Signature Ranks of Units in Real Biquadratic and Multiquadratic Extensions[1]

David S. Dummit
(joint with Hershy Kisilevsky)

Abstract: We prove a number of results on the unit signature ranks of real biquadratic and multiquadratic fields. For example, we give explicit infinite families of real biquadratic fields K for each of the three possible unit signature ranks 1, 2, or 3, in the case when all three quadratic subfields of K have a totally positive fundamental unit. As one application we prove the rank of the totally positive units modulo squares in the totally real subfield of cyclotomic fields can be arbitrarily large.

Maine-Québec Number Theory Conference
University of Maine, Orono
October 5-6, 2019

[1]Additional details/results in paper with same title on arXiv

Suppose F is a totally real field, assumed for simplicity to be Galois, of degree n over $\mathbb{Q}$, and fix a real embedding of F into $\mathbb{R}$.

If $0 \neq \alpha \in F$, the *signature* of α is the n-tuple

$$\mathrm{sgn}(\alpha) = (\ldots, \mathrm{sign}(\sigma(\alpha)), \ldots)_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \in \{\pm 1\}^n,$$

where $\mathrm{sign}(\sigma(\alpha)) = \pm 1$ is the sign of $\sigma(\alpha)$ in the fixed real embedding.

If we identify $\{\pm 1\}$ with the finite field $\mathbb{F}_2$ of two elements, we may view $\mathrm{sgn}(\alpha)$ additively as an element in the vector space $\mathbb{F}_2^n$.

The collection of all the signatures $\mathrm{sgn}(\varepsilon)$ where ε varies over the units of F (the *unit signature group*) is a subspace of $\mathbb{F}_2^n$. The integer between 1 and n given by the rank of this subspace is called the *unit signature rank* of F—it is a measure of how many different possible sign configurations arise from the units of F.

Define the *(unit signature rank) "deficiency" of* F, denoted $\delta(F)$, to be the corank of the unit signature group of F, i.e., n minus the signature rank of the units of F. Then $0 \leq \delta(F) \leq n-1$.

The deficiency of F is the difference between the unit signature rank of F and its maximum possible value, so $\delta(F) = 0$ if and only if there are units of every possible signature type, and $\delta(F) = n-1$ if and only if F has a system of fundamental units that are totally positive.

The deficiency is also the rank of the group of totally positive units of F modulo squares, and measures the difference between the class number and strict (or narrow) class number of F:

$$|C_F^+| = 2^{\delta(F)}|C_F|.$$

The deficiency never decreases in an extension of totally real fields, namely, for any finite extension L/F of totally real fields we have $\delta(F) \leq \delta(L)$, a result of Edgar, Mollin and Peterson (1986).

Proof: Let H_L (resp., H_L^{st}) denote the Hilbert class field (resp. strict Hilbert class field) of L and similarly for F. Then (CFT exercise!) $H_F = H_L \cap H_F^{\mathrm{st}}$, so $[H_F^{\mathrm{st}} : H_F] = 2^{\delta(F)}$ and $[H_L^{\mathrm{st}} : H_L] = 2^{\delta(L)}$, gives the result.

$$\begin{tikzcd}
 & & & \boldsymbol{H_L^{\mathrm{st}}} \\
 & & H_L H_F^{\mathrm{st}} \arrow[ur, dash] \arrow[dd, dash] & \\
 & \boldsymbol{H_L} \arrow[ur, equal] \arrow[dd, dash] & & \\
L \arrow[ur, dash] \arrow[dd, dash] & & \boldsymbol{H_F^{\mathrm{st}}} & \\
 & \boldsymbol{H_F}\ \boxed{(= H_L \cap H_F^{\mathrm{st}})} \arrow[ur, equal] & & \\
F \arrow[ur, dash] & & &
\end{tikzcd}$$

The 'm-technology'

Suppose $k = \mathbb{Q}(\sqrt{d})$ is a real quadratic field ($d > 1$ a squarefee integer) with fundamental unit ε, normalized as usual so that $\varepsilon > 1$ with respect to the embedding of k into $\mathbb{R}$ for which $\sqrt{d} > 0$.

If $\mathrm{Norm}_{k/\mathbb{Q}}(\varepsilon) = +1$ then, by Hilbert's Theorem 90,

$$\boxed{\varepsilon = \sigma(\alpha)/\alpha}$$

for some $\alpha \in \mathbb{Q}(\sqrt{d})$.

The 'm-technology'

Suppose $k = \mathbb{Q}(\sqrt{d})$ is a real quadratic field ($d > 1$ a squarefee integer) with fundamental unit ε, normalized as usual so that $\varepsilon > 1$ with respect to the embedding of k into $\mathbb{R}$ for which $\sqrt{d} > 0$.

If $\mathrm{Norm}_{k/\mathbb{Q}}(\varepsilon) = +1$ then, by Hilbert's Theorem 90,

$$\varepsilon = \sigma(\alpha)/\alpha$$

for some $\alpha \in \mathbb{Q}(\sqrt{d})$.

May further assume:

- $\boxed{\alpha \text{ is an algebraic integer}}$
  (e.g., $\alpha = \sigma(\varepsilon) + 1$)

The 'm-technology'

Suppose $k = \mathbb{Q}(\sqrt{d})$ is a real quadratic field ($d > 1$ a squarefee integer) with fundamental unit ε, normalized as usual so that $\varepsilon > 1$ with respect to the embedding of k into $\mathbb{R}$ for which $\sqrt{d} > 0$.

If $\mathrm{Norm}_{k/\mathbb{Q}}(\varepsilon) = +1$ then, by Hilbert's Theorem 90,

$$\varepsilon = \sigma(\alpha)/\alpha$$

for some $\alpha \in \mathbb{Q}(\sqrt{d})$.

May further assume:

- α is an algebraic integer
- $\boxed{\text{the ideal } (\alpha) \text{ is the product of distinct ramified primes}}$
  $((\alpha)$ is an ambiguous ideal since $(\sigma(\alpha)) = (\alpha))$

The 'm-technology'

Suppose $k = \mathbb{Q}(\sqrt{d})$ is a real quadratic field ($d > 1$ a squarefee integer) with fundamental unit ε, normalized as usual so that $\varepsilon > 1$ with respect to the embedding of k into $\mathbb{R}$ for which $\sqrt{d} > 0$.

If $\mathrm{Norm}_{k/\mathbb{Q}}(\varepsilon) = +1$ then, by Hilbert's Theorem 90,

$$\varepsilon = \sigma(\alpha)/\alpha$$

for some $\alpha \in \mathbb{Q}(\sqrt{d})$.

May further assume:

- α is an algebraic integer
- the ideal (α) is the product of distinct ramified primes
- $\boxed{\alpha \text{ is totally positive, in fact } 0 < \alpha < \sigma(\alpha)}$
  (α and $\sigma(\alpha)$ have the same sign and $\varepsilon > 1$).

- α is an algebraic integer
- the ideal (α) is the product of distinct ramified primes
- $0 < \alpha < \sigma(\alpha)$

With these conditions, the element α is unique.

Let m denote the norm of α:

$$\boxed{m = \alpha\ \sigma(\alpha).}$$

Note that $\varepsilon = \sigma(\alpha)/\alpha$ and $m = \alpha\ \sigma(\alpha)$ implies $m\,\varepsilon = (\sigma(\alpha))^2$, so that

$$\boxed{m\,\varepsilon \text{ is a square in } k.}$$

Hence

$$\boxed{\text{if } \varepsilon \text{ has norm } +1 \text{ in } \mathbb{Q}(\sqrt{d})}$$

then there is a positive, squarefree, integer $m = m_\varepsilon$ such that

- m divides the discriminant of $k = \mathbb{Q}(\sqrt{d})$, $m \neq 1, d$
- m is the norm of an integer in k
- $\Rightarrow$ $m\,\varepsilon$ is a square in k $\Leftarrow$

[Although not needed here, in fact m is the squarefree part of the positive integer $\mathrm{Norm}_{k/\mathbb{Q}}(\varepsilon + 1)$.]

The fact that $m\,\varepsilon$ is a square in k means in particular that

$$\sqrt{\varepsilon} \in k(\sqrt{m}) = \mathbb{Q}(\sqrt{d}, \sqrt{m}).$$

In fact, if

$$\alpha = A + B\sqrt{d},$$

then

$$A > 0\ ,\ \ B < 0 \text{ and } A^2 - dB^2 = m,$$

with

$$\boxed{\sqrt{\varepsilon} = \frac{1}{\sqrt{m}}\,(A - B\sqrt{d})}$$

(all square roots positive). In this expression, $A - B\sqrt{d}$ is totally positive, so this explicit form allows the determination of the sign of various conjugates of $\sqrt{\varepsilon}$—they have the same signs as the corresponding conjugates of $\sqrt{m}$.

Applications

The 'm-technology' gives a very elementary proof of a result of Dirichlet (1834):

Proposition: (Dirichlet) Suppose p is a prime $\equiv 1 \bmod 4$. Then the fundamental unit of $k = \mathbb{Q}(\sqrt{p})$ satisfies $\mathrm{Norm}_{k/\mathbb{Q}}(\varepsilon) = -1$.

Proof. Suppose $\mathrm{Norm}_{k/\mathbb{Q}}(\varepsilon) = +1$. Then the integer $m = m_\varepsilon$ divides p and is neither 1 nor p, which is impossible. $\square$

The next result was also proved by Dirichlet:

Proposition: (Dirichlet) Suppose p_1 and p_2 are primes $\equiv 1 \bmod 4$ with $(\frac{p_1}{p_2}) = -1$. If ε denotes the fundamental unit of $k = \mathbb{Q}(\sqrt{p_1 p_2})$, then $\mathrm{Norm}_{k/\mathbb{Q}}(\varepsilon) = -1$.

Proof. Suppose $\mathrm{Norm}_{k/\mathbb{Q}}(\varepsilon) = +1$. Then the integer $m = m_\varepsilon$ divides $p_1 p_2$ and is neither 1 nor $p_1 p_2$, so $m = p_1$ or p_2.

Next we use the fact that m is the norm of an integer from the quadratic field k. In this case, if $m = p_1$, this would imply

$$a^2 - p_1 p_2 b^2 = 4p_1$$

has integral solutions a, b, which contradicts the fact that p_1 is not a square mod p_2. Similarly m cannot equal p_2, a contradiction concluding the proof. $\square$

These two propositions provide *infinitely many real biquadratic fields* $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$, $p_1 \equiv p_2 \equiv 1 \bmod 4$, *all of whose quadratic subfields have a fundamental unit of norm* -1.

We use the m-technology to show the unit signature rank deficiency of a real multiquadratic extension can be arbitrarily large:

Theorem: Suppose $q_1, q_2, \ldots, q_{2t}$ are distinct primes, each $\equiv 3 \mod 4$. Then the field $L = \mathbb{Q}(\sqrt{q_1 q_2}, \ldots, \sqrt{q_{2t-1} q_{2t}})$ contains at least t totally positive units that are independent modulo squares in L, i.e., the deficiency of L is at least t: $\delta(L) \geq t$.

Proof. Let ε_i be the fundamental unit for the quadratic subfield $k_i = \mathbb{Q}(\sqrt{q_{2i-1} q_{2i}})$ (necessarily of norm $+1$). Then the integer m_i associated to ε_i divides $q_{2i-1} q_{2i}$ and is neither 1 nor $q_{2i-1} q_{2i}$, hence equals q_{2i-1} (if $(\frac{q_{2i-1}}{q_{2i}}) = +1$) or q_{2i} (if $(\frac{q_{2i-1}}{q_{2i}}) = -1$).

Now, suppose some product

$$\varepsilon_1^{a_1} \varepsilon_2^{a_2} \cdots \varepsilon_t^{a_t},$$

where each exponent a_i is either 0 or 1, is a square in L.

$\boxed{\text{Suppose } \varepsilon_1^{a_1}\varepsilon_2^{a_2}\cdots\varepsilon_t^{a_t} \text{ is a square in } L = \mathbb{Q}(\sqrt{q_1q_2},\ldots,\sqrt{q_{2t-1}q_{2t}})}$

Since m_i and ε_i differ by a square in k_i, hence by a square in L, it would follow that the integer

$$m = m_1^{a_1}m_2^{a_2}\cdots m_t^{a_t}$$

would be a square in L.

But if m were a square in L, then $\mathbb{Q}(\sqrt{m})$ would be a subfield of L, so is either $\mathbb{Q}$ or one of the $2^t - 1$ quadratic subfields of L.

As a result, m would differ by a rational square from some product

$$(q_1q_2)^{b_1}\ldots(q_{2t-1}q_{2t})^{b_t}$$

where the exponents b_i are either 0 or 1. Since the q_i are distinct primes and each m_i equals just q_{2i-1} or q_{2i}, it is clear that this can only happen if $a_i = 0$ for every $i = 1, 2, \ldots, t$.

It follows that $\varepsilon_1, \ldots, \varepsilon_t$ are totally positive units that are independent modulo squares in L, which proves the theorem. $\square$

This has the following consequence for cyclotomic fields:

Theorem: Suppose the positive integer n is divisible by at least $2t$ distinct primes congruent to 3 mod 4. Then the unit signature rank deficiency of the maximal real subfield $\mathbb{Q}(\zeta_n)^+$ of the cyclotomic field of nth roots of unity is at least t.

In particular, the unit signature rank deficiency for real cyclotomic fields can be arbitrarily large.

Proof. If $q_1, \ldots, q_{2t}$ are distinct primes congruent to 3 mod 4 that divide n, then $\mathbb{Q}(\sqrt{q_1 q_2}, \ldots, \sqrt{q_{2t-1} q_{2t}}) \subset \mathbb{Q}(\zeta_n)^+$. Since the deficiency never decreases in an extension of totally real fields, the results follow. $\square$

The unboundedness of the unit signature rank deficiency in real cyclotomic fields was proved in *Signature Ranks of Units in Cyclotomic Extensions of Abelian Number Fields*, D. D., Evan Dummit, H. Kisilevsky, Pac. J., 2019, but that proof was conditional on the existence of infinitely many cyclic cubic fields with a totally positive system of fundamental units.

The existence of such cyclic cubic fields has recently been proved by Voight, Breen, Varma, and Elkies.

Remark: As previously mentioned, and used in the previous proof, if F and F' are totally real number fields with $F \subseteq F'$, then their unit signature rank deficiencies satisfy $\delta(F) \leq \delta(F')$ ('the deficiency never decreases').

This is not, in general, due to totally positive units in F that are independent modulo squares in F remaining independent modulo squares in F', however.

For example, the fundamental unit in $\mathbb{Q}(\sqrt{q_1 q_2})$ (distinct primes $q_1 \equiv q_2 \equiv 3 \bmod 4$) is always a square in $\mathbb{Q}(\sqrt{q_1}, \sqrt{q_2})$. Hence, if $n = 4q_1 q_2 \ldots q_{t-1} q_t$, then *all* t of the units used to show that $\delta(\mathbb{Q}(\zeta_n)^+) \geq t$ are squares in $\mathbb{Q}(\zeta_n)^+$, i.e., *none* of these units *themselves* contribute to the deficiency of $\mathbb{Q}(\zeta_n)^+$.

Unit Signatures in Real Biquadratic Fields

Suppose K is a real biquadratic extension of $\mathbb{Q}$ with unit group E_K, having quadratic subfields k_1, k_2, k_3, with corresponding fundamental units ε_1, ε_2 and ε_3.

Then

$$E_K / \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$$

is an elementary abelian 2-group of rank at most 3.

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
k_1 \arrow[dr, dash] & k_2 \arrow[d, dash] & k_3 \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

While the fundamental units ε_1, ε_2 and ε_3 from the quadratic subfields are independent units in the biquadratic field K, even if none of these units is totally positive, they do not have independent signs:

EXAMPLE: Suppose each ε_i has norm -1, i.e., the units of the subfields k_1, k_2, and k_3 have all possible (namely, two) signatures. The matrix of signatures of $\{-1, \varepsilon_1, \varepsilon_2, \varepsilon_3\}$ (viewed additively: 0 if the sign is positive, 1 if negative) in the biquadratic field K is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

which has rank 3—so the unit signature rank of the units of K is either 3 or 4, and if it is 4 it is not due simply to the signs of the units from the quadratic subfields.

EXAMPLE: $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$

$$\sigma : \begin{cases} \sqrt{5} \mapsto 2.236... \\ \sqrt{13} \mapsto -3.606... \end{cases} \qquad \tau : \begin{cases} \sqrt{5} \mapsto -2.236... \\ \sqrt{13} \mapsto 3.606... \end{cases}$$

	id	σ	τ	$\sigma\tau$
-1	-1	-1	-1	-1
$\varepsilon_1 = (1+\sqrt{5})/2$	1.618...	1.618...	$-0.6180...$	$-0.6180...$
$\varepsilon_2 = (3+\sqrt{13})/2$	3.303...	$-0.303...$	3.303...	$-0.303...$
$\varepsilon_3 = 8+\sqrt{65}$	16.062...	$-0.062...$	$-0.062...$	16.062...
$(7+5\sqrt{5}+3\sqrt{13}+\sqrt{65})/4$	9.265...	$-0.175...$	$-0.356...$	$-1.734...$

with signatures $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$, so in fact K has unit signature rank 4.

For each possibility of signatures for the units ε_1, ε_2, ε_3 we show there exist infinitely many biquadratic fields with each of the possible unit signature ranks.

For example, if ε_1, ε_2, ε_3 all have norm $+1$, they contribute nothing to the unit signature rank of the biquadratic K. We prove there are infinitely many fields K of each of the possible signature ranks 1,2, or 3. The situation of rank 2 or 3 is relatively straightforward, but the situation of rank 1, i.e., where the biquadratic has a system of totally positive fundamental units, requires more work.

Theorem: Suppose the primes $q_1, \ldots, q_6$, each $\equiv 3 \bmod 4$, are chosen so that the following quadratic residue relations are satisfied:

$$\left(\frac{q_1}{q_2}\right) = \left(\frac{q_1}{q_3}\right) = \left(\frac{q_1}{q_4}\right) = \left(\frac{q_1}{q_5}\right) = -1, \left(\frac{q_1}{q_6}\right) = \left(\frac{q_2}{q_3}\right) = +1,$$

$$\left(\frac{q_2}{q_4}\right) = -1, \left(\frac{q_2}{q_5}\right) = +1, \left(\frac{q_2}{q_6}\right) = \left(\frac{q_3}{q_4}\right) = +1,$$

$$\left(\frac{q_3}{q_5}\right) = -1, \left(\frac{q_3}{q_6}\right) = \left(\frac{q_4}{q_5}\right) = +1, \left(\frac{q_4}{q_6}\right) = \left(\frac{q_5}{q_6}\right) = -1.$$

Let ε_1 denote the fundamental unit for $k_1 = \mathbb{Q}(\sqrt{q_1q_2q_3q_4})$, ε_2 the fundamental unit for $k_2 = \mathbb{Q}(\sqrt{q_1q_2q_5q_6})$, and ε_3 the fundamental unit for $k_3 = \mathbb{Q}(\sqrt{q_3q_4q_5q_6})$. Then $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ is a set of fundamental units for the biquadratic field $K = \mathbb{Q}(\sqrt{q_1q_2q_3q_4}, \sqrt{q_1q_2q_5q_6})$, so there exist infinitely many real biquadratic fields K having unit signature rank 1.

Example: $K = \mathbb{Q}(\sqrt{31 \cdot 47 \cdot 67 \cdot 7}, \sqrt{31 \cdot 47 \cdot 19 \cdot 11})$ with $C_K \cong (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})$ and $C_K^+ \cong (\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/4\mathbb{Z})^2$.

Proof. (Sketch)

- $\boxed{m_1 = q_2q_3q_4}$ for the field $\mathbb{Q}(\sqrt{q_1q_2q_3q_4})$.

  All other possibilities are ruled out. For example, suppose $m_1 = q_1q_4$. Then $a^2 - q_1q_2q_3q_4b^2 = 4q_1q_4$ has solutions, as also does $q_1q_4(a')^2 - q_2q_3b^2 = 4$. This implies
  $$\left(\frac{q_1}{q_2}\right)\left(\frac{q_4}{q_2}\right) = +1,$$
  but by assumption
  $$\left(\frac{q_1}{q_2}\right) = -1 \quad \text{and} \quad \left(\frac{q_2}{q_4}\right) = -1.$$

- $\boxed{m_2 = q_2}$ for the field $\mathbb{Q}(\sqrt{q_1q_2q_5q_6})$ and $\boxed{m_3 = q_4q_6}$ for the field $\mathbb{Q}(\sqrt{q_3q_4q_5q_6})$.

- $m_1^{n_1}m_2^{n_2}m_3^{n_3}$ $(n_1, n_2, n_3 \in \{0, 1\}$, not all 0) is, up to a square, one of q_2, q_3q_4, $q_2q_3q_4$, q_3q_6, $q_2q_3q_6$, q_4q_6, or $q_2q_4q_6$.

- none of these is $1, q_1q_2q_3q_4, q_1q_2q_5q_6$ or $q_3q_4q_5q_6$

$\square$

For biquadratic fields where one of the subfields has fundamental unit of norm -1, different techniques are required.

Case: ε_1, ε_2, ε_3 all have norm -1, the biquadratic K has rank 3.

Theorem: Suppose $n > 1$ is an integer with $n \not\equiv 2 \bmod 5$ such that $n^2 + 1$ and $(n+1)^2 + 1$ are both squarefree. Then each of the fundamental units ε_1, ε_2, and ε_3 of the three quadratic subfields of $K = \mathbb{Q}(\sqrt{n^2+1}, \sqrt{(n+1)^2+1}\,)$ has norm -1 and the unit signature rank of K is 3: a set of fundamental units for K is given by $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$. There are infinitely many such fields.

Proof. (Sketch)

- If $N = n(n+1) + 1$, $N^2 + 1$ is squarefree ($n \not\equiv 2 \bmod 5$).
- $\varepsilon_1 = n + \sqrt{n^2+1}$, $\varepsilon_2 = (n+1) + \sqrt{(n+1)^2+1}$, and $\varepsilon_3 = N + \sqrt{N^2+1}$, and each has norm -1
- $\varepsilon_1\varepsilon_2\varepsilon_3$ is not a square in K : if $\eta = \sqrt{\varepsilon_1\varepsilon_2\varepsilon_3} \in K$, then $\mathrm{Norm}_{K/k_1}(\eta) = (-1)^{\nu_1}\varepsilon_1$, $\mathrm{Norm}_{K/k_2}(\eta) = (-1)^{\nu_2}\varepsilon_2$, and then $\mathrm{Norm}_{K/k_3}(\eta) = (-1)^{\nu_1+\nu_2+1}\varepsilon_3$ for some $\nu_1, \nu_2 \in \{0, 1\}$; writing $\eta = x + y\sqrt{n^2+1} + z\sqrt{(n+1)^2+1} + w\sqrt{N^2+1}$, x, y, z, w rational leads to a contradiction because n^2+1, $(n+1)^2+1$ and N^2+1 are squarefree and greater than 2 (since $n > 1$).
- Easy sieve shows infinitely many n. $\square$

Thank you for your attention.

A special thank you
to the conference organizers,
particularly Professor Andrew Knightly.

Thank you also to Eduardo Friedman and Robert Auffarth, whose questions involving unit signature ranks in cyclotomic extensions and their application to the number of principal polarizations of abelian varieties prompted us to take a closer look at multiquadratic extensions.