SMALL NORMS IN QUADRATIC FIELDS

FRANZ LEMMERMEYER

1. Introduction

The computation of units in algebraic number fields usually is a rather hard task. Therefore, families of number fields with an explicitly given system of independent units have been of interest to mathematicians in connection with the computation of

- inhomogeneous minima of number fields;
- unramified extensions of number fields;
- capitulation of ideal classes therein;
- complete solution of Thue and index form equations, etc.

The first such number fields have been given by Richaud, namely the quadratic number fields of R-D-type (named after Richaud and Degert). These number fields have the form $k = \mathbb{Q}(\sqrt{m}\,)$, where $m = t^2 + r$, $|r| \le t$, $r|4t$. In [ACH] it was shown how to prove the class numbers of such fields to be strictly bigger than 1 by making use of a lemma due to Davenport. Hasse [H] has extended this result to other quadratic fields of R-D-type without being able to handle all cases. The most complete effort to this date is by Zhang [Zh2], who used a continued fraction approach (see [Zh] for sketches of some of the proofs). In this paper we intend to show how to prove Zhang's results using a geometric idea; this has the advantage that it can be generalized to a family of cubic (and possibly quartic) fields. For some history and an extensive list of references, see the forthcoming book of Mollin [M].

2. Quadratic Fields

In order to show how the proof works in a simple case, we first will look at quadratic fields $k = \mathbb{Q}(\sqrt{m}\,)$. Let $\varepsilon > 1$ be its fundamental unit; for $\alpha \in$ k we let α' denote the conjugate of α. In particular, we have $N\xi = \xi\xi'$, where $N = N_{k/\mathbb{Q}}$ denotes the absolute norm.

Now let $\xi \in$ k and a real positive number c be given; we can find a unit $\eta \in E_k$ such that

$$c \le |\,\xi\eta\,| < c\varepsilon. \tag{1}$$

Letting $n = |N\xi|$ we find $|\xi'\eta'| = n/|\xi\eta|$, so equation (1) yields

$$\frac{n}{c\varepsilon} \le |\,\xi'\eta'\,| < \frac{n}{c}. \tag{2}$$

Writing $\alpha = \xi\eta = a + b\sqrt{m}$ gives $|2a| = |\alpha + \alpha'| \le |\alpha| + |\alpha'| < c\varepsilon + \frac{n}{c}$, and correspondingly, $|2b\sqrt{m}\,| = |\alpha - \alpha'| \le |\alpha| + |\alpha'| < c\varepsilon + \frac{n}{c}$. Because we want the coefficients a and b to be as small as possible, we have to choose c in such a way that $c\varepsilon + n/c$ becomes a minimum. Putting $c = \sqrt{n/\varepsilon}$ we get

$$|2a| < 2\sqrt{n\varepsilon}, \quad |2b\sqrt{m}\,| < 2\sqrt{n\varepsilon}. \tag{3}$$

Making use of a lemma due to Cassels, we can improve these bounds:

Lemma 1. *Suppose that the positive real numbers x, y satisfy the inequalities $x \le s$, $y \le s$, and $xy \le t$. Then, $x + y \le s + t/s$.*

Proof. $0 \le (x-s)(y-s) = xy - s(x+y) + s^2 \le s^2 + t - s(x+y)$.

Putting $x = |\alpha|$ and $y = |\alpha'|$ in Lemma 1 we find

$$|2a| \le |\alpha| + |\alpha'| < \sqrt{n\varepsilon} + \sqrt{n/\varepsilon},$$

and likewise

$$|2b\sqrt{m}\,| < \sqrt{n\varepsilon} + \sqrt{n/\varepsilon}.$$

We have proved

Proposition 2. *Let $k = \mathbb{Q}(\sqrt{m}\,)$ be a real quadratic number field, $\varepsilon > 1$ a unit in k, and $0 \ne n = |N\xi\,|$ for $\xi \in k$. Then there is a unit $\eta = \varepsilon^j$ such that $\xi\eta = a + b\sqrt{m}$ and*

$$|a| < \frac{\sqrt{n}}{2}(\sqrt{\varepsilon} + 1/\sqrt{\varepsilon}\,), \qquad |b| < \frac{\sqrt{n}}{2\sqrt{m}}(\sqrt{\varepsilon} + 1/\sqrt{\varepsilon}\,).$$

Suppose that we are looking for a $\xi \in \mathbb{Z}[\sqrt{m}\,]$ with given norm $\pm n$. If we know a unit $\varepsilon > 1$, we can use Proposition 2 to find a power η of ε such that $\xi\eta = a + b\sqrt{m}$ has bounded integral coefficients a, b. Moreover, the bounds do not depend on ξ. In order to test if a given n is a norm in $k/\mathbb{Q}$, we therefore have to compute only the norms of a finite number of elements of k. Similar results are valid in case $\{1, \theta\}$ is an integral basis of the ring $\mathcal{O}_k$ of integers in k, where $\theta = \frac{1}{2}(1 + \sqrt{m}\,)$.

After these preparations, it is an easy matter to prove the following result originally due to Davenport:

Proposition 3. *Let m, n, t be natural numbers such that $m = t^2 + 1$; if the diophantine equation $|x^2 - my^2| = n$ has solutions in $\mathbb{Z}$ with $n < 2t$, then n is a perfect square.*

Proof. Let $\xi = x + y\sqrt{m}$; then $|\,N\xi\,| = n$, and since $\varepsilon = t + u\sqrt{m} > 1$ is a unit in $\mathbb{Z}[\sqrt{m}\,]$, we can find a power η of ε such that $\xi\eta = a + b\sqrt{m}$ has coefficients a, b which satisfy the bounds in Proposition 2.2. Since $2t < \varepsilon < 2\sqrt{m}$, we find

$$|b| \le \frac{\sqrt{n}}{2\sqrt{m}}\left(\sqrt{\varepsilon} + \frac{1}{\sqrt{\varepsilon}}\right) < 1 + \frac{1}{t}.$$

Since the assertion is trivial if $t = 1$, we may assume that $t \ge 2$, and now the last inequality gives $|b| \le 1$. If $b = 0, |N\xi| = a^2$ would be a square; therefore, $b = \pm 1$, and this yields $\alpha = \xi\eta = a \pm \sqrt{m}$. Now $|N\xi| = |N\alpha| = |a^2 - m|$ is minimal for values of a near $\sqrt{m}$, and we find

$$\begin{aligned} |a^2 - m| &= 2t \quad \text{if } a = t-1; \\ |a^2 - m| &= 1 \quad \text{if } a = t; \\ |a^2 - m| &= 2t \quad \text{if } a = t+1. \end{aligned}$$

This proves the claim.

Using the idea in the proof of Proposition 3 one can easily show more:

Proposition 4. *Let m, n, t be natural numbers such that $m = t^2 + 1$; if the diophantine equation $|x^2 - my^2| = n$ has solutions in $\mathbb{Z}$ with $n < 4t+3$, then $n = 4t-3$, $n = 2t$, or n is a perfect square.*

In [ACH], Proposition 3 was used to show that the ideal class group of $k = \mathbb{Q}(\sqrt{m}\,)$ has non-trivial elements (i.e. classes that do not belong to the genus class group) if $m = t^2 + 1$ and $t = 2lq$ for $l > 1$ and prime q: since $m \equiv 1 \bmod q$, q splits in k, i.e. we have $(q) = \mathfrak{p}\mathfrak{p}''$. If $\mathfrak{p}$ were principal, the equation $x^2 - my^2 = \pm 4q$ would have solutions in $\mathbb{Z}$; but since $4q < 2t = 4lq$ is no square, this contradicts Proposition 2.

If we consider the case $m = t^2 + 2$ instead of $m = t^2 + 1$, then the method used above does not seem to work: for example, the equation $x^2 - my^2 = -2$ is solvable (put $x = t, y = 1$) and 2 is no square. Therefore, we have to modify our proof in order to get non-trivial results.

Proposition 5. *Let m, n, t be natural numbers such that $m = t^2 + 2$ and $t \geq 12$; if the diophantine equation $|x^2 - my^2| = n$ has solutions in $\mathbb{Z}$ and if neither n nor $2n$ are perfect squares, then $n = 2t \pm 1, 4t - 7, 4t - 2$, or $n \geq 4t + 2$.*

Proof. Let $\xi = x + y\sqrt{m}, n = |N\xi|$, and suppose that neither n nor $2n$ are perfect squares. Letting $\delta = t + \sqrt{m}$, we find $\delta^2 = 2\varepsilon$, where ε is a unit in $\mathbb{Z}[\sqrt{m}\,]$. Obviously we can find a power η of ε such that

$$\sqrt{n\sqrt{\varepsilon}}/\varepsilon \leq |\xi\eta| < \sqrt{n\sqrt{\varepsilon}}.$$

Now we distinguish two cases:

1.: $\sqrt{n/\sqrt{\varepsilon}} \leq |\xi\eta| < \sqrt{n\sqrt{\varepsilon}}$: Writing $\xi\eta = a + b\sqrt{m}$, we find that $|b| \leq 1$. If $b = 0$, then b is a square, so assume $b = \pm 1$. Then the same reasoning as in Proposition 3 shows that either $n = 2$, i.e. $2n$ is a square, or that $n = 2t \pm 1, n = 4t - 2$ or $n \geq 4t + 2$.

2.: $\sqrt{n\sqrt{\varepsilon}}/\varepsilon \leq |\,\xi\eta\,| < \sqrt{n\sqrt{\varepsilon}}$: Multiplying $\xi\eta$ with δ we get

$$\sqrt{2n/\sqrt{\varepsilon}} \leq |\,\xi\eta\delta\,| < \sqrt{2n\sqrt{\varepsilon}}.$$

As in case 1. above, we find $|b| \leq 1$, where $\xi\eta\delta = a + b\sqrt{m}$; if $b = 0$, then $2n = |N(\xi\eta\delta)| = a^2$ is a square. If $b = \pm 1$, then $a^2 - mb^2$ must be even (because $|N\xi\delta|$ is even), or $|N\xi\delta| = 4t \pm 2, = 8t - 14$, or $\geq 8t + 14$ (because $12t - 34 \geq 8t + 14$ for all $t \geq 12$).

Exactly as after the proof of Proposition 3, we can deduce results about the ideal class group of $\mathbb{Q}(\sqrt{m}\,)$ from Proposition 5 if $m = t^2 + 2$. Moreover we remark that we have treated these two cases only to explain the method; similar results can be proved for other quadratic fields of R-D-type. As an example, we give the corresponding result for $m = t^2 - 2$:

Proposition 6. *Let m, n, t be natural numbers such that $m = t^2 - 2$ and $t \geq 12$; if the diophantine equation $N(\xi) = |x^2 - my^2| = n$ has solutions $\xi = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}\,]$, then either $\xi = n\eta$ for some $n \in \mathbb{Z}$ and some unit $\eta \in Z[\sqrt{m}\,]$, or $n = 2t \pm 3, 4t - 9, 4t \pm 6$, or $n \geq 4t + 6$, and ξ is associated to one of $\{t \pm 1 \pm \sqrt{m},\ t \pm 2 \pm \sqrt{m},\ 2t - 1 \pm 2\sqrt{m},\ 2t \pm 2 \pm 2\sqrt{m}\}$.*

References

[ACH] N. C. Ankeny, S. Chowla, H. Hasse, *On the class number of the real subfield of a cyclotomic field*, J. Reine Angew. Math. **217** (1965), 217–220 1, 3

[H] H. Hasse, *Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper*, El. Math. **20** (1965), 49–59 1

[M] R. Mollin, *Quadratics*, CRC 1

[Zh] Xian-ke Zhang, *Determination of solutions and solvabilities of diophantine equations and quadratic fields*, preprint 1

[Zh2] Xian-ke Zhang, *Solutions of the diophantine equations related to real quadratic fields*, Chin. Sci. Bull **37** (1992), 885–889 1

Bilkent University, Dept. Mathematics, 06800 Bilkent, Ankara
E-mail address: hb3@ix.urz.uni-heidelberg.de, franz@fen.bilkent.edu.tr