CLASSES OF ORDER 4 IN THE STRICT CLASS GROUP OF NUMBER FIELDS AND REMARKS ON UNRAMIFIED QUADRATIC EXTENSIONS OF UNIT TYPE

DAVID S. DUMMIT

Abstract. Let $K$ be a number field of degree $n$ over $\mathbb{Q}$. Then the 4-rank of the strict class group of $K$ is at least $\text{rank}_2 \left( E_K^+ / E_K^2 \right) - \lfloor n/2 \rfloor$ where $E_K$ and $E_K^+$ denote the units and the totally positive units of $K$, respectively, and $\text{rank}_2$ is the dimension as an elementary abelian 2-group. In particular, the strict class group of a totally real field $K$ with a totally positive system of fundamental units contains at least $(n-1)/2$ (n odd) or $n/2 - 1$ (n even) independent elements of order 4. We also investigate when units in $K$ are sums of two squares in $K$ or are squares mod 4 in $K$.

Résumé. Soit $K$ est un corps de nombres de degré $n$ sur $\mathbb{Q}$. Alors le 4-rang du groupe de classes au sens strict de $K$ est au moins $\text{rang}_2 \left( E_K^+ / E_K^2 \right) - \lfloor n/2 \rfloor$ où $E_K$ et $E_K^+$ désignent respectivement le groupe des unités et le groupe des unités totalement positives de $K$, et où $\text{rang}_2$ se veut la dimension en tant que 2-groupe abélien élémentaire. En particulier, le groupe de classes au sens strict d’un corps $K$ totalement réel avec un système fondamental d’unités totalement positives contient au moins $(n - 1)/2$ pour $n$ impair (respectivement $n/2 - 1$ pour $n$ pair) éléments indépendants d’ordre 4. Nous nous demandons aussi quand les unités de $K$ sont des sommes de deux carrés de $K$ ou sont des carrés mod 4 de $K$.

1. Introduction

In 1967 Armitage and Fröhlich proved a result involving the 2-ranks of the usual class group and the strict (or “narrow”) class group of a number field $K$. They showed in particular that if there are many totally positive units in $K$ then there are independent elements of order 2 in the class group of $K$. A result of Hayes in 1997 shows that much of this contribution to the class group of $K$ is provided by unramified extensions $K(\sqrt{\varepsilon})$ where $\varepsilon$ is a totally positive unit in $K$ (the “unramified quadratic extensions of unit type”).

In the first part of this paper, we show that the Armitage-Fröhlich theorem implies that if there are many totally positive units in $K$ then there are independent elements of order 4 in the strict class group of $K$.

In the second part of this paper, we make some remarks related to the unramified quadratic extensions of unit type considered by Hayes. In particular, the question of whether they can be embedded in cyclic quartic extensions (which might provide the classes of order 4 in the strict class group) leads to consideration of canonical subgroups of the group of units of a number field.

---

Date: November 15, 2018.
2010 Mathematics Subject Classification. 11R29 (primary), and 11R37, 11R27, 11E25 (secondary).
2. Classes of order 4 in the strict class group

Let $K$ be an algebraic number field of degree $n$ over $\mathbb{Q}$ having $r_1$ real and $r_2$ complex places. If $C_K$ denotes the class group of $K$ and $C^+_K$ denotes the strict class group of $K$, then there is an exact sequence

$$0 \rightarrow P_K/P^+_K \rightarrow C^+_K \rightarrow C_K \rightarrow 0 \quad (1)$$

where $P_K$ denotes the group of principal ideals, and $P^+_K$ the group of totally positive principal ideals. The natural map $\alpha \mapsto (\alpha)$ gives an exact sequence

$$1 \rightarrow E_K \rightarrow K^* \rightarrow P_K \rightarrow 1, \quad (2)$$

where $E_K$ denotes the group of units of $K$. The image in $P_K$ of the subgroup $K^{**}$ of totally positive elements of $K^*$ is $P^+_K$, which gives the isomorphism

$$P_K/P^+_K \simeq K^*/E_KK^{**}, \quad (3)$$

so (1) may be written

$$0 \rightarrow K^*/E_KK^{**} \rightarrow C^+_K \rightarrow C_K \rightarrow 0. \quad (4)$$

The group $K^*/E_KK^{**}$ is an elementary abelian 2-group, and the sequence (4) splits if and only if the corresponding sequence with $C_K$ and $C^+_K$ replaced by their 2-primary parts splits.

Let $\mathbb{F}_2$ denote the field of order 2 and for a finite abelian group $A$, let $\text{rank}_2(A)$ denote the dimension over $\mathbb{F}_2$ of $A/2A$ (equivalently, the dimension over $\mathbb{F}_2$ of $A[2] = \{a \in A \mid 2a = 0\}$). By the 4-rank of a finite abelian group $A$ we mean the number of invariant factors of $A$ divisible by 4, or, equivalently, $\text{rank}_2(2A)$.

Define

$$\rho = \text{rank}_2 C_K$$

$$\rho^+ = \text{rank}_2 C^+_K$$

$$\rho_\infty = \text{rank}_2 (P_K/P^+_K)$$

The homomorphism from $K^*$ to $P_K$ in (2) mapping $E_KK^{**}$ to $P^+_K$, together with several natural inclusions, gives the diagram

$$\begin{array}{ccc}
K^* & \longrightarrow & P_K \\
| & & | \\
E_K & \longrightarrow & E_KK^{**} \longrightarrow P^+_K \\
| & & | \\
E^+_K & \longrightarrow & K^{**} \\
| & & | \\
E^2_K &
\end{array}$$

from which various rank relations can be determined, as follows. The signature map taking an element of $K^*$ to its sign in each of the $r_1$ real embeddings of $K$ is a surjective map from $K^*$ to $\{\pm 1\}^{r_1}$ with kernel $K^{**}$, so $K^*/K^{**}$ is an elementary abelian 2-group with $\text{rank}_2 (K^*/K^{**}) = r_1$. We have $\text{rank}_2 (K^*/E_KK^{**}) = \text{rank}_2 (P_K/P^+_K) = \rho_\infty$ by the isomorphism (3), and $E_K \cap K^{**} = E^+_K$ shows $E_KK^{**}/K^{**} \simeq E_K/(E_K \cap K^{**}) = E_K/E^+_K$, so that $\text{rank}_2 (E_KK^{**}/K^{**}) = \text{rank}_2 (E_K/E^+_K)$. Since the group $E_K/E^2_K$ is an elementary abelian
2-group with \( \operatorname{rank}_2 (E_K/E_K^2) = r_1 + r_2 \) by the Dirichlet unit theorem, we deduce the following rank relations:

\[
\begin{align*}
\operatorname{rank}_2 (K^*/E_K K^{++}) &= \operatorname{rank}_2 (P_K/P_K^+) = \rho_\infty \\
\operatorname{rank}_2 (E_K K^{++}/K^{++}) &= \operatorname{rank}_2 (E_K/E_K^+) = r_1 - \rho_\infty \\
\operatorname{rank}_2 (E_K^+/E_K^2) &= r_2 + \rho_\infty.
\end{align*}
\]

We now examine more carefully group extensions of abelian 2-groups as in the (2-primary parts of the) sequences (1) and (4).

**Proposition 1.** Suppose \( B \) is a finite abelian 2-group and \( A \leq B \) is a subgroup with quotient \( C \), so the sequence \( 0 \to A \to B \to C \to 0 \) is exact, where the first map is the inclusion of \( A \) into \( B \). Then

(a) the 4-rank of \( B \) is at least \( \operatorname{rank}_2 A + \operatorname{rank}_2 C - \operatorname{rank}_2 B \).

(b) if \( A \) is an elementary abelian 2-group, then the maximal rank of a subgroup of \( A \) that is a direct summand of \( B \) is \( \operatorname{rank}_2 B - \operatorname{rank}_2 C \) and the sequence \( 0 \to A \to B \to C \to 0 \) splits if and only if \( \operatorname{rank}_2 B = \operatorname{rank}_2 A + \operatorname{rank}_2 C \).

**Proof.** Let \( A_1 = \{ a \in A \mid a = 2b \text{ for some } b \in B \} \).

It is easy to see (e.g., by the snake lemma or directly) that the sequence of elementary abelian 2-groups

\[
0 \to A/A_1 \to B/2B \to C/2C \to 0
\]

is exact. In particular, the sequence splits and \( \operatorname{rank}_2 B = \operatorname{rank}_2 (A/A_1) + \operatorname{rank}_2 C \). Then \( \operatorname{rank}_2 A_1 + \operatorname{rank}_2 (A/A_1) \geq \operatorname{rank}_2 A \) gives \( \operatorname{rank}_2 B \geq (\operatorname{rank}_2 A - \operatorname{rank}_2 A_1) + \operatorname{rank}_2 C \), i.e., \( \operatorname{rank}_2 A_1 \geq (\operatorname{rank}_2 A + \operatorname{rank}_2 C) - \operatorname{rank}_2 B \). Since the 4-rank of \( B \) is at least \( \operatorname{rank}_2 A_1 \), this proves (a).

For (b), note first that since \( B/2B \) is the Frattini quotient for \( B \), any collection of elements of \( B \) projecting to a basis for the elementary abelian 2-group \( B/2B \) will give a minimal set of generators for \( B \). It follows that a subgroup \( A' \) of \( A \) is a direct summand of \( B \) if and only if \( A' \cap A_1 = 0 \), as follows. If \( B = A' \oplus B' \) for some subgroup \( B' \), then \( 2B = 2B' \), so \( A' \cap A_1 = A' \cap 2B \leq A' \cap B' = 0 \). Conversely, suppose \( A' \cap A_1 = 0 \). Then \( A' \) injects into the elementary abelian 2-group \( B/2B \) in the exact sequence (5), hence has a complement. Let \( S \) be a collection of elements of \( B \) projecting to a basis for a complement to \( A' \), and let \( B' \) be the subgroup of \( B \) generated by the elements of \( S \). As noted previously, a basis for \( A' \) together with the elements of \( S \) give a minimal set of generators for \( B \), so \( B = A' + B' \).

Any element in the intersection of \( A' \) and \( B' \) projects to 0 in \( B/2B \) since \( B' \) projects to a complement for \( A' \) in \( B/2B \), hence would be an element of \( A_1 \). Since \( A' \cap A_1 = 0 \) by assumption, this shows the sum is direct: \( B = A' \oplus B' \).

It follows that the maximal rank of a subgroup of \( A \) that is a direct summand of \( B \) occurs for a maximal subgroup of \( A \) intersecting trivially with \( A_1 \), i.e., for any complement to \( A_1 \) in \( A \). The rank of such a complement is \( \operatorname{rank}_2 (A/A_1) \), which is precisely \( \operatorname{rank}_2 B - \operatorname{rank}_2 C \) by the exact sequence (5).

Finally, the sequence splits if and only if the maximal subgroup of \( A \) that is a direct summand of \( B \) is \( A \), which by the previous result happens if and only if \( \operatorname{rank}_2 B - \operatorname{rank}_2 C \) equals \( \operatorname{rank}_2 A \). \(\square\)
Remark 1. It is important that $A$ is an elementary abelian 2-group in (b) of the proposition: if $B = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $A$ denotes the (non-elementary) cyclic subgroup of order 4 generated by $(2, 1) \in B$, then the quotient $C = B/A$ is cyclic of order 4 and both statements of (b) are false.

Applying Proposition 1 to the groups in (1) and (4) immediately gives

**Proposition 2.** The sequence $0 \to K^*/E_K^+K^* \to C^+_K \to C_K \to 0$ in (4) splits if and only if $\rho^+ = \rho_\infty + \rho$. The 4-rank of $C^+_K$ is at least $(\rho_\infty + \rho) - \rho^+$.

In [A-F], Armitage and Fröhlich prove that $\rho^+ - \rho \leq [r_1/2]$. While they explicitly state only a weaker version of this result (namely that $\rho_\infty - \rho \leq [r_1/2]$), they prove the stronger version (see equations (3) and (4) of their paper—note $\rho^+ = \dim_2(X_2)$ and $\rho = \dim_2(Ker \rho \cap X_2)$ in their terminology). Another proof of the Armitage-Fröhlich theorem can be found in Oriat [O] (to whom the stronger version is occasionally incorrectly credited), a particularly nice proof due to Hayes (unpublished) can be found in [D-V], and a nice proof that highlights the conceptual basis for the result can be found in Greither-Hayes [G-H] (also outlined in [D-V]).

Using this result we obtain the following theorem.

**Theorem 1.** Suppose $K$ is a number field with $\text{rank}_2(E^+_K/E^2_K) > [n/2]$ (equivalently, $\rho_\infty > [r_1/2]$). Then

(a) the sequence $0 \to K^*/E_K^+K^* \to C^+_K \to C_K \to 0$ does not split, and
(b) the 4-rank of the strict class group is at least $\text{rank}_2(E^+_K/E^2_K) - [n/2]$.

In particular, if $K$ is a totally real number field of degree $n$ with a totally positive system of fundamental units, then the strict class group of $K$ contains at least $(n - 1)/2$ (n odd) or $n/2 - 1$ (n even) independent elements of order 4.

**Proof.** By the Armitage-Fröhlich theorem, $\rho^+ - \rho \leq [r_1/2]$, so $(\rho_\infty + \rho) - \rho^+ \geq \rho_\infty - [r_1/2]$ and (a) and (b) follow from Proposition 2 since $\rho_\infty - [r_1/2] = \text{rank}_2(E^+_K/E^2_K) - [n/2]$. If $K$ is totally real with a totally positive system of fundamental units then $\text{rank}_2(E^+_K/E^2_K) = n - 1$, which gives the final statement in the Theorem. \(\square\)

**Remark 2.** When $K$ is a real quadratic field, the splitting behavior of (1) is well-known (cf. [Ha]) and follows from the result that $\text{rank}_2(C^+_K) = 1 + \text{rank}_2(C_K)$ if and only if there is no element $\omega \in K$ with $\text{Norm}_{K/Q}(\omega) = -1$: the sequence (1) splits if and only if either (a) there is a unit $\varepsilon$ with $\text{Norm}_{K/Q}(\varepsilon) = -1$, in which case $P_K/\ell^+ = 1$, or (b) there is no element $\omega \in K^*$ with $\text{Norm}_{K/Q}(\omega) = -1$, in which case $P_K/\ell^+ = \mathbb{Z}/2\mathbb{Z}$ and $C^+_K \cong C_K \oplus \mathbb{Z}/2\mathbb{Z}$; in the remaining case (where there is an element $\omega \in K^*$ with $\text{Norm}_{K/Q}(\omega) = -1$ but no unit with the property), then $|C^+_K| = 2|C_K|$ but the groups have the same 2-rank.

We briefly recall the proof of the rank result from [Ha]. Let $I_K$ denote the group of nonzero fractional ideals of $K$, let $G$ be the subgroup of ideals $\mathfrak{a}$ whose norm agrees, up to sign, with the norm of some element $\alpha$ of $K^*$: $\text{Norm}_{K/Q}(\mathfrak{a}) = \pm\text{Norm}_{K/Q}(\alpha)$, and let $G^+$ be the subgroup of those $\mathfrak{a}$ whose norm agrees with the (necessarily positive) norm of some element $\alpha$ of $K$: $\text{Norm}_{K/Q}(\mathfrak{a}) = \text{Norm}_{K/Q}(\alpha)$. If $\tau$ is the nontrivial automorphism of $K$, then $I_K^{1-\tau} \subseteq G^+$ since $\text{Norm}_{K/Q}(\mathfrak{a}/(\mathfrak{a}^{\tau})) = 1$. Also, if $\mathfrak{a} \in G^+$, then $\text{Norm}_{K/Q}(\mathfrak{a}/(\mathfrak{a}^{\tau})) = \text{Norm}_{K/Q}(\alpha)$ for some $\alpha \in K^*$, and since $\text{Norm}_{K/Q}(\alpha) > 0$, the principal ideal $(\alpha)$ lies in $\ell^+$. Then $\text{Norm}_{K/Q}(\mathfrak{a}/(\alpha)) = 1$, so the prime ideal decomposition of $\mathfrak{a}/(\alpha)$ is a product of ideals of the
form $p/p^+$ where $p$ is a split prime in $K$. Hence $\mathfrak{A} \in I_K^{1-\tau} P_K^+$, so $G^+ = I_K^{1-\tau} P_K^+$ and it follows that $G^+/P_K^+ = (G/K)_2^+$ since $\tau$ acts by inversion on $G/K_2$. The same argument shows $G/P_K = C_K^2$ (the “Principal Genus Theorem”). It follows that $I_K/G = (I_K/P_K)/(G/P_K) = C_K/C_K^2$ and similarly $I_K/G^+ = C_K^+/(C_K^+)^2$, so $[I_K : G] = 2^{\text{rank}_2(C_K)}$ and $[I_K : G^+] = 2^{\text{rank}_2(C_K^+)}$. Since $[G : G^+] = 1$ or 2, with $[G : G^+] = 1$ if and only if there is an element $\omega \in K$ with $\text{Norm}_{K/Q}(\omega) = -1$, the rank result follows.

Remark 3. It is perhaps worth noting that the hypotheses of Proposition 1 and Theorem 1 most likely do not hold for cyclotomic fields, since the signature rank of the units in such extensions is expected to be nearly maximal. This is known to be true, for example, for the cyclotomic fields of prime power conductor $p^n$ for $n$ sufficiently large ([D-D-K]).

3. Subfields of the Hilbert class field: Unramified extensions of unit type.

As previously noted, in [A-F] Armitage and Fröhlich explicitly give the inequality $\rho \geq \rho_{\infty} - [\tau_1/2]$. Theorem 1 shows there are $\rho_{\infty} - [\tau_1/2] = \text{rank}_2(E_K^+/E_K) - [\nu/2]$ elements of order 4 in the strict class group, and these survive passing to the quotient $C_K$, which ‘explains’ the Armitage-Fröhlich result. In response to a question/conjecture of the author (based on computations in the case of totally real cubic fields), Hayes ([H]) and then Greither and Hayes ([G-H]) proved that a subgroup of 2-rank at least $\rho_{\infty} - [\tau_1/2]$, precisely the contribution to the class group guaranteed by the explicit theorem of Armitage and Fröhlich, is accounted for by totally unramified quadratic extensions $K(\sqrt{\varepsilon})$ for units $\varepsilon \in E_K$ (cf. also [D-V] for a proof of this result).

The result in Theorem 1, showing that a large number of totally positive units modulo squares implies the existence of a number of cyclic quartic extensions of $K$ that are unramified at all finite primes, then raises the analogous question of whether one can similarly explicitly describe a number of cyclic quartic extensions from these units.

With an eye to addressing this question, we make some remarks about the “unramified extensions of unit type” given by $K(\sqrt{\varepsilon})$ for units $\varepsilon \in E_K$.

Let $O_K$ denote the ring of integers of $K$, let $O_{K,(2)}$ denote its localization at 2, and for every place $v$ of $K$, let $O_v$ denote the ring of integers in the completion $K_v$ of $K$ at $v$.

Lemma 1. Suppose $\varepsilon$ is a unit in $K$. Then the following are equivalent:

(a) There are integers $\alpha, \beta$ in $O_K$ with $\varepsilon = \alpha^2 + 4\beta$.

(b) There are 2-integral elements $\alpha_2, \beta_2$ in $O_{K,(2)}$ with $\varepsilon = \alpha_2^2 + 4\beta_2$. Equivalently, $\varepsilon = \alpha_2^2(1 + 4\beta_2)$ for some 2-integral elements $\alpha_2, \beta_2 \in O_{K,(2)}$.

(c) For every place $v$ dividing 2, there are elements $\alpha_v, \beta_v$ in $O_v$ with $\varepsilon = \alpha_v^2 + 4\beta_v$. Equivalently, $\varepsilon = \alpha_v^2(1 + 4\beta_v)$ for some $\alpha_v, \beta_v$ in $O_v$.

Proof. The two statements in (c) are equivalent since $\varepsilon = \alpha_v^2 + 4\beta_v$ implies $\alpha_v$ is locally a unit, so $\varepsilon = \alpha_v^2(1 + 4\beta_v)$. Similarly, the two statements in (b) are equivalent. Clearly (a) implies (b) implies (c), so it remains to show (c) implies (a). Suppose for every $v$ dividing 2 there are elements $\alpha_v, \beta_v$ in $O_v$ so that $\varepsilon = \alpha_v^2 + 4\beta_v$. Choose an integer $\alpha \in O_K$ so that for every $v$ dividing 2, $\alpha \equiv \alpha_v \mod 4$ locally at $v$. The element $\beta = (\varepsilon - \alpha^2)/4$ in $K$ is clearly integral at every place of $K$ not dividing 2. Since $\beta \in \beta_v + O_v = O_v$ for places $v$ dividing 2, $\beta$ is also integral at 2, hence $\beta \in O_K$, so $\varepsilon = \alpha^2 + 4\beta$ with $\alpha, \beta \in O_K$. □
Definition. Let $E_{K,A}$ denote the units in $E_K$ satisfying any of the equivalent conditions in Lemma 1, referred to as ‘the units of $K$ that are squares mod 4’.

The units $\varepsilon$ of $E_{K,A}$ are precisely the units of $K$ such that the extension $K(\sqrt{\varepsilon})$ is unramified over $K$ at all finite primes (see, for example, [D-V, Proposition 4.8]).

Remark 4. The results in Lemma 1 show the questions of whether a unit $\varepsilon$ is ‘a square mod 4’ in an additive sense (i.e., $\varepsilon = \alpha^2 + 4\beta^2$) globally, globally at 2, and locally at primes over 2, are all equivalent. By (b) and (c) of the lemma, the questions of whether a unit $\varepsilon$ is ‘a square mod 4’ in a multiplicative sense (i.e., $\varepsilon = \alpha^2(1 + 4\beta^2)$) globally at 2 and locally at primes over 2 are also equivalent (and equivalent to the additive version). The first example following Theorem 3 below (see Remark 6) shows that for $\varepsilon \in E_{K,A}$, it may not be possible to express $\varepsilon$ globally in the form $\alpha^2(1 + 4\beta^2)$ where $\alpha$ and $\beta$ are in $\mathcal{O}_K$, so the conditions in the lemma are not equivalent to this global multiplicative version. As a result, some mild care should be exercised with the phrase ‘$\varepsilon$ is a square mod 4’.

As motivation for the next definition, recall that a quadratic extension $K(\sqrt{\alpha})$ can be embedded in a cyclic quartic extension of $K$ if and only if $\alpha$ is a sum of two squares in $K$ (cf. for example Exercise 19, Section 14.6 in [D-F]).

Definition. Let $E_{K,\Box}^\square$ denote the units in $E_K$ that are the sum of two squares (in $K$): $\varepsilon = \alpha^2 + \beta^2$, $\alpha, \beta \in K$.

Each of $E_{K,A}$ and $E_{K,\Box}^\square$ is a canonical subgroup of $E_K$ containing the squares $E_K^2$.

The first part of the following theorem is the result of Hayes mentioned previously.

Theorem 2. With notation as above, we have:

(a) (Hayes, Greither-Hayes) rank$_2(E_{K,A} \cap E_K^+) \geq \rho_{\infty} - [n/2]$. Equivalently, there are at least rank$_2(E_{K,A}^+ / E_K^+) - [n/2]$ independent unramified quadratic extensions $K(\sqrt{\varepsilon})$ of unit type.

(b) The unit $\varepsilon \in E_K^+$ is a sum of two rational squares in $K$, i.e., $\varepsilon \in E_K^{2+}$, if and only if the quadratic Hilbert symbol $(\varepsilon, -1)_v$ is 1 at all primes $v$ dividing 2 in $K$ (equivalently, $(\varepsilon, \varepsilon)_v = 1$, i.e., $\varepsilon$ is ‘isotropic’, at all such $v$). In particular, every unit in $E_{K,A} \cap E_K^+$ is a sum of two squares:

$$E_K^2 \subseteq E_{K,A} \cap E_K^+ \subseteq E_K^{2+} \subseteq E_K^+ \subseteq E_K.$$  

(c) If $g$ denotes the number of primes dividing 2 in $K$, then rank$_2(E_K^{2+} / E_K^{2+}) \leq g - 1$.

In particular, for a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ with squarefree integral $d > 0$ in which 2 is either ramified or inert, a unit is totally positive if and only if it is a sum of two squares in $K$.

Proof. For (a) see [D-V].

For (b): the unit $\varepsilon$ is a sum of two squares, $\varepsilon = x^2 + y^2$, if and only if $\varepsilon$ is a norm from the extension $K(i)$ (note that if $i \in K$ then every element $\alpha$, in particular $\varepsilon$, in $K$ is a sum of two squares: take $x = (\alpha + i)/2$ and $y = i(\alpha - 1)/2$). Hence $\varepsilon$ is a sum of two squares if and only if the global quadratic Hilbert symbol $(\varepsilon, -1)$ is 1, which is the case if and only if each local symbol is 1. The symbol $(\varepsilon, -1)_v = 1$ at all infinite places $v$ since $\varepsilon \in E_K^+$ is totally positive, and $(\varepsilon, -1)_v = 1$ at all odd places $v$ since $K(\sqrt{\varepsilon})$ is then unramified at $v$ and all units are locally norms. This proves the first statement in (b) (noting that since $(\varepsilon, -\varepsilon)$ is
always \(1, (\varepsilon, -1)_v = 1\) is equivalent to \((\varepsilon, \varepsilon)_v = 1\). For \(\varepsilon \in E_{K,4} \cap E_K^+\), the extension \(K(\sqrt{\varepsilon})\) is also unramified at primes dividing 2, so just as for odd primes, \((\varepsilon, -1)_v = 1\) at all the even places \(v\), so every unit in \(E_{K,4} \cap E_K^+\) is the sum of two squares (in \(K\)).

For (c): if \(g\) is the number of primes dividing 2, the map
\[
E_K^+ \to \prod_{v \mid 2} (\pm 1) \simeq (\pm 1)^g
\]
\[
\varepsilon \mapsto (\ldots, (\varepsilon, -1)_v, \ldots)
\]
defined by the quadratic Hilbert norm residue symbols, is a homomorphism with kernel \(E_{K,4}^+\) by (b). The image lies in the subgroup of codimension 1 consisting of elements whose product is +1 since \(\prod_{v \mid 2} (\varepsilon, -1)_v = 1\) by the product formula, so rank\((E_K^+/E_{K,4}^+)\) \(\leq g - 1\).

The ranks of the index relations for these subgroups of the group of units are summarized in the following diagram.

**Example: Real quadratic fields.** Suppose \(K = \mathbb{Q}(\sqrt{d})\) with squarefree integral \(d > 0\). Then rank\((E_K^+/E_K^2)\) = 2 and rank\((E_K^+/E_{K,4}^+)\) \(\geq 1\). If a fundamental unit \(\varepsilon_K\) has negative norm (the situation when all possible signatures of units occur), then \(E_K^+ = E_K^2\), so \(E_{K,4}^+ = E_K^+\) and rank\((E_K^+/E_{K,4}^+)\) = 2, so (b) of Proposition 3 becomes
\[
E_K^2 = E_{K,4} \cap E_K^+ = E_K^\square = E_K^+ \subseteq E_K^4 \subseteq E_K.
\]
where the underscript 4 indicates the index of the subgroup.

Assume for the remainder of the example that the fundamental unit \(\varepsilon_K\) is totally positive and has been normalized so that \(\varepsilon_K > 1\) with respect to the embedding for which \(\sqrt{d} > 0\). Then \(\text{Norm}_{K/\mathbb{Q}}(\varepsilon_K) = +1\) and \(E_K^+\) has index 2 in \(E_K^4\):
\[
E_K^2 \subseteq E_{K,4} \cap E_K^+ \subseteq E_K^\square \subseteq E_K^+ \subseteq E_K^4 \subseteq E_K.
\]
(6)

By Hilbert’s Theorem 90, \(\text{Norm}_{K/\mathbb{Q}}(\varepsilon_K) = +1\) implies
\[
\varepsilon_K = \frac{\sigma(\alpha)}{\alpha}
\]
(7)
for some \(\alpha \in \mathbb{Q}(\sqrt{d})\), which may be assumed to be an algebraic integer (for example, take \(\alpha = \sigma(\varepsilon_K) + 1\)). Since \(\sigma(\alpha) = (\alpha)\), the principal ideal \((\alpha)\) is invariant under \(\sigma\) (i.e., is an ambiguous ideal), so the element \(\alpha\) in (7) can be further chosen so that the ideal \((\alpha)\) is the product of distinct ramified primes without altering (7). For such a choice of \(\alpha\), let \(m\) denote the norm of \(\alpha\):
\[
m = \alpha \sigma(\alpha).
\]
(8)
Then \(m\) is a squarefree integer dividing the discriminant of \(K = \mathbb{Q}(\sqrt{d})\).
From (7) we have
\[ m \varepsilon_K = \alpha \sigma(\alpha) \frac{\sigma(\alpha)}{\alpha} = \sigma(\alpha)^2 \] (9)
so \( m \varepsilon_K \) is a square in \( K^* \). We have
\[ \varepsilon_K + 1 = \frac{\sigma(\alpha)}{\alpha} + 1 = \frac{\alpha + \sigma(\alpha)}{\alpha}, \]
so
\[ \text{Norm}_{K/Q}(\varepsilon_K + 1) = \frac{(\alpha + \sigma(\alpha))^2}{m}, \] (11)
where \( \alpha + \sigma(\alpha) \in \mathbb{Z} \). Hence \( m \text{Norm}_{K/Q}(\varepsilon_K + 1) \) is a square in \( \mathbb{Z} \) and it follows that \( m \) is the squarefree part of \( \text{Norm}_{K/Q}(\varepsilon_K + 1) \) and that \( m > 1 \) since \( \varepsilon_K + 1 > 1 \) with respect to both embeddings of \( K \).

We summarize this in the following proposition.

**Proposition 3.** Suppose \( \text{Norm}_{K/Q}(\varepsilon_K) = +1 \) in \( \mathbb{Q}(\sqrt{d}) \) as above, and let \( m \) denote the squarefree part of the positive integer \( \text{Norm}_{K/Q}(\varepsilon_K + 1) \). Then \( m > 1 \), \( m \) divides the discriminant of \( \mathbb{Q}(\sqrt{d}) \), and \( m \varepsilon_K \) is a square in \( \mathbb{Q}(\sqrt{d}) \).

**Remark 5.** Since the discriminant \( D \) of \( \mathbb{Q}(\sqrt{d}) \) is a square in \( \mathbb{Q}(\sqrt{d}) \), the integers \( m \) and \( D/m \) differ by a square in \( \mathbb{Q}(\sqrt{d}) \), so the squarefree part of \( D/m \) times \( \varepsilon_K \) is also a square in \( \mathbb{Q}(\sqrt{d}) \). As above, one can show that the squarefree part of \( D/m \) is equal to the squarefree part of the positive integer \( -\text{Norm}_{K/Q}(\varepsilon_K - 1) \). Also, if \( A \) is \( 1/2 \) of the positive square root of (the positive square integer) \( m \text{Norm}_{K/Q}(\varepsilon_K + 1) \) and \( B \) is \( 1/2 \) of the negative square root of (the positive square integer) \( -m \text{Norm}_{K/Q}(\varepsilon_K - 1)/d \), then \( \alpha \) in (7) can be taken to be \( A + B\sqrt{d} \).

The following theorem gives a complete classification of the possible indices in (6) in terms of the integers \( d \) and \( m \).

**Theorem 3.** Suppose \( \varepsilon_K \) in \( K = \mathbb{Q}(\sqrt{d}) \) has norm +1 and the positive integer \( m \) is as in Proposition 3. Then

(a) \([E_{K,4} \cap E_K^+ : E_K^2] = 2\) (i.e., \( \varepsilon_K \) is a square mod 4), and so
\[ E_K^2 \subseteq E_{K,4} \cap E_K^+ = E_K^{\square+} = E_K^+ \subseteq \frac{1}{2} E_K, \]
if and only if one of the following conditions is satisfied:
(i) \( d \equiv 1 \mod 4 \) and \( m \equiv 1 \mod 4 \),
(ii) \( d \equiv 3 \mod 4 \) and \( m \) is odd,
(iii) \( d \equiv 2 \mod 4 \) and \( m \equiv 1 \mod 4 \),
(iv) \( d \equiv 2 \mod 8 \) and \( m \equiv 2 \mod 8 \), or
(v) \( d \equiv 6 \mod 8 \) and \( m \equiv 6 \mod 8 \),

(b) \([E_K^+ : E_K^{\square+}] = 2\) (i.e., \( \varepsilon_K \) is not the sum of two squares in \( K \)), and so
\[ E_K^2 = E_{K,4} \cap E_K^+ = E_K^{\square+} \subseteq \frac{1}{2} E_K^+ \subseteq \frac{1}{2} E_K, \]
if and only if \( d \equiv 1 \mod 8 \) and \( m \equiv 3 \mod 4 \), and
(c) in all other cases $[E^\square_K : E^\square_{K, A} \cap E^\square_K] = 2$ (i.e., $\varepsilon_K$ is the sum of two squares in $K$ but is not a square mod 4), and so

$$E^2_K = E^\square_{K, A} \cap E^\square_K \subseteq E^\square_{K, A} \cap E^\square_K = E^\square_K.$$

**Proof.** For (a), we have $[E_{K, A} \cap E^\square_K : E^\square_K] = 2$ if and only if $\varepsilon_K \in E_{K, A} \cap E^\square_K$. Since $m \varepsilon_K$ is a square in $K = \mathbb{Q}(\sqrt{d}), K(\sqrt{v}) = K(\sqrt{m}) = \mathbb{Q}(\sqrt{d}, \sqrt{m})$, so $\varepsilon_K \in E_{K, A} \cap E^\square_K$ if and only if the extension $\mathbb{Q}(\sqrt{d}, \sqrt{m})/\mathbb{Q}(\sqrt{d})$ is unramified at 2.

Since $m$ is a squarefree divisor of the discriminant of $K$, there are several possibilities: (1) $d \equiv 1 \mod 4$ and $m$ is a divisor of $d$, (2) $d \equiv 3 \mod 4$ and $m$ is a divisor of $d$, (3) $d \equiv 3 \mod 4$, and $m = 2d'$ where $d'$ is a divisor of $d$, (4) $d \equiv 2 \mod 4$ and $m$ is a divisor of $d$. For (1), the extension $\mathbb{Q}(\sqrt{d}, \sqrt{m})/\mathbb{Q}(\sqrt{d})$ is unramified at 2 if and only if $m \equiv 1 \mod 4$, which is case (i). For (2), the extension is always unramified at 2, which is case (ii), and for (3) the extension is never unramified at 2. Finally, for (4), precisely one of $m$ and $d/m$ is odd and the extension is unramified at 2 if and only if this odd number is $\equiv 1 \mod 4$, which gives cases (iii), (iv) and (v). This proves (a).

For (b), $m \varepsilon_K$ a square in $K$ implies that $\varepsilon_K$ is a sum of two squares in $K$ if and only if $m$ is a sum of two squares in $K$. Equivalently, $\varepsilon_K$ is a sum of two squares in $K$ if and only if $m$ is a norm from $K(i) = \mathbb{Q}(\sqrt{d}, \sqrt{-1})$ to $K$.

By the Hasse norm theorem, $m$ is a norm from $K(i)$ to $K$ if and only if $m$ is locally a norm from $K(i)_v$ to $K_v$ for every place $v$. Since $m$ is positive, $m$ is locally a norm at the infinite places.

If $v$ does not divide 2 and does not divide $m$, then $K(i)_v$ is unramified over $K_v$ and $m$ is a unit at $v$, so $m$ is locally a norm at $v$.

It remains to consider those primes $v$ that divide 2 and those that divide $m$. If $\mathbb{Q}_v = \mathbb{Q}_p$ for $p$ an odd prime $\equiv 1 \mod 4$ dividing $m$, then $\mathbb{Q}_v(i) = \mathbb{Q}_p$ and $K(i)_v = K_v$, so $m$ is locally a norm at $v$.

For the remaining primes, recall that, by class field theory, the norms $\alpha_v \in K_v$ from $K(i)_v$ to $K_v$ are the elements of $K_v$ such that $\text{Norm}_{K_v/\mathbb{Q}_v}(\alpha_v)$ is a norm from $\mathbb{Q}_v(i)$ to $\mathbb{Q}_v$ (see, for example, [Iw2, Theorem 7.6].

If $\mathbb{Q}_v = \mathbb{Q}_p$ for $p$ an odd prime $\equiv 3 \mod 4$ dividing $m$, then $\mathbb{Q}_v(i) = \mathbb{Q}_p(i)$ is the unramified quadratic extension of $\mathbb{Q}_p$. Since $m$ divides $2d$, the prime $p$ divides $d$, so $K_v = \mathbb{Q}_p(\sqrt{d})$ is ramified of degree 2 over $\mathbb{Q}_p$. Hence $\text{Norm}_{K_v/\mathbb{Q}_v}(m) = m^2$, which is a norm from $\mathbb{Q}_v(i)$ to $\mathbb{Q}_v$, so $m$ is locally a norm at $v$.

Finally, suppose $v$ is a prime dividing 2. As before, if $\mathbb{Q}_2(\sqrt{d})$ is of degree 2 over $\mathbb{Q}_2$, then $\text{Norm}_{K_v/\mathbb{Q}_v}(m) = m^2$, which is a norm from $\mathbb{Q}_2(i)$ to $\mathbb{Q}_2$, so $m$ is a local norm. Hence $m$ is locally a norm at all $v$ unless $\mathbb{Q}_2(\sqrt{d}) = \mathbb{Q}_2$, which requires $d \equiv 1 \mod 8$. In this case, $m$ would be odd, and the units that are norms from $\mathbb{Q}_2(i)$ to $\mathbb{Q}_2$ are the elements congruent to 1 mod 4. Hence $m$ is a local norm from $K(i)_v$ to $K_v$ for every place $v$ unless $d \equiv 1 \mod 8$ and $m \equiv 3 \mod 4$.

This completes the proof of (b) and hence also the proof of the proposition since the three cases are exhaustive and mutually exclusive.  

The following are explicit examples for each of the three possibilities in Theorem 3:
(a) $d = 30$, $\varepsilon_K = 11 + 2\sqrt{30}$, $\text{Norm}_{K/Q}(\varepsilon + 1) = 24$, $m = 6$. Here $\varepsilon_K$ is a square mod 4: $\varepsilon_K = (1 + \sqrt{30})^2 + 4(-5)$ and is a sum of two squares in $K$ (but not the sum of two integral squares): $\varepsilon_K = (1 + \sqrt{30}/5)^2 + (2 + 2\sqrt{30}/5)^2$.

Remark 6. Note that while $\varepsilon_K$ is a square mod 4, it is not globally a square mod 4 in the multiplicative sense: if $\varepsilon_K = \alpha^2(1 + 4\beta)$ with integers $\alpha$ and $\beta$ in $K$, then $\alpha$ would be a unit in $K$, hence of the form $\pm \varepsilon_K^n$ for some integer $n$. Since $\varepsilon_K^2 = 241 + 44\sqrt{30} \equiv 1 \mod 4$, this would imply $\varepsilon_K \equiv 1 \mod 4$, which is not.

(b) $d = 33$, $\varepsilon_K = 23 + 4\sqrt{33}$, $\text{Norm}_{K/Q}(\varepsilon + 1) = 48$, $m = 3$. Here $\varepsilon_K$ is not the sum of two squares in $K$.

(c) $d = 3$, $\varepsilon_K = 2 + \sqrt{3}$, $\text{Norm}_{K/Q}(\varepsilon + 1) = 6$, $m = 6$. Here $\varepsilon_K$ is the sum of two squares in $K$ (but not the sum of two integral squares): $\varepsilon_K = ((1 + \sqrt{3}/2)^2 + (1/2)^2$, and $\varepsilon_K$ is not a square mod 4.

Additional remarks. The unramified quadratic extensions of unit type have other properties that distinguish them from generic quadratic extensions, even among the unramified quadratic extensions of $K$. For example, they have trivial Steinitz class over $K$, a property shared by all the units in $E_{K,4}$ whether or not they are totally positive:

**Proposition 4.** If $\varepsilon \in E_{K,4}$, then the ring of integers $\mathcal{O}_L$ in $L = K(\sqrt{\varepsilon})$ is free (of rank 2) as a module over $\mathcal{O}_K$, in fact $\mathcal{O}_L = \mathcal{O}_K + \mathcal{O}_K(\alpha + \sqrt{\varepsilon})/2$ where $\varepsilon = \alpha^2 + 4\beta$.

**Proof.** By Narkiewicz, [N, Proposition 4.12], if $A = \mathcal{O}_K[a] \subseteq \mathcal{O}_L$ with $a \in \mathcal{O}_L$ generating $L$ over $K$, then $f_A = \delta_{L/K}(a)\delta_{L/K}^{-1}$ where $f_A = \{x \in A \mid x\mathcal{O}_L \subseteq A\}$, $\delta_{L/K}(a)$ is the different of the element $a$ for the extension $L/K$ and $\delta_{L/K}$ is the different of the extension. Since $\mathcal{O}_{L/K} = \mathcal{O}_L$ because $L$ is unramified over $K$, it follows that $A = \mathcal{O}_L$ if and only if $(\delta_{L/K}(a)) = \mathcal{O}_L$. The element $a = (\alpha + \sqrt{\varepsilon})/2$ is a root of the polynomial $x^2 - \alpha x - \beta$, so $\delta_{L/K}(a) = 2a - \alpha = \sqrt{\varepsilon}$, which generates the trivial ideal in $\mathcal{O}_L$ since $\sqrt{\varepsilon}$ is a unit. Hence $A = \mathcal{O}_L$, i.e., $\mathcal{O}_L = \mathcal{O}_K[(\alpha + \sqrt{\varepsilon})/2]$. \hfill $\square$

As noted, the result in Proposition 4 does not require that $\varepsilon$ be totally positive (so the extension $K(\sqrt{\varepsilon})/K$ may be ramified at infinity). The extensions generated by units congruent to squares modulo 4 (but not necessarily totally positive) appear in the work of Haggenmüller ([Ha1], [Ha2]) in the context of ‘free quadratic’, or ‘QF’, extensions of $\mathcal{O}_K$: these are the rings that are free of rank 2 as modules over $\mathcal{O}_K$ that are also separable with a Galois action of order 2 in the sense of Galois theory of rings. It is noted in Haggenmüller ([Ha1, Lemma 2.2]) that the rings of integers of quadratic subfields of the Hilbert class field of $K$ include a complete set of representatives for the nonidentity elements of the group of isomorphism classes of these rings.

It would be interesting to examine the unramified quadratic extensions of unit type with respect to other arithmetic questions, for example capitulation questions, involving $K$.

**Acknowledgments.** I would like to thank Richard Foote and Hershy Kisilevsky for many helpful conversations. I would also like to thank the anonymous referee, who passed along the observation that the squarefree part of $\text{Norm}_{K/Q}(\varepsilon + 1)$ gives an integer $m$ with $m\varepsilon$ a square in $K$ and suggested a complete answer for quadratic fields such as in Theorem 3 would be possible (rather than just examples of each type as in the original manuscript).
References

[A-F] Armitage, J.V., Fröhlich, A.: Class numbers and unit signatures, Mathematika 14 (1967), 94–98.

[D-D-K] Dummit, D., Dummit, E. and Kisilevsky, H.: Signature ranks of units in cyclotomic extensions of abelian number fields, 2018, to appear in Pac. J. Math.

[D-F] Dummit, D. and Foote, R.: Abstract Algebra, Third Edition, John-Wiley, 2004.

[D-V] Dummit, D. and Voight, J.: The 2-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units, to appear in Proc. London Math. Soc., 2018.

[G-H] Greither, C. and Hayes, D.: A note on the theorem of Armitage–Fröhlich, (unpublished). Pre-publication 97-8, Collection Mathématique, Département de Mathématiques et de Statistique, Université Laval, Quebec, Canada, 1–8.

[H] Hayes, D.: On the 2-ranks of Hilbert Class Fields (Working Paper), unpublished.

[Ha1] Haggenmüller, R.: Signaturen von Einheiten und unverzweigte quadratische Erweiterungen total-reeller Zahlkörper, Arch. Math. 39 (1982), 312–321.

[Ha2] Haggenmüller, R.: Diskriminanten und Picard-Invarianten freier quadratischer Erweiterungen, Manuscripta Math. 36 (1981/82), no. 1, 83–103.

[Ha] Hasse, H.: Number Theory, Springer-Verlag, 1978.

[Iw] Iwasawa, K.: A note on ideal class groups. In Ichiro Satake et al. (Eds.), Kenkichi Iwasawa Collected Papers, (Vol. II, pp. 239-247), Springer-Verlag, 2001 (original work published 1966).

[Iw2] Iwasawa, K.: Local Class Field Theory, Oxford University Press, New York, 1986.

[Le] Lemmermeyer, F.: Selmer groups and quadratic reciprocity, Abh. Math. Sem. Univ. Hamburg 76 (2006), 279–293.

[N] Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers, Second Edition, Springer-Verlag, 1980.

[O] Oriat, B.: Relation entre les 2-groupes de classes d’idéaux au sens ordinaire et restreint de certains corps de nombres, Bull. Soc. Math. France 104 (1976), 301-307.

Department of Mathematics, University of Vermont, Lord House, 16 Colchester Ave., Burlington, VT 05405, USA
E-mail address: dummit@math.uvm.edu