NOTES ON UNITS IN QUADRATIC FIELDS

JACQUES MARTINET

Abstract. These are notes on units in quadratic fields, taken from a first draft of March 23 rd, 2018, to which I have added on November 20 th, 2020, this abstract and a few references before putting them on line.

Ambiguous classes. We shall make use of the two formulae below which describe invariant classes in a cyclic extension of prime degree ℓ, especially when $\ell = 2$. These classes are called (from Hilbert) *ambiguous classes*. We refer to Lemmermeyer for the notation and proofs. Thus, let L/K be a cyclic extension of number fields, of degree ℓ and Galois group $G = \langle\sigma\rangle$, $\mathrm{Am}(L/K)$ is the group of invariant classes, and Am_{st} *st for strict* is the subgroup of Am of those classes which contain an invariant ideal. In a finite extension k_1/k_0, N_{k_1/k_0} (or N for short) denotes the norm, and Tr_{k_1/k_0} (or Tr for short) denotes the trace.

We shall also make use of the some traditional notation relative to a number field k: Cl_k denotes its class group, h_k the order of Cl_k, E_k its unit group, and μ_K its subgroup of roots of unity. Moreover, $\delta_{k'/k}$ denotes the discriminant (an ideal in k) of the finite extension k'/k.

Theorem 0.1. (Ambiguous classes formulae). *The orders of the groups* $\mathrm{Am}(L/K)$ *and* $\mathrm{Am}_{st}(L/K)$ *are as follows:*

$$|\mathrm{Am}(L/K)| = h_K \, \frac{\ell^{t-1}}{[E_K : E_K \cap \mathrm{N}(L^*)]} \, ;$$

$$|\mathrm{Am}_{st}(L/K)| = h_K \, \frac{\ell^{t-1}}{[E_K : \mathrm{N}(E_L)]} \, .$$

In these formulae t *denotes the number of ramified primes in* L/K, including the infinite primes.

Note that infinite primes need not be considered unless $\ell = 2$. Another specificity of quadratic extensions is that if $h_K = 1$, then for any $c \in \mathrm{Cl}_L$, we have $c \cdot \sigma c = 1$, so that $c^2 = 1$ holds if and only if c belongs to $\mathrm{Am}_{L/K}$. (If $\ell > 2$ there may exists cyclic fields of degree ℓ having non-invariant classes of order ℓ besides invariant ones.)

In the sequel, given a finite Abelian group A, we set

2000 *Mathematics Subject Classification.* 11R11.

Key words and phrases. quadratic fields, units, (narrow) classes.

$$_\ell A = \{x \in A \mid x^\ell = 1\} \text{ and } d_\ell(A) = \dim_{\mathbb{F}_\ell} {}_\ell A\,.$$

Note that we also have (by duality) $d_\ell(A) = \dim_{\mathbb{F}_\ell} A/\ell A$.

Here are a few comments.

(1) The first unit index divides the second, and equality between them characterizes extensions in which every invariant class contains an invariant ideal.
(2) If h_K is prime to ℓ and if a unique prime ramifies in L/K, then h_L is also prime to ℓ.
(3) If L/K is unramified, then some non-principal ideal in K becomes principal in L. (This is Hilbert's theorem 94.)
(4) Thanks to Hasse's norm theorem in cyclic extensions, the first index can be calculated locally once E_K is known; the second index is of a global nature, and except in special cases, its calculation needs the knowledge of E_L.
(5) In his thesis, Chevalley extended Theorem 0.1 to arbitrary cyclic extensions, in order to simplify the proofs of Class Field Theory (CFT for short). However this generalization is not very useful for explicit calculations of class groups and units.

Related results. Besides Theorem 0.1 we quote two related results, namely the *Hasse index theorem* (1) and the *relative Stickelberger congruence* (2).

(1) *Let K be a CM field (K is a totally imaginary quadratic extension of a totally real number field K_0). Then the* Hasse index $[E_K : \mu_K E_{K_0}]$ *is equal to* 1 *or* 2.

(2) *Let L/K be a finite extension of number fields. Then we have* $\mathrm{N}_{L/K}(\delta_{L/K}) \equiv 0$ *or* $(1)^c \mod 4$*, where c denotes the number of complex embeddings of L ramified in L/K (i.e., lying above a real embedding of K).* [This reduces to the case of quadratic extensions, the only interesting case. For instance it tells us that in an extension which ramifies only at infinite primes, then c is even.]

Also ambiguous classes formulae have a "narrow" counterpart, established by Gras; we shall not use them, but shall make use of the *narrow class group* Cl_k^+ (group of fractional ideals modulo its subgroup of principal ideals having a totally positive generator), the order of which we denote by h_k^+. We have a natural epimorphism $\mathrm{Cl}_k^+ \to \mathrm{Cl}_k$, the kernel of which is 2-elementary; if k has signature (r_1, r_2) ($r_1 + 2r_2 = [k : \mathbb{Q}]$), its rank is bounded from above by $r_1 - 1$ (0 if $r_1 = 0$).

Quadratic fields: standard results. We consider a quadratic field $K = \mathbb{Q}(\sqrt{m})$ where $m \in \mathbb{Z}$ is square-free, of discriminant d. We consider the three possible congruences $m \equiv 1, 2, 3 \mod 4$ related to the exponent (0, 2 or 3) of 2 in d; we have $d \equiv 1 \mod 4$, $d \equiv 0 \mod 8$

and $d \equiv 4 \mod 8$, and more precisely $d \equiv 1 \mod 4$, $d \equiv 8 \mod 16$ and $d \equiv 12 \mod 16$, respectively.

We denote by r *the number of ramified prime numbers in* K; thus if $d < 0$ Theorem 0.1 must be applied with $t = r + 1$. The unit indices are 2 or 1, depending on whether -1 is a norm (from K^* of from E_K), and we have $-1 \in \mathrm{N}(K^*)$ if and only if d is a sum of two squares in $\mathbb{Q}^*$, thus if and only if d is positive and is not divisible by a prime congruent to 3 modulo 4 (Hasse's norm theorem, here equivalent to the Hasse-Minkowski theorem for binary quadratic forms).

Hilbert's results on the 2-rank of class groups of quadratic field can be recovered by applying Theorem 0.1, considering three cases as suggested by the above discussion:

(1) *K imaginary: then $d_2(Cl_K) = r - 1$;*
(2) *K is real and at least some prime $\ell \equiv 3 \mod 4$ ramifies in K: then $d_2(Cl_K) = r - 2$;*
(3) *K is real and no prime $\ell \equiv 3 \mod 4$ ramifies in K: then $d_2(Cl_K) = r - 1$.*

Moreover all classes of order 2 *contain an invariant ideal except in case (3) if a fundamental unit ε has norm -1, where only half of them contain an invariant ideal.*

[Note that in particular h_k is odd if and only if either $r = 1$, or $r = 2$, K is real, and at least one prime $\ell \equiv 3 \mod 4$ ramifies in K, and that in the former case, $\mathrm{N}(\varepsilon) = -1$ if K is real.]

The special rule which holds in case (2) disappears if we consider the narrow class group Cl_K^+ instead of the ordinary class group Cl_K. To this end we may (though this could be avoided) consider unramified quadratic extensions of K. These are Galois of type $(2, 2)$ over $\mathbb{Q}$. Since a biquadratic field L containing three quadratic subfields K_i of discriminant d_i has discriminant $d_L = d_1 d_2 d_3$ (product of conductors), L/K_3, say, is (weakly) unramified if and only if $d_3 = d_1 d_2$. We find this way 2^{r-1} weakly unramified quadratic extensions of K_3 (including K_3/K_3), half of which are imaginary in case (2), all real in case (3).

This shows that $d_2(Cl_k+) = r-1$ in all cases, and consequently that the extension $\mathrm{Cl}_k^+ \to \mathrm{Cl}_k$ splits except in case (3) when $\mathrm{N}(\varepsilon) = -1$.

We shall consider later unramified extensions of the form $K(\sqrt{\pm\varepsilon})$. Just note for the while that $K(\sqrt{-1})$ is unramified if and only if $m \equiv 3 \mod 4$, corresponding to the choice $d_1 = -4$.

Quadratic fields: extracting square roots of units. Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field, of discriminant d ($d = m$ or $d = 4m$), and let ε be a fundamental unit of positive trace. Write $\varepsilon = a + b\sqrt{m}$.

Replacing ε by its cube if need be, we may assume that $a, b \in \mathbb{Z}$. Then if $m \equiv 1 \mod 4$ and $\mathrm{N}(\varepsilon) = -1$ (resp. $+1$), a is even (resp. odd).
[If $\varepsilon = \frac{\alpha+\beta\sqrt{m}}{2}$ and $\varepsilon^3 = a + b\sqrt{m}$, then if $\mathrm{N}(\varepsilon) = -1$ (resp. $+1$), we have $a \equiv 2 \mod 4$ (resp. $a \equiv -\alpha \mod 4$).]
If $m \equiv 2 \mod 4$, or if $m \equiv 1 \mod 4$ and $\mathrm{N}(\varepsilon) = +1$, a is odd, whereas both parities may occur if $m \equiv 3 \mod 4$, which suggest that in this latter case, the parity of a (we shall say the *parity of* ε) might be a kind of analogue of the sign of the units in the former cases.

If $\mathrm{N}(\varepsilon) = -1$, $K(\sqrt{\varepsilon})$ and $K(\sqrt{-\varepsilon})$ define two pairs (L_+, L'_+) and (L_-, L'_-) of non-Galois quartic fields having the same Galois closure M, dihedral with Galois group D_4 of degree 8 over $\mathbb{Q}$, cyclic over $\mathbb{Q}(\sqrt{-1})$, "the" outer automorphism of D_4 exchanging the pairs (L_+, L'_+) and (L_-, L'_-).

Assume now that $\mathrm{N}(\varepsilon) = +1$. Then extracting a square root of ε (or of $-\varepsilon$) is explicit: solving the equation $\sqrt{u_1} + \sqrt{u_2} = \sqrt{\varepsilon}$ we find the two equations

$$u_1 + u_2 = a \text{ and } u_1 u_2 = \tfrac{mb^2}{4}\,,$$

hence

$$\{u_1, u_2\} = \{\tfrac{a-1}{2}, \tfrac{a+1}{2}\}\,,$$

and similarly $\{u_1, u_2\} = \{\frac{-a-1}{2}, \frac{-a+1}{2}\}$ for $\sqrt{-\varepsilon}$.

Assume first that a is odd. Then writing $u_1 = m_1\lambda_1^2$ and $u_2 = m_2\lambda_2^2$ with square-free m_1, m_2, we have $m_1 m_2 = m$ and $\lambda_1\lambda_2 = \pm\frac{b}{2}$. (To deal with $K(\sqrt{-\varepsilon})$, one just has to replace (m_1, m_2) by $(-m_2, -m_1)$.) It is clear that both extensions are (weakly) unramified if $m \equiv 3 \mod 4$ and that only one of them is otherwise, and that this is $\mathbb{Q}(\sqrt{+\varepsilon})$ if d has no prime factor $\ell \equiv 3 \mod 4$.

Note than if one of u_1, u_2 were a square, then ε would be itself a square, which is excluded. This remark has the following consequence:

If m is an odd prime ℓ, then a is even.
[If $\ell \equiv 1 \mod 4$ we recover the fact (Hilbert) that $\mathrm{N}(\varepsilon) = -1$.]

If $\ell \equiv 3 \mod 4$ we prove below a more precise result:

Statement 1. *If $\ell \equiv 3 \mod 8$ (resp. $\ell \equiv 7 \mod 8$), then $a - 1$ (resp. $a + 1$) is an odd square. In particular, we have $a \equiv 2 \mod 8$ (resp. $a \equiv 0 \mod 8$).*

Indeed, since $(a-1)(a+1) = \ell b^2$, $a-1$ or $a+1$ is a square. If $\ell \equiv 3 \mod 8$, we have trivially $a \equiv 2 \mod 4$, hence $a+1 \equiv 3 \mod 4$ is not a square, so that $a-1$ is an odd square, and is congruent to 1 modulo 8. The case when $\ell \equiv 7 \mod 8$ is dealt with in the same way. □

If a is even, then both the extensions $K\sqrt{\pm\varepsilon}/K$ are ramified (above 2). Explicitly, we have

$$\varepsilon = \eta^2 \text{ with } \eta = \frac{\sqrt{2(a-1)}+\sqrt{2(a+1)}}{2},$$

so that, in $K(\sqrt{-1},\sqrt{\varepsilon})$, we have

$$\pm\eta = i\frac{\sqrt{a-1}+\sqrt{a+1}}{1+i}.$$

Embedding quadratic fields into biquadratic fields. Embedding a quadratic field K into a biquadratic field L and applying Theorem 0.1 to the various quadratic extensions L/K_i (where, say, $K = K_3$) proves often useful to obtain properties of h_K and its fundamental unit ε.

We denote by $K_i = \mathbb{Q}(\sqrt{m_i})$ (m_i square-free) the quadratic subfields, d_i their discriminants, h_i their class numbers, E_i their unit groups, ε_i (when K_i is real) their fundamental units, and similarly h and E for L. We also denote by N_i (resp. N'_i) the norm in L/K_i (resp. in $K_i/\mathbb{Q}$) and by $\mathrm{N} = \mathrm{N}'_i \circ \mathrm{N}_i$ the norm in $L/\mathbb{Q}$.

Let Q be the index in E of the product of the E_i. If L is imaginary, this is a Hasse index, equal to 1 or 2. If L is real, Q may be equal to 1, 2 or 4. Indeed it suffices to evaluate the number of products of $\pm\varepsilon_i$ which are totally positive. If one ε_i has norm -1, the only possibility is $\varepsilon_1\varepsilon_2\varepsilon_3$, hence $Q = 1$ or 2. Otherwise, we must consider products of ε_i of norm $+1$. If $\varepsilon_3 = \eta^2$, we have $m_3 = m_1m_2$, so that at most one of the ε_i can be a square in L. There remains the possibilities $\varepsilon_1\varepsilon_2\varepsilon_3 = \eta^2$ or $\varepsilon_2\varepsilon_3 = \eta^2$ with $\varepsilon_2, \varepsilon_3$ of the same parity, whence $Q \le 4$, with equality only if $L = \mathbb{Q}(\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2\varepsilon_3})$.

In the examples we shall consider we shall choose as often as possible the following notation: p, p_i stand for primes congruent to 1 modulo 4 (or maybe $p = 2$ or $p_1 = 2$) whereas q, q_i stand for primes congruent to 3 modulo 4. Thus in Statement 1 we could have written q instead of ℓ, a notation we use in the next neighbour statement.

Statement 2. *Let $K = \mathbb{Q}(\sqrt{2q})$, $q \equiv 3 \mod 4$, with fundamental unit $\varepsilon = a + b\sqrt{2q}$. Then if $q \equiv 3 \mod 8$ (resp. $q \equiv 7 \mod 8$), $a-1$ (resp. $a+1$) is a square.*

Indeed take for L the compositum of $K_1 = \mathbb{Q}(\sqrt{-p})$ and $K_2 = \mathbb{Q}(\sqrt{-2})$, so that $K_3 = \mathbb{Q}(\sqrt{2q})$. Write $\varepsilon_3 = a + b\sqrt{2q}$. In L we have

$$-\varepsilon_3 = \eta^2 \text{ where } \eta = \sqrt{-\tfrac{a-1}{2}} + \sqrt{-\tfrac{a+1}{2}}.$$

Recall that $\frac{a\mp1}{2} = 2\lambda^2$ and $\frac{a\pm1}{2} = q\mu^2$. We now apply the ambiguous class formulae, noting that $E = \langle -1, \eta\rangle$. If $q \equiv 3 \mod 8$, we have $t = 1$ in L/K_1, hence $\mathrm{N}_1(E) = E_1$, and $-1 \in \mathrm{N}_1(E)$ implies that $\frac{a-1}{2} = 2\lambda^2$. If $q \equiv 7 \mod 8$, we apply the same augments, replacing

L/K_1 by L/K_2. □

[The equalities $a = 2\lambda^2 + q\mu^2$ and $2\lambda^2 - q\mu^2 = \mp 1$ moreover show that we have $a \equiv 5 \mod 32$ (resp. $a \equiv -1 \mod 16$).]

Statements involving norms of units (and/or class numbers) are more strongly motivated than mere congruence properties of units, and consequently numerous papers have been published on these questions. Here is a well-known example.

Example 1. *Let* $K = \mathbb{Q}(\sqrt{p_1 p_2})$, $p_i \equiv 1 \mod 4$ *(or* $p_1 = 2$*).*
If $\left(\frac{p_1}{p_2}\right) = -1$, *then* $h_K \equiv 2 \mod 4$ *and* $\mathrm{N}(\varepsilon_K) = -1$.

Indeed take $K_1 = \mathbb{Q}(\sqrt{p_1})$ and $K_2 = \mathbb{Q}(\sqrt{p_3})$, so that $K = K_3$. In L/K_1 we have $t = 1$, which implies that h is odd and that $E_1 = \mathrm{N}(E)$, hence that $\varepsilon_1 = \mathrm{N}_1(\eta)$ for some unit η of L. We then have

$$\mathrm{N}'_3\left(\mathrm{N}_3(\eta)\right) = \mathrm{N}(\eta) = \mathrm{N}'_1\left(\mathrm{N}_1(\eta)\right) = \mathrm{N}'_1(\varepsilon_1) = -1\,,$$

which shows that $\mathrm{N}'_3(\varepsilon_3) = -1$, and making use of L/K_3, we check that $h_3 \equiv 2 \mod 4$. □

Note that we may achieve $\eta^2 = \varepsilon_1\,\varepsilon_2\,\varepsilon_3$, as in the numerical example below for which $m_1 = 5$, $m_2 = 13$ and $m_3 = 5 \cdot 13$:

$$\varepsilon_1 = \tfrac{1+\sqrt{5}}{2},\ \varepsilon_2 = \tfrac{1+\sqrt{13}}{2},\ \varepsilon_3 = 8 + \sqrt{65},\ \text{ and }\ \eta = \tfrac{7+5\sqrt{5}+3\sqrt{13}+\sqrt{65}}{4}\,.$$

For products $p_1 p_2$ with $\left(\frac{p_1}{p_2}\right) = +1$, $\mathrm{N}(\varepsilon)$ may be $+1$ or -1. Examples: $\mathrm{N}(35 + 6\sqrt{34}) = \mathrm{N}(\frac{15+\sqrt{221}}{2}) = +1$, $\mathrm{N}(9 + \sqrt{82}) = \mathrm{N}(12 + \sqrt{145}) = -1$.

Real quadratic fields with two ramified primes. Besides fields $\mathbb{Q}(\sqrt{q})$, $\mathbb{Q}(\sqrt{2q})$ and $\mathbb{Q}(\sqrt{p_1 p_2})$ (including $p_1 = 2$) considered above, there remains a fourth possibility, namely $\mathbb{Q}(\sqrt{q_1 q_2})$. Here q_1 and q_2 do not play the same rôle, because $\left(\frac{q_1}{q_2}\right)\left(\frac{q_2}{q_1}\right) = -1$. Exchanging q_1 and q_2 if need be, we may assume that $\left(\frac{q_2}{q_1}\right) = +1$.

Statement 3. *Let* $K = \mathbb{Q}(\sqrt{m})$, $m = q_1 q_2$, *with fundamental unit* $\varepsilon = a + b\sqrt{m}$. *Then we have* $a \equiv 1 \mod q_1$ *and* $a \equiv -1 \mod q_2$.

We prove this taking $K_1 = \mathbb{Q}(\sqrt{q_1})$ and $K_2 = \mathbb{Q}(\sqrt{q_2})$, hence $K = K_3$. As a system of fundamental units for L take $\{\varepsilon_1, \eta, \eta'\}$ where $\eta^2 = \varepsilon_3$ and $\eta'^2 = \varepsilon_1\varepsilon_2$. Since a single prime ramifies in L/K_1, we have $\mathrm{N}_1(E) = E_1$, and since $\mathrm{N}_1(\eta') = \pm\varepsilon_1$, we have $\mathrm{N}_1(\eta) = -1$, which means that modulo squares, we have $\frac{a-1}{2} = q_1\lambda^2$ and $\frac{a+1}{2} = q_2\mu^2$ for some $\lambda, \mu \in \mathbb{Z}$.
[Alternative proof: work in $\mathbb{Q}(\sqrt{-q_1}, \sqrt{-q_2})$.] □

Real quadratic fields with three ramified primes. We consider the case when $m = pq$ so that $2, p, q$ ramify, and again consider the parity of the fundamental unit ε of $K := \mathbb{Q}(\sqrt{m})$.

Statement 4. *Let $K = \mathbb{Q}(\sqrt{m})$, $m = pq$, with fundamental unit $\varepsilon = a + b\sqrt{m}$. Assume that $\left(\frac{p}{q}\right) = -1$. Then a is even, and according to the classes modulo 8 of p and q, we have*

(1) $(p, q) \equiv (1, 7)$: $p, q \mid a - 1$;
(2) $(p, q) \equiv (1, 3)$: $p, q \mid a + 1$;
(3) $(p, q) \equiv (5, 7)$: $p \mid a - 1$, $q \mid a + 1$;
(4) $(p, q) \equiv (5, 3)$: $p \mid a + 1$, $q \mid a - 1$.

Without any hypothesis on $\left(\frac{p}{q}\right)$ take $K_1 = \mathbb{Q}(\sqrt{q})$ and $K_2 = \mathbb{Q}(\sqrt{p})$, so that $K = K_3$ and $\varepsilon = \varepsilon_3$. We know that h_1 and h_2 are odd and that $\mathrm{N}'_2(\varepsilon_2) = -1$, which shows that $-1 \in \mathrm{N}_1(E)$, and moreover that modulo squares, a unit in $\prod E_i$ can be a square only if it is one of ε_1, ε_3 or $\varepsilon_1\varepsilon_3$. But ε_1 is of even type. Hence as a system of fundamental units for L we may take $\{\varepsilon_1, \varepsilon_2, \eta\}$ where if ε_3 is even (resp. odd), $\eta^2 = \varepsilon_1\varepsilon_3$ (resp. $\eta^2 = \varepsilon_3$), which implies that $\mathrm{N}_1(\eta) = \pm\varepsilon_1$ (resp. $\mathrm{N}_1(\eta) = \pm 1$), hence $[E_1 : \mathrm{N}_1(E)] = 1$ (resp. $[E_1 : \mathrm{N}_1(E)] = 2$).

Assume now that $\left(\frac{p}{q}\right) = -1$. In L/K_1 we then have $t = 1$, hence $[E_1 : \mathrm{N}_1(E)] = 1$, which shows that $\varepsilon_1\varepsilon_3$ is a square, hence that ε_3 is of even type, and that $h \equiv 1 \mod 2$.

In L/K_2 ramified primes are one prime above q and one (resp, two) primes above 2 if $p \equiv 5 \mod 8$ (resp. $p \equiv 1 \mod 8$), and since ε_2 (of norm -1) is not a norm in L/K_2, we have $[E_2 : \mathrm{N}_2(E)] = 2$ (resp. 4), thus $-1 \in \mathrm{N}_2(E)$ (resp. $-1 \notin \mathrm{N}_2(E)$).

Write $\varepsilon_1 = \frac{\nu_1^2}{2}$ and $\varepsilon_3 = \frac{\nu_3^2}{2}$, where

$$\nu_1 = \alpha_1 + \beta_1\sqrt{q} \text{ and } \nu_3 = \alpha_3\sqrt{q} + \beta_3\sqrt{p} \text{ or } \alpha_3 + \beta_3\sqrt{pq}\,.$$

Observe that if the second case holds for ν_3 then p divides $a - 1$ or $a+1$, which implies $\pm 2 \equiv \alpha_3^2 \mod p$, hence $p \equiv 1 \mod 8$, and similarly $\pm 2 \equiv q a_3^2 \mod p$, hence $p \equiv 5 \mod 8$ if the first case holds.

The norm $\mathrm{N}_2(\nu_1\nu_3)$ is thus negative (resp. positive), and since we know the sign of $\alpha_1^2 - q\beta_1^2$ by Statement 1, we can check that the divisibility of $a + 1$ and $a - 1$ by p is as given in the statement; the corresponding result for q then follows. □

Statement 5. *Let $K = \mathbb{Q}(\sqrt{m})$, $m = pq$, with fundamental unit $\varepsilon = a + b\sqrt{m}$. Assume that $\left(\frac{p}{q}\right) = +1$ and $p \equiv 5 \mod 8$. Then a is odd, p divides $a + 1$, and q divides $a - 1$.*

We keep the notation above. Since $\left(\frac{p}{q}\right) = +1$, p splits in $K_1 = \mathbb{Q}(\sqrt{q})$. For any $\mathfrak{p} \mid p$ in K_1, we have

$$\left(\tfrac{\varepsilon_1}{\mathfrak{p}}\right) = \left(\tfrac{\nu_1^2/2}{\mathfrak{p}}\right) = \left(\tfrac{2}{\mathfrak{p}}\right) = \left(\tfrac{2}{p}\right) = -1\,.$$

In L/K_1 we have $t = 2$ and $-1 \in \mathrm{N}_1(\varepsilon_2) \in E_1$, but $2 \notin \mathrm{N}_1(L^*)$. This shows first that $h = 1$, and next that ε_1 is not a norm in L/K_1, hence

that $\varepsilon_1\varepsilon_3$ is not a square, which shows that ε_3 is odd, hence the square of a unit η_3, of the form $\alpha_3\sqrt{q}+\beta_3\sqrt{p}$.

In L/K_2 we have $t=3$ (two ideals above q and one above 2). Since h and h_2 are odd, we have $[E_2 : \mathrm{N}_2(E)]=4$, which shows that $-1\notin \mathrm{N}_2(E)$, hence that $\mathrm{N}_2(\eta_3)=+1$, i.e., that $\beta_2\sqrt{p}>\alpha_3\sqrt{p}$, thus that $p \mid a+1$ (and consequently, that $q \mid a-1$). □

Consider the set of quadratic fields $K=\mathbb{Q}(\sqrt{m})$ in which at least one prime $q\equiv 3 \mod 4$ ramifies. We have $r\geq 2$, and when $r=2$, m is of one of the three types q, $2q$, or q_1q_2, those of Statements 1 to 3. When $r=3$, we have either $m=pq$, the case of Statements 4 and 5, or $m=pq_1q_2$. In this latter case, $p=2$ is not excluded.

Statement 6. *Let $K=\mathbb{Q}(\sqrt{m})$, $m=pq_1q_2$, where $p\equiv 1 \mod 4$ or $p=2$, and $q_1\equiv q_2\equiv 3 \mod 4$, with fundamental unit $\varepsilon=a+b\sqrt{m}$. Assume that $\left(\frac{p}{q_1}\right)=\left(\frac{p}{q_2}\right)=-1$. Then ε is odd, p divides $a-1$, and q_1 and q_2 divide $a+1$.*

For the proof we take $K_1=\mathbb{Q}(\sqrt{q_1q_2})$ and $K_2=\mathbb{Q}(\sqrt{p})$, so that $K=K_3$. Since p splits in $K_1/\mathbb{Q}$ and q_1 and q_2 are inert in $K_2/\mathbb{Q}$, we have $t=2$ in L/K_1 and L/K_2.

In L/K_2, $\pm\varepsilon_2$ are not norms (because $\mathrm{N}'_2(\varepsilon_2)=-1$), which implies first $[E_2 : E_2\cap \mathrm{N}_2(L^*)]\geq 2$, then $[E_2 : E_2\cap \mathrm{N}_2(L^*)]=2$, $h\equiv 1 \mod 2$ and $-1\in \mathrm{N}_2(E)$.

In L/K_1, since h and h_1 are odd, we have $[E_1 : E_1\cap \mathrm{N}_1(L^*)]=2$, and since $-1=\mathrm{N}_1(\varepsilon_2)\in \mathrm{N}_1(E)$, $\pm\varepsilon_1$ nor $\pm\varepsilon_1\varepsilon_3$ are squares. But since $-1\in \mathrm{N}_2(E)$, there exists a unit $\eta\in E$, $\notin \prod E_1$. We may take $\eta^2=\varepsilon_3$. This shows that ε_3 is odd. Then η is of the form $\alpha_3\sqrt{q_1q_2}+\beta_3\sqrt{p}$, and $\mathrm{N}_2(\eta)=-1$ implies $p\beta_3^2-q_1q_2\alpha_3^2<0$, hence $p \mid a-1$ and $q_1q_2 \mid a+1$. □

Statement 7. *Let $K=\mathbb{Q}(\sqrt{m})$, $m=pq_1q_2$, where $p\equiv 1 \mod 4$ or $p=2$, and $q_1\equiv q_2\equiv 3 \mod 4$, with fundamental unit $\varepsilon=a+b\sqrt{m}$. Assume that $\left(\frac{p}{q_2}\right)=-\left(\frac{p}{q_1}\right)$. Then ε is odd. Choosing q_1 such that $\left(\frac{p}{q_1}\right)=+1$, then pq_2 divides $a+\left(\frac{q_2}{q_1}\right)$ and q_1 divides $a-\left(\frac{q_2}{q_1}\right)$.*

We again take $K_1=\mathbb{Q}(\sqrt{q_1q_2})$ and $K_2=\mathbb{Q}(\sqrt{p})$, so that $K=K_3$. In a first step we do not choose which q_i satisfies $\left(\frac{p}{q_i}\right)=+1$. Since p is inert in $K_1/\mathbb{Q}$, we have $t=1$ in L/K_1, which implies $E_1=\mathrm{N}_1(E)$ and $h\equiv 1 \mod 2$. Since $\varepsilon_1\in \mathrm{N}_1(E)$ at least one of the units $\varepsilon_1, \varepsilon_1\varepsilon_3$ is a square in L. But $K_1(\sqrt{\varepsilon}_1)=\mathbb{Q}(\sqrt{q_1},\sqrt{q_2})$ is not contained in L. Hence we have $\varepsilon_1\varepsilon_3=\eta^2$ for some $\eta\in E$, and since ε_1 is odd and not a square in L, so is also ε_3. In $M:=\mathbb{Q}(\sqrt{p},\sqrt{q_1},\sqrt{q_2})$, we can extract square roots η_1 of ε_1 and η_3 of ε_3 (so that $\eta=\eta_1\eta_3$), of the form $\eta_1=\alpha_1\sqrt{q_1}+\beta_1\sqrt{q_2}$ and $\eta_3=\alpha_3\sqrt{pq_1}+\beta_3\sqrt{q_2}$ for some choice of

q_1 in $\{q_1, q_2\}$. Calculating $\mathrm{N}_2(\eta)$ amounts to negate one of the square roots of q_1, q_2 in M, say, of q_2.

In L/K_2, we have $t = 3$, hence $[E_2 : \mathrm{N}(E)] = 4$ (h and h_2 are odd), which implies that -1 is not a norm in L/K_2, hence that the contributions coming from η_1 and η_3 have the same sign. Statement 3 gives us the contribution of η_1, from which the result follows. □

To exhaust all possible cases with three ramified primes, at least one of which of type q, there remains to consider fields with $m = 2pq$. The decomposition $m = m_1 m_2$ associated with $K(\sqrt{\varepsilon})$ can be predicted for 6 out of the 8 values of $(\left(\frac{2}{p}\right), \left(\frac{2}{q}\right), \left(\frac{p}{q}\right)) \in (\pm 1, \pm 1, \pm 1)$ (just exclude $(+1, \pm 1, +1)$).

Concluding remarks.

(1) The structure of Cl_2 for quadratic fields suggests that real quadratic fields in which r primes including one $\equiv 3 \mod 4$ ramify behave like those having $r - 1$ ramified primes, all $\equiv 1 \mod 4$ (or 2). Though considering more than three ramified primes is possible, results on parity of units and distribution of primes among divisors of $a-1$ and $a+1$ then become complicated and it is then difficult to write down simple statements.

(2) The question of the parity of the unit does not appear when the prime 2 is highly ramified (i.e., $m \equiv 2 \mod 4$). Could one guess a more subtle invariant in this case?

References

Ambiguous classes: F. Lemmermeyer, J. Ramanujan Math. Soc. (2013), 415–421, = arXiv 4 Sep 2013.

Narrow ambiguous classes: G. Gras's thesis, Ann.Inst. Fourier **23** (1973,) no. 3 p. 1-48 & no. 4 p. 1-44.

Relative Stickelberger formula: J. Martinet, J. Th. Nombres Bordeaux **1** (1989), 197–204; *generalized* by G. Gras, *id.*, **22** (2010), 397–402.

Jacques Martinet,
Villa 30, Hameau de Noailles,
33400 Talence, France
Email address: Jacques.Martinet@math.cnrs.fr