{(\alpha\beta, \gamma\beta) \mid \alpha \in \mathcal{M}_v, \gamma \in \mathcal{M}_{v'}$ and $\beta \in \mathbf{Q}_2(i)^*\}$. By transitivity of norm,

$$N_{v/\pi}(\mathcal{M}_v) = \{x \in \mathbf{Q}_2^* \mid x \text{ is a norm from } \mathbf{Q}_2(\mu_\infty)\}.$$

This is well known to be the cyclic subgroup of $\mathbf{Q}_2^*$ generated by 2. Using (4) it follows that

$$N_{E/K}(\mathcal{M}J_F) \subset (T \times \mathbf{C}^* \times \prod_{\varrho \notin S_K} U_\varrho)K \quad \text{where} \quad T = \{(2^a b, 2^c b) \mid a, c \in \mathbf{Z}, b \in U_2\}.$$

Conversely, suppose $N_{E/K}(x_w) \in (T \times \mathbf{C}^* \times \prod_{\varrho \notin S_K} U_\varrho)(k)$ for some principal idele (k). Clearly $(T \times \mathbf{C}^* \times \prod_{\varrho \notin S_K} U_\varrho) \subset N_{E/K}(\mathcal{M}J_F)$. Then k is a norm everywhere locally, and hence globally from E^*. Hence $(x_w) \in \mathcal{M}J_F\,\mathbf{E} \cdot \operatorname{Ker} N_{E/K}$. It follows from (5) that $J_E^{1+\sigma\tau} \subset \mathcal{M}J_F\,\mathbf{E}$. Hence $\operatorname{Ker} N_{E/K} = J_E^{1-\tau} \subset \mathcal{M}J_F\,\mathbf{E}$. We have therefore shown that

$$(6) \qquad (x_w) \in \mathcal{M}J_F\,\mathbf{E} \quad \text{if and only if} \quad N_{E/K}(x_w) \in (T \times \mathbf{C}^* \times \prod_{\varrho \notin S_K} U_\varrho)\,\mathbf{K}.$$

By Lemma 4.1, we have $A_S(E)/\iota\{A_S(F)\} \cong A_S(K)$. From (2) we obtain the exact sequence

$$0 \to E_v/\bar{X} \to I(E/F) \to A_S(K) \to 0$$

with $X = \{x \in E_v^* \mid (x, 1, 1, \ldots) \in \mathcal{M}J_F\,\mathbf{E}\}$. Let

$$Y = \{y \in U_2 \mid (y, 1, 1, \ldots) \in (T \times \mathbf{C}^* \times \prod_{\varrho \notin S_K} U_\varrho)\,\mathbf{K}\}.$$

Since X contains a prime element of E_v, we have $E_v^*/\bar{X} \cong U_v/(U_v \cap \bar{X}) = U_2/\bar{Y}$, the last isomorphism being induced by $N_{v/\pi}$ in view of (6).

We determine Y more explicitly. If $(y, 1, 1, \ldots) \in (T \times \mathbf{C}^* \times \prod_{\varrho \notin S_K} U_\varrho)(k)$

for some principal idele (k), then k must be a unit outside 2. Furthermore, replacing k by $k/2^{\operatorname{ord}_\pi(k)}$, we may assume that $k \in U_{\{\pi'\}}$. Let k_0 be the image of k in $K_\pi \cong \mathbf{Q}_2$. Since $N_{K/\mathbf{Q}}(k) = 2^t$ for some integer t, the image of k in $K_{\pi'}$ is $2^t/k_0$. In the semi-local component of J_K over 2 we therefore have $(y, 1) = (2^a b, 2^c b)(k_0, 2^t/k_0)$ for some $a, c \in \mathbf{Z}$ and some $b \in U_2$. Since y and k_0 are units, $y = k_0^2$. Hence $Y = U^2_{\{\pi'\}}$ and $E_v/\bar{X} = U_2/\bar{U}^2_{\{\pi'\}}$ as desired.

Finally, we prove the splitting of our exact sequence. If G is a finite group, let $[G]$ denote its 2-rank. Since $U_2/\bar{U}^2_{\{\pi'\}}$ is cyclic, it suffices to show that $[I(E/K)] > [A_S(K)]$. Using Corollary 2.2 with v_0 being an archimedean prime of F and $q = 2$, it is easy to check that $\sqrt{2} \in L$. By Lemma 3.2, $[I(E/F)] = [LE\colon E]$. Let B be the maximal unramified elementary 2-extension of K which is split over 2. Then $[A_S(K)] = [B\colon K] = [BE\colon E]$. But LE properly contains BE because $\sqrt{2}$ introduces ramification. It follows that $[I(E/K)] > [A_S(K)]$.

5. Examples. We preserve the notation of Section 4. Our goal is to determine the 2-Sylow subgroup of $R_2 F$ for various real quadratic fields F. If G is a finite abelian group, let $[G]$ denote the rank of G/G^2 and let $\#[G]$ be the number of direct summands of G of order exactly 2. By the results of Section 4, Proposition 2.1 and Lemma 3.2,

$$(7) \qquad [R_2 F] = [I(E/F)] = \begin{cases} [A_S(K)]+1 & \text{if } D \equiv -1 \pmod 8, \\ [A_S(K)]-1 & \text{if } D \equiv 1 \pmod 8 \text{ and all possible signatures occur over } S_F^-, \\ [A_S(K)] & \text{otherwise.} \end{cases}$$

Let $\mathcal{U} = U_2/\bar{U}^2_{\{\pi'\}}$ be as defined in Proposition 4.4. We have the following formulas for the number of direct summands of order exactly 2.

$$(8) \qquad \#[R_2 F] = \begin{cases} \#[A_S(K)] + \#[\mathcal{U}] & \text{if } D \equiv -1 \pmod 8, \\ \#[A_S(K)]-1 & \text{if } D \equiv 1 \pmod 8 \text{ and all possible signatures occur over } S_F^-, \\ \#[A_S(K)] & \text{if } D \not\equiv \pm 1 \pmod 8. \end{cases}$$

Our first examples treat $D \not\equiv \pm 1 \pmod 8$. We begin by showing that the 2-Sylow subgroup of the wild kernel can be elementary abelian of arbitrary rank.

PROPOSITION 5.1. *Let p_0 be a prime, $p_0 \equiv 3 \pmod 8$. There exist primes $p_i \equiv 1 \pmod 8$ having the following Legendre symbols:*

$$(p_i/p_0) = -1 \quad \text{for } i = 1, \ldots, t \quad \text{and} \quad (p_j/p_i) = 1 \text{ for } 1 \leqslant i < j \leqslant t.$$

If $D = p_0 p_1 \ldots p_t$ with the primes p_i satisfying the above conditions, then the 2-

Sylow subgroups of $R_2 F$ and $K_2 O_F$ are elementary abelian of rank t and $t+2$ respectively. The Birch–Tate formula for the order of $K_2 O_F$ is valid.

Proof. By Dirichlet's theorem, one can choose the primes p_i successively, satisfying appropriate congruences modulo $8p_1 \cdot \ldots \cdot p_{i-1}$. The prime 2 is inert in K over $\mathbf{Q}$, and $[A(K)] = [A_S(K)] = t$ by genus theory. As representatives for a basis of ${}_2A(K)$ we may choose the prime ideals P_i over p_i in K for $i = 1, \ldots, t$. Since each P_i is inert in the unramified extension of K given by $K(\sqrt{p_i})$, the ideal class of P_i is not a square. Hence the 2-Sylow subgroup of $A_S(K)$ is elementary abelian of rank t. The same is true for $R_2 F$ by (7) and (8).

Clearly $-2 \in N_{F/\mathbf{Q}}(F^*)$ because -2 is a norm everywhere locally. By Lemma 5.2 below, $K_2 O_F[2]$ also is elementary abelian, of rank $t+2$. Thus the Birch–Tate formula is valid for F by [9].

LEMMA 5.2. *Suppose $D \not\equiv \pm 1 \pmod 8$. The following sequence is exact, where the components of the map λ are the real symbols. It splits if and only if -1 or -2 is a norm from F to $\mathbf{Q}$*

$$0 \to R_2 F[2] \to K_2 O_F[2] \xrightarrow{\lambda} \mu_2 \times \mu_2 \to 0.$$

Proof. Let v_0 be the prime over 2 in F. Exactness is clear, based on Moore's theorem, the fact that $m_{v_0}/2$ is odd, and the fact that λ_v^{tame} is an odd power of λ_v for non-archimedean v outside 2. The symbol $\{-1, -1\}$ certainly generates a direct summand of $K_2 O_F$ of order 2. Therefore, we can split the sequence if and only if there exists an element $s = \{-1, f\}$ in $K_2 O_F$ such that $Nf < 0$, where N is the norm from F to $\mathbf{Q}$. If there is such an element s, then $\mathrm{Tr}_{F/\mathbf{Q}}(s) = \{-1, Nf\}$. It follows from the computation of $K_2 \mathbf{Z}$ in [11] that Nf is an element of $-\mathbf{Q}^2$ or $-2\mathbf{Q}^2$ as desired. Conversely, if there is an element f such that Nf is -1 or -2, then it is easy to see that there is an ideal $\mathfrak{a}$ of F and a rational number r such that $(f) \equiv (r)\,\mathfrak{a}^2$ up to multiplication by the ideals over 2. Then $s = \{-1, f/r\}$ is the desired element of $K_2 O_F$.

Remark. The following exact sequences also are well known, but the conditions for splitting are somewhat more complicated:

$$0 \to R_2 F[2] \to K_2 O_F[2] \to \mu_2 \times \mu_2 \times \mu_2 \to 0 \quad \text{if } D \equiv 1 \pmod 8,$$
$$0 \to R_2 F[2] \to K_2 O_F[2] \to \mu_4 \times \mu_2 \to 0 \quad \text{if } D \equiv -1 \pmod 8.$$

In certain cases, Urbanowicz ([13], p. 80) has restated the conjectured formula of Birch and Tate for the order of $K_2 O_F[2]$ in terms of the factors of D, by ascertaining the power of 2 in $w_F \zeta_F(-1)$. The conjectures of Urbanowicz are settled by Kolster [9] when $K_2 O_F[2]$ is elementary abelian. We proceed to settle the rest of these conjectures.

EXAMPLE 5.3. Let $h_K = |A(K)|$. For the cases in Table 1 below, $w_F \zeta_F(-1) \equiv 2u h_K \pmod{16}$, where u is a 2-adic unit, by [13], Theorems 4 and 5. We shall verify the Birch–Tate formula that $|K_2 O_F[2]| = 8$ if 4 exactly divides h_K, and also obtain the weaker divisibility result that 16 divides $|K_2 O_F|$ if and only if $8 \mid h_K$.

Table 1

		B	$[A(K)]$
Case 1	$D = 2p,\ p \equiv 7(8)$	$K(\sqrt{-p})$	1
Case 2	$D = pq,\ p \equiv 3,\ q \equiv 7(8)$	$K(i, \sqrt{q})$	2
Case 3	$D = 2pq,\ p \equiv \pm 3(8)$	$K(\sqrt{p^*}, \sqrt{q^*})$	2
Notation: $p^* = \pm p \equiv 5(8),\ q^* = \pm q \equiv 1(4)$			

In each case, the ideal P over 2 in K is not principal, and satisfies $P^2 = (2)$. It follows that $|A(K)| = 2|A_S(K)|$. In Table 1, we list the 2-rank of $A(K)$, as determined by genus theory, and the class field B corresponding to $A(K)/A(K)^2$. The ideal class of P generates a direct summand of $A_S(K)$ if and only if P does not split completely in B. Using this condition, the reader can verify that 4 divides h_K and that $A_S(K)[2]$ is non-trivial cyclic in each case. By (7), $R_2 F[2]$ also is a non-trivial cyclic group. Moreover, 4 divides $|R_2 F|$ if and only if 4 divides $|A_S(K)|$ by (8).

By Lemma 5.2, we have the following possibilities, with $b \geqslant 1$, and $b = 1$ if and only if $8 \nmid h_K$.

$$K_2 O_F[2] \cong \begin{cases} \mathbf{Z}/(2^b) \times \mathbf{Z}/2 \times \mathbf{Z}/2 & \text{in case 3, provided either} \\ & p \equiv 5(8) \text{ and } q \equiv 1(4), \text{ or} \\ & p \equiv 3(8) \text{ and } q \equiv 1 \text{ or } 3(8), \\ \mathbf{Z}/(2^{b+1}) \times \mathbf{Z}/2 & \text{otherwise.} \end{cases}$$

We now turn our attention to $D \equiv -1 \pmod 8$. Write $D = p_1 \cdot \ldots \cdot p_t$. Let π and π' be the primes over 2 in K. Let h be the order of the ideal class of π' in $A(K)$, and choose a generator u for $(\pi')^h$. Then the group $U_{\{\pi'\}}$ of elements of K which are units outside π' is generated by -1 and u. In the embedding to $K_\pi \cong \mathbf{Q}_2$, let $\langle u^2 \rangle$ be the multiplicative subgroup generated topologically by u^2. Then $\mathscr{U} = U_2/\langle u^2 \rangle$. To apply (8) effectively, we need the following lemma.

LEMMA 5.4. *If some $p_i \equiv \pm 3 \pmod 8$, then $u \in \pm n K^2$ for some integer n dividing D. If each $p_i \equiv \pm 1 \pmod 8$, then $u^2 \equiv (-D)^h \pmod{\pi^4}$.*

Proof. By genus theory, the 2-rank of $A(K)$ is $t-1$ and a basis for ${}_2A(K)$ is given by the classes of the prime ideals P_i lying over p_i for

$i = 1, \ldots, t-1$. Suppose some $p_i \equiv \pm 3 \pmod 8$. Then the ideal class of π' is not a square in $A(K)$ because π' is inert in an unramified quadratic extension of K. Hence h is even and $(\pi')^{h/2} = \prod_{i=1}^{t-1} p_i^{e_i}(z)$ for some principal ideal (z). It follows that $u \in \pm nK^2$ for some integer n dividing D by squaring both sides and matching generators.

Next suppose that each $p_i \equiv \pm 1 \pmod 8$. It is easy to see that if $\mathfrak{B}$ is an ideal of K such that $\mathfrak{B}^2 = (\beta)$ is principal, then $\pm\beta$ is a square in each of the 2-adic completions of K. Since $-D$ is a norm from $\boldsymbol{Q}(\sqrt{2})$, we may in fact write $-D = a^2 - 8b^2$, where $a, b \in \boldsymbol{Z}$ and a is odd. Let $x = (a+\sqrt{-D})/2$ with the sign of a chosen so that $v_{\pi'}(x)$ is odd. Then $N_{K/\boldsymbol{Q}}(x) = 2b^2$. It follows that $\pi'(x)$ is the square of an ideal. Hence (ux^h) is the square of an ideal. Therefore $u \in \pm x^h K_\pi^{*2}$. By taking the 2-adic expansion for $\sqrt{-D}$ in terms of a and b the reader can check that $x\sqrt{-D} \in \pm K_\pi^{*2}$. It follows that $u^2 \equiv (-D)^h \pmod{\pi^4}$, as claimed.

Example 5.5. Suppose that $D \equiv -1 \pmod 8$. If D is a prime, then $R_2F \cong \boldsymbol{Z}/(2^b)$ with $b \geqslant 1$, and $b = 1$ if and only if $D \equiv 7 \pmod{16}$. Furthermore $K_2 O_F[2] \cong \boldsymbol{Z}/(2^{b+2}) \times \boldsymbol{Z}/2$. If $D = pq$ with $p \equiv \pm 3 \pmod 8$, then $R_2F[2] \cong \boldsymbol{Z}/2$ and $K_2 O_F[2] \cong \boldsymbol{Z}/8 \times \boldsymbol{Z}/2$.

Proof. To determine $R_2F[2]$, we apply (7), (8) and Lemma 5.4. In particular, for $D = pq$, the only possibility is that $u \in \pm pK^2$, since u is not a square in K. If D is a prime, then h is odd.

As for the tame kernel, let v_0 (resp., v_1, v_2) be the primes in F over 2 (resp., ∞). By Moore's theorem, there exists $s \in K_2 O_F$ such that $\lambda_{v_2}(s) = 1$, $\lambda_{v_1}(s) = -1$ and $\lambda_{v_0}(s) = i$. Replacing s by a suitable odd power, we may assume that s has 2-power order. By genus theory, $A_S(F)/A_S(F)^2$ is trivial. Hence $K_2 O_F[2]$ has rank 2 by exact sequence (1). Clearly then $K_2 O_F[2]$ is generated by $\{-1, -1\}$ and s. Since s has order 4 modulo R_2F, the claimed description of $K_2 O_F[2]$ follows.

Remark. If $D \equiv -1 \pmod 8$ has 2 prime factors neither of which is $\pm 3 \pmod 8$ or if D has 3 or more prime factors, then $[A_S(K)] \geqslant 2$ by genus theory. Hence $[R_2F] \geqslant 2$ by (7). But $|K_2 O_F| = |R_2F| \cdot |\mu_{v_0} \times \mu_{v_1}| = 8 \cdot |R_2F|$ by Moore's theorem, as used in Example 5.5. Hence $|K_2 O_F[2]| \geqslant 32$. Together with the above example, this verifies [13], Conjecture (i), p. 80. It follows from the congruences on $w_F \zeta_F(-1)$ in [13] that the Birch–Tate formula is valid if $|K_2 O_F[2]| = 16$ while the weaker divisibility result that $|K_2 O_F[2]|$ is divisible by 32 if and only if $w_F \zeta_F(-1)$ is divisible by 32 also holds.

Similarly, Example 5.3, together with [9] when $K_2 O_F[2]$ is elementary abelian, and a dimension count when D has more prime factors, can be used to verify [13], Conjectures (ii), (iii).

6. The case of prime $D = p \equiv 1 \pmod 8$. To complete the range of examples, we concentrate in this section on a case for which not all possible signatures occur over S_F^-. By genus theory, $F = \boldsymbol{Q}(\sqrt{p})$ has odd class number. Let π and π' be the places over 2 in F. We may choose an element α of F which has even ordinal outside π and odd ordinal at π. Since $p \equiv 1 \pmod 4$ the fundamental unit ε of F satisfies $N_{F/\boldsymbol{Q}}(\varepsilon) = -1$. Hence we may adjust α by $\pm\varepsilon$ so that α is totally positive. These conditions determine α up to multiplication by a square in F.

It is easy to see, using for example exact sequence (1), that ${}_2(K_2 O_F)$ has rank 3 and is generated by $\{-1, -1\}$, $\{-1, \varepsilon\}$ and $\{-1, \alpha\}$. Therefore, $R_2F[2]$ is cyclic, and in fact is trivial if and only if $\lambda_\pi\{-1, \alpha\} = -1$.

Certainly p is a norm from $\boldsymbol{Z}[\sqrt{2}]$. Making judicious use of $\boldsymbol{Z}[\sqrt{2}]$, we may write $p = u^2 - 32v^2$ with $u > 0$. Then one choice of α is $\alpha = (u+\sqrt{p})/2$. Clearly the 2-adic embeddings of $\sqrt{p}$ are $\pm u \pmod{16}$. Hence

$$\lambda_\pi\{-1, \alpha\} = \lambda_{\pi'}\{-1, \alpha\} = \begin{cases} +1, & u \equiv 1 \pmod 4, \\ -1, & u \equiv 3 \pmod 4. \end{cases}$$

If $u \equiv 3 \pmod 4$, we therefore have $K_2 O_F[2] \cong \boldsymbol{Z}/2 \times \boldsymbol{Z}/2 \times \boldsymbol{Z}/2$. Then by [9] the Birch–Tate formula is valid. As a further check, it is well known that $u \equiv 3 \pmod 4$ if and only if the order h_K of $A(K)$ is exactly divisible by 4. Furthermore, the congruence $w_F \zeta_F(-1) \equiv 2h_K \pmod{16}$ holds by [13]. This is the case in which all possible 2-adic signatures occur over S_F^-.

From now on we assume that h_K is divisible by 8. Equivalently, $u \equiv 1 \pmod 4$. Then all possible signatures do not occur over S_F^- and $R_2F[2]$ is cyclic, with element of order 2 given by $\{-1, \alpha\}$. We will determine below when $R_2F[2]$ has order exactly 2. However, the explicit results of [13] or [3] only yield the divisibility result that 16 divides $w_F \zeta_F(-1)$ in these cases.

By the vanishing of all Hilbert norm-residue symbols on $\{-1, \alpha\}$, we may write α as a norm from E, say $\alpha = Nz$. Let w be the prime of E over π'. Since $2i$ is a square in $\boldsymbol{Q}_2(i) \cong E_w$ and $\lambda_w^4 = 1$, commutative diagram (3) yields

$$\begin{aligned} \lambda_{\pi'} \operatorname{Tr}\{i, z\} &= \lambda_w\{i, z\}^2 = \lambda_w\{2, z\}^2 = \lambda_{\pi'}\{2, N_{E/F}z\} \\ &= \lambda_{\pi'}\{2, \alpha\} = \lambda_{\pi'}\{2, u\} = (-1)^{(u-1)/4}. \end{aligned}$$

Using reciprocity to obtain $\lambda_\pi \operatorname{Tr}\{i, z\}$, and the fact that $p \equiv u^2 \pmod{32}$, we have

$$(9) \qquad \lambda_v \operatorname{Tr}\{i, z\} = (-1)^{(p-1)/8} \quad \text{if } v \mid 2.$$

Select a prime $q \equiv 3 \pmod 4$ such that $(p/q) = -1$. Let $\mathfrak{B}$ be a prime over q in K. By genus theory, $A(K)[2]$ is cyclic. Since $\mathfrak{B}$ is inert in the unramified extension $K(i)$ over K, a suitable odd power of the ideal class of $\mathfrak{B}$ generates $A(K)[2]$. In fact, by Chebotarev density, we may choose q so that the class of $\mathfrak{B}$ itself generates $A(K)[2]$. Since F has odd class number, $[J_F : U_F F]$ is odd. It follows from the same arguments as in Lemma 4.1, that the sequence below is exact:

$$0 \to A(E)[2] \overset{N_{E/K}}{\to} A(K)[2] \to \mathrm{Gal}(E/K) \to 0.$$

Therefore $A(E)[2]$ is generated by the class of $\mathfrak{B}\cdot O_E$ and is cyclic of order $h/2$, where h is the 2-primary part of h_K.

Let P be the ideal over π in E. Then P cannot be principal since $N_{E/K} P$ is not principal in K. Furthermore $P^2 = \pi O_E$, so a suitable odd power, say P^a, represents an ideal class of order exactly 2 in $A(E)$. Therefore $\mathfrak{B}^{h/4} P^a = (Z)$ is principal for some Z in E^*. Since $N_{E/F}(Z)$ is totally positive and has odd ordinal only at π, it follows that $N_{E/F}(Z)$ differs multiplicatively from α by a square. By (9), $\lambda_v \mathrm{Tr}\{i, Z\} = (-1)^{(p-1)/8}$ if $v \mid 2$. Since $N_{E/F}\mathfrak{B} = (q) O_F$ we have

$$\lambda_v \mathrm{Tr}\{i, Z\} = \begin{cases} (-1)^{h/8}, & v = q, \\ 1, & v \nmid 2q \end{cases}$$

by Lemma 3.3. Let $s = \{-1, q\}^{h/8}\mathrm{Tr}\{i, Z\}$. Then $s^2 = \{-1, \alpha\}$ and

$$\lambda_v(s) = \begin{cases} (-1)^{(p-1)/8}(-1)^{h/8}, & v \mid 2, \\ 1, & v \nmid 2. \end{cases}$$

By Moore's theorem, there is an element $g \in K_2 O_F$, which we may take to have 2-power order, such that $\lambda_v(g) = 1$ if $v \nmid 2$, and $\lambda_v(g) = -1$ if $v \mid 2$. Then $K_2 O_F[2]$ is generated by g, $\{-1, \varepsilon\}$ and $\{-1, -1\}$. If either $p \equiv 1 \pmod{16}$ and $16 \nmid h$ or else $p \equiv 9 \pmod{16}$ and $16 \mid h$, we may take $g = s$. Then $K_2 O_F[2] \cong \mathbf{Z}/4 \times \mathbf{Z}/2 \times \mathbf{Z}/2$. Otherwise s is an even power of g and 32 divides $|K_2 O_F|$. Therefore the Birch–Tate conjecture leads to the following

Conjecture (implied by Birch–Tate). *Let $F = \mathbf{Q}(\sqrt{p})$ for $p \equiv 1 \pmod 8$. Suppose that the class number h_K of $K = \mathbf{Q}(\sqrt{-p})$ is divisible by 8. It is known that $16 \mid w_F \zeta_F(-1)$. Then 32 divides $w_F \zeta_F(-1)$ if and only if either $p \equiv 1 \pmod{16}$ and $16 \mid h_K$ or else $p \equiv 9 \pmod{16}$ and $16 \nmid h_K$.*

Mr. Ze Li Dou has verified this conjecture by numerical computation if $p < 1000$.

Added in proof. Since the submission of this article, J. Browkin has proven the above conjecture.

References

[1] A. Bak and U. Rehman, *K_2 analogs of Hasse's norm theorems*, Comment. Math. Helvetici 59 (1984), 1–11.

[2] J. Browkin and A. Schinzel, *On Sylow 2-subgroups of $K_2 O_F$ for quadratic number fields F*, J. für Mathematik, Band 331, 104–113.

[3] K. S. Brown, *Euler characteristics of discrete group and G-spaces*, Invent. Math. 27 (1974), 229–264.

[4] J. Coates, *On K_2 and some classical conjectures in algebraic number theory*, Ann. Math. 95 (1972), 99–116.

[5] L.J. Federer, *The non-vanishing of Gross' p-adic regulator Galois cohomologically*, Société Mathématique de France, Astérisque, 147–148 (1987), 71–77.

[6] A. Fröhlich, *Central extenstons, Galois groups, and ideal class groups of number fields*, Contemporary Mathematics 24, American Math. Soc., Providence, 1983.

[7] G. Gras, *Remarks on K_2 of number fields*, J. Number Theory 23 (1986), 322–335.

[8] R. Greenberg, *On p-adic L-functions and cyclotomic fields, I, II*, Nagoya Math. J. 56 (1974), 61–74; 67 (1977), 139–158.

[9] M. Kolster, *The structure of the 2-Sylow subgroup of $K_2 O$, I*, Comment. Math. Helvetici 61 (1986), 376–388.

[10] B. Mazur and A. Wiles, *Class fields of abelian extensions of Q*, Invent. Math. 76 (1984), 179–330.

[11] J. Milnor, *Introduction to algebraic K-theory*, Annals of Math. Study 72, Princeton University Press, Princeton 1971.

[12] J.T. Tate, *On relations between K_2 and Galois cohomology*, Invent. Math. 36 (1976), 257–274.

[13] J. Urbanowicz, *On the 2-primary part of a conjecture of Birch and Tate*, Acta Arith. 43 (1983), 69–81.

DEPARTMENT OF MATHEMATICS
DREW UNIVERSITY MADISON
New Jersey, 07940

DEPARTMENT OF MATHEMATICS
QUEENS COLLEGE (CUNY) FLUSHING
New York 11367

Received on 21.1.1987
and in revised form on 31.7.1987 (1700)