# Euclidean Number Fields 2

Hendrik W. Lenstra, Jr.*

## A Method of Hurwitz

The problem we considered in the previous section (this journal, vol. 2, pp. 6) may be immediately generalised to more general number fields. Let

$$g = X^n + q_{n-1}X^{n-1} + \ldots + q_1 X + q_0$$

be an irreducible polynomial with rational coefficients; let $\gamma$ be a zero of $g$, and let $K$ be the field generated by $\gamma$. Each element $\xi$ of $K$ is uniquely representable by an expression of the shape

$$(1) \quad p_0 + p_1\gamma + \ldots + p_{n-1}\gamma^{n-1},$$
$$p_0, p_1, \ldots, p_{n-1} \text{ rational.}$$

The *norm* $N(\xi)$ of $\xi$ is defined to be the absolute value of the product of the numbers (1) as $\gamma$ runs through the complex zeros of $g$. Obviously we have $N(\xi\eta) = N(\xi)N(\eta)$ for all $\xi$ and $\eta$ in $K$, and it can be shown that $N(\xi)$ is a rational number which is zero only if $\xi = 0$.

In $K$ we shall consider rings $R$ which, roughly speaking, are to be to $K$ as the ring of integers is to the field of rational numbers. More precisely, $R$ is to satisfy two conditions. Firstly, each element $\xi$ of $K$ must have some multiple $m\xi$ in $R$, where $m$ is a positive integer. Secondly, there should be elements $\theta_0, \theta_1, \ldots, \theta_{d-1}$ in $K$ such that an element $\xi$ in $K$ is in $R$ if and only if it can be expressed in the form

$$(2) \quad \xi = a_0\theta_0 + a_1\theta_1 + \ldots + a_{d-1}\theta_{d-1},$$
$$a_0, a_1, \ldots, a_{d-1} \text{ integers.}$$

It can be shown that if such $\theta_0, \ldots, \theta_{d-1}$ exist then they can be chosen so that $d = n$; if so, the representation (2) is unique. In order that $R$ be a ring the $\theta_i$ must have the property that all the products $\theta_i\theta_j$ are again of the shape (2). Moreover, we shall always suppose that 1 belongs to $R$.

We can readily find rings $R$ that satisfy the conditions just described. Suppose, for example, that the coefficients $q_i$ of $g$ are integers – this can always be arranged by replacing $\gamma$ by some multiple $m\gamma$ – then we may take $d = n$, $\theta_i = \gamma^i$. The elements of $R$ now look exactly like the numbers (1) of the previous section:

$$(3) \quad a_0 + a_1\gamma + \ldots + a_{n-1}\gamma^{n-1}$$
$$a_0, a_1, \ldots, a_{n-1} \text{ integers.}$$

It can be shown that the union $R_0$ of all rings that satisfy our conditions is itself a ring with those properties. The ring $R_0$ is called the ring of *algebraic integers* of $K$.

The ring $R$ is said to be *euclidean with respect to the norm*, or, more briefly, *norm-euclidean* if for every pair of elements $\alpha$ and $\beta$ of $R$, with $\beta \neq 0$, it is possible to find a quotient $\kappa$ and a remainder $\rho$, both belonging to $R$, so that

$$\alpha = \kappa\beta + \rho$$
$$N(\rho) < N(\beta).$$

Here we observe that $N(\beta)$ is always *an integer* if $\beta$ belongs to $R$. Indeed, if $\beta$ is in $R$, and is not zero, one can interpret $N(\beta)$ as the number of *residue classes* of $R$ modulo $\beta$. Here two elements $\rho$ and $\rho'$ of $R$ are said to be in the same residue class modulo $\beta$ if $\rho - \rho'$ is divisible in $R$ by $\beta$.

We call the field $K$ *euclidean* if $R_0$ is norm-euclidean. Actually it turns out that $R_0$ is the only $R$ that can be norm-euclidean.

The principal motive for this definition is the same as in the previous section:

(4) if $R$ is norm-euclidean then the theorem of unique factorisation into prime factors holds in $R$.

Once again this can be demonstrated by Euclid's arguments.

The case $n = 32$ of the previous section showed us that the converse does not hold. We get a simpler example by considering the numbers $a + b\sqrt{14}$ with $a$ and $b$ integers, or the numbers $\frac{1}{2}(a + b\sqrt{-19})$ with $a$ and $b$ integers and $a - b$ even.

How are we to decide whether $R$ is norm-euclidean? If we write $\xi = \alpha/\beta$ then the definition implies:

$R$ is norm-euclidean if and only if for each $\xi$ in $K$ we can find a $\kappa$ in $R$ such that $N(\xi - \kappa) < 1$.

* Translated by Alf van der Poorten.

We can use this to give a geometric formulation to the problem.

The polynomial $g$ has $n$ complex zeros, $r$ of which, say $\gamma_1, \ldots, \gamma_r$ are real. The remaining $n - r$ zeros can be arranged into $s$ complex conjugate pairs. Choose one zero from each pair, this gives $s$ additional zeros $\delta_1, \ldots, \delta_s$ and we have $r + 2s = n$. We embed the field $K$ in the $n$-dimensional real vector space $\mathbb{R}^r \times \mathbb{C}^s$ by mapping the expression $f(\gamma) = p_0 + p_1\gamma + \ldots + p_{n-1}\gamma^{n-1}$, as in (1), to

$$(f(\gamma_1), \ldots, f(\gamma_r), f(\delta_1), \ldots, f(\delta_s)).$$

Then $K$ is dense in $\mathbb{R}^r \times \mathbb{C}^s$. Now

$$N(f(\gamma)) = \left| \prod_{i=1}^{r} f(\gamma_i) \cdot \prod_{j=1}^{s} f(\delta_j) f(\bar{\delta}_j) \right|,$$

so we can extend the domain of definition of the norm $N$ to the whole space $\mathbb{R}^r \times \mathbb{C}^s$ by

$$N(x_1, \ldots, x_r, y_1, \ldots, y_s) = \left| \prod_{i=1}^{r} x_i \cdot \prod_{j=1}^{s} y_j \bar{y}_j \right|,$$

with the $x_i$ real and the $y_j$ complex.

The embedding in $\mathbb{R}^r \times \mathbb{C}^s$ makes $R$ a *lattice*; that is to say, there is a basis $\theta_0, \ldots, \theta_{n-1}$ of $\mathbb{R}^r \times \mathbb{C}^s$ over the reals so that the numbers in $R$ become exactly the vectors of the shape

(5) $a_0\theta_0 + a_1\theta_1 + \ldots + a_{n-1}\theta_{n-1}$,

$a_0, a_1, \ldots, a_{n-1}$ *integers.*

We see that:

(6) $R$ is norm-euclidean if each element $\xi$ of $\mathbb{R}^r \times \mathbb{C}^s$ can be expressed as the sum of an element $\kappa$ in $R$ and an element that belongs to the set

$$V = \{y : N(y) < 1\}.$$

In the case $r = 0, s = 1$ the set $V$ is an open disc with centre 0. If $r = 2, s = 0$ then $V$ is an unbounded set in the plane, bordered by hyperbolae. Generally $V$ is an open set containing 0 and is bounded only if $r + s = 1$. By virtue of (6) the question now is whether the translates

$$\kappa + V, \quad \kappa \text{ in } R$$

together cover the whole space. In order to see whether $\xi$ belongs to one of these translates it is plain that we may freely add elements of $R$ to $\xi$; seeing that these elements are of the shape (5) it follows that we need only consider those $\xi$ that lie in the parallelepiped

(7) $\{q_0\theta_0 + q_1\theta_1 + \ldots + q_{n-1}\theta_{n-1} : 0 \leqslant q_0 < 1,$
$0 \leqslant q_1 < 1, \ldots, 0 \leqslant q_{n-1} < 1\}.$

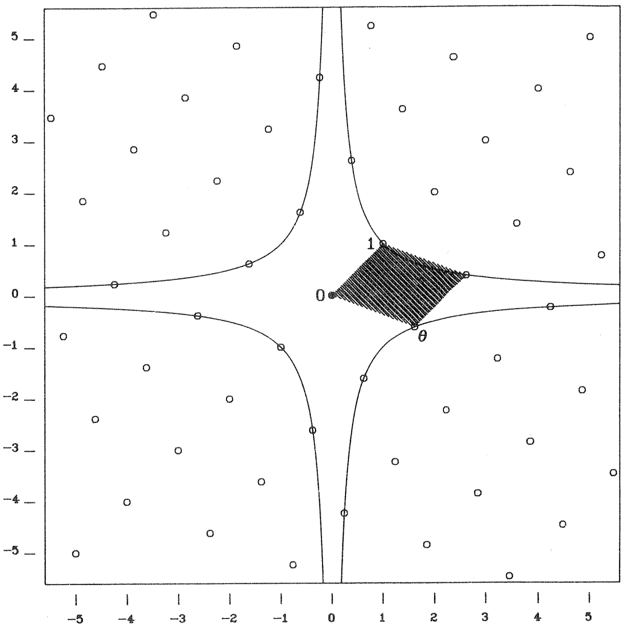

**Figure 1.** This illustration shows a portion of the ring $R = \{a + b\theta : a$ and $b$ integers$\}$, with $\theta^2 - \theta - 1 = 0$, embedded in $\mathbb{R} \times \mathbb{R}$ by mapping $a + b$ to $(a + b(1 + \sqrt{5})/2, a + b(1 - \sqrt{5})/2)$. The hyperbolae bound the region $V$ consisting of points of norm less than one. The elements of $R$ lying on the hyperbolae are the units of the ring. The shaded region is the parallelepiped (7). The small part of this parallelepiped not contained in $V$ is easily seen to be contained in $1 + V$. It follows from this that the ring $R$ is norm-euclidean.

This is a bounded set, and it is not difficult to see that *if* it is covered by some infinite set of translates $\kappa + V$, then it is already covered by some *finite* subset thereof.

Should we happen to succeed in covering the parallelepiped (7) then we would have proved more than is strictly necessary: to prove that $R$ is norm-euclidean we need consider only those vectors $\xi$ which lie in $K$; these correspond to *rational* $q_0, q_1, \ldots, q_{n-1}$ in (7). Were the converse of (6) to hold then the two questions would be equivalent; however, this converse has not been proved, nor is a counterexample known. One should compare this with an unproved conjecture of Barnes and Swinnerton-Dyer [1, p. 313].

If we assume the converse of (6) then the question whether $R$ is euclidean with respect to the norm is decidable. Indeed, let $\beta_1, \beta_2, \beta_3, \ldots$ be a list of all non-zero elements of $R$. Then one can check sequentially for $n = 1, 2, 3, \ldots$ whether the following conditions are or are not satisfied:

$I_n$: There is an $\alpha$ in $R$ such that $\alpha \not\equiv \rho \bmod \beta_n$ for all $\rho$ in $R$ with $N(\rho) < N(\beta_n)$;

$II_n$: The parallelepiped (7) is covered by the $n + 1$ translates $V, \beta_1 + V, \ldots, \beta_n + V$.

If one or other of the conditions is satisfied then stop: if $I_n$ holds then $R$ is not norm-euclidean, and if $II_n$ holds then $R$ is norm-euclidean. Suppose that this decision procedure fails to terminate. Then both $I_n$ and $II_n$ are false for all $n$, so $R$ is norm-euclidean though the translates $\kappa + V$ with $\kappa$ in $R$ fail to cover the space $\mathbb{R}^r \times \mathbb{C}^s$. This contradicts our assumption of the converse of (6). We add that it is decidable for any fixed $n$ whether $I_n$ and $II_n$ are satisfied.

It is indicative of the lack of general results in the theory that even the decidability of the question whether $R$ is norm-euclidean cannot be established unconditionally. The only thing in which the theory is rich is in examples, but even the most clearcut question concerning the extent of these riches:

> are there, up to isomorphism, infinitely many euclidean $K$?

remains unanswered. The most significant result of this nature is a theorem of Davenport, see [2], which states that, up to isomorphism, there are only finitely many euclidean fields with $r + s \leqslant 2$. His methods have been used to determine all euclidean $K$ with $n \leqslant 2$. Finally there is a finiteness theorem of Heilbronn which applies to certain classes of abelian fields, see [5].

Up to isomorphism, 334 different euclidean fields are known. The table below, derived from that in [7] and including new fields found by Cioffari, Leutbecher, Martinet, Mestre and myself, indicates the distribution of these fields relative to $n$ and $r + s$.

| $n$<br>$r + s$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | total |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 5 | | | | | | | | | 6 |
| 2 | | 16 | 52 | 34 | | | | | | | 102 |
| 3 | | | 57 | 11 | 12 | 28 | | | | | 108 |
| 4 | | | | 9 | 10 | 30 | 27 | 27 | | | 103 |
| 5 | | | | | 1 | 7 | 1 | 2 | 0 | 2 | 13 |
| 6 | | | | | | 2 | 0 | 0 | 0 | 0 | 2 |
| total | 1 | 21 | 109 | 54 | 23 | 67 | 28 | 29 | 0 | 2 | 334 |

For references to some of the immense volume of the literature on these matters see [7].

Quite diverse methods have been applied to determine these fields. For some elementary proofs in the quadratic case ($n = 2$) one should consult Hardy and Wright [4, § 14.7/8]. Most of the cubic examples ($n = 3$) have been found with the aid of electronic computers; the techniques used can be viewed as refinements of the decision procedure we sketched above.

We shall describe a method that harks back to an idea of Hurwitz. He bases a now unfashionable approach to ideal theory on the following variant of the euclidean division algorithm which is valid for all $K$ and $R$:

(8) there is an integer $m > 1$, so that for each $\xi$ in $K$ there is a $\kappa$ in $R$ and an integer $j$, $0 < j < m$, with

$$N(j\xi - \kappa) < 1.$$

Here $m$ is dependent on $R$. It is plain that $R$ is norm-euclidean if and only if we can take $m = 2$.

We shall sketch a proof of (8). Because the set $V$ is open we can choose a neighbourhood $U$ of 0 in $\mathbb{R}^r \times \mathbb{C}^s$ so that $U - U$ is contained in $V$; that is

$$(9) \quad N(u - u') < 1, \qquad \text{for all} \quad u, u' \text{ in } U.$$

Now let $\xi$ be an element of $K$ and consider all the translates

$$i\xi + U, \quad i = 1, 2, \ldots, m$$

of $U$, where $m$ is an integer greater than 1 which we fix later. We adjust each element of $i\xi + U$ by subtracting that element of $R$ which brings the adjusted number into the parallelepiped (7). This process yields a set, say $(i\xi + U)^*$, contained in (7), and of the same volume as $i\xi + U$. Were this not so then there would be two distinct points of $i\xi + U$ that are adjusted to the same point of (7), thus points that have their difference in $R$; but this is impossible because of (9).

If we note that $i\xi + U$ and $U$ plainly have the same volume then we can conclude that we have $m$ sets

$$(10) \quad (\xi + U)^*, (2\xi + U)^*, \ldots, (m\xi + U)^*$$

contained in (7), each with a volume equal to that of $U$. Suppose that we now choose $m$ so that $m$ times the volume of $U$ is larger than the, plainly finite, volume of the parallelepiped (7). This is a choice that does not depend on $\xi$. Then the sets (10) cannot be disjoint and thus there are integers $i$ and $i'$, $1 \leqslant i < i' \leqslant m$, elements $u$ and $u'$ of $U$, and $\lambda$, $\lambda'$ in $R$ so that

$$i\xi + u - \lambda = i'\xi + u' - \lambda'.$$

With $\kappa = \lambda' - \lambda$ and $j = i' - i$ we have

$$N(j\xi - \kappa) = N(i'\xi - \lambda' - i\xi + \lambda) = N(u - u') < 1,$$

and $j$ is an integer, $0 < j < m$. This proves Hurwitz's theorem.

In order to make this proof yield as small a value of $m$ as possible one must of course attempt to choose $U$ as large as possible. Even then one obtains the desired $m = 2$ only in a few cases. Much more can be achieved by making a small modification to Hurwitz's theorem. If, in place of the sets $\xi + U, 2\xi + U, \ldots, m\xi + U$, we were to consider the sets $\omega_1\xi + U, \omega_2\xi + U, \ldots, \omega_m\xi + U$ with $\omega_1, \omega_2, \ldots, \omega_m$ arbitrary elements of $K$, then in an entirely analogous way we would find that

(11) there is an integer $m > 1$, so that for all $\omega_1, \omega_2, \ldots, \omega_m$ and $\xi$ in $K$ there is a $\kappa$ in $R$ so that

(12) $N((\omega_i - \omega_j)\xi - \kappa) < 1 \qquad$ for some $i, j$, $1 \leqslant i < j \leqslant m$.

Suppose now that the $\omega_1, \omega_2, \ldots, \omega_m$ can be so chosen that all their differences $\omega_i - \omega_j$ $(i \neq j)$ are *units*, that is, they have an inverse in $R$. Then $N(\omega_i - \omega_j) = 1$, and (12) implies that

$$N(\xi - \kappa \cdot (\omega_i - \omega_j)^{-1}) < 1$$

Since $\kappa \cdot (\omega_i - \omega_j)^{-1}$ is an element of $R$ we conclude that $R$ is norm-euclidean. In other words

(13) if $R$ has *sufficiently* many elements all differences of which are units, then $R$ is euclidean with respect to the norm.

As an example we consider the field $K$ generated by a zero $\gamma$ of $g = X^5 - X^3 + X^2 - X - 1$, which has $r = 3$, $s = 1$; for $R$ we take the set of numbers (3). It turns out that if $U$ is well chosen in the above proof, then one can take $m = 5$. So $R$ is norm-euclidean if it is possible to find five elements with all their differences units. We assert that the five elements

$$0, 1, \gamma, \frac{1}{1-\gamma}, \frac{\gamma - 1}{\gamma}$$

will do for our purpose. It is quite easy to see that this is equivalent to the claim that all three of the elements $\gamma$, $\gamma - 1$ and $\gamma^2 - \gamma + 1$ are units. But from

$$\gamma^5 - \gamma^3 + \gamma^2 - \gamma - 1 = g(\gamma) = 0$$

it follows that

$$\gamma \cdot (\gamma^4 - \gamma^2 + \gamma - 1) = 1$$
$$(\gamma - 1) \cdot (\gamma^4 + \gamma^3 + \gamma) = 1$$
$$(\gamma^2 - \gamma + 1) \cdot (\gamma^3 + \gamma^2 - \gamma - 1) = \gamma.$$

We conclude that $K$ is euclidean.

For further examples we refer the reader to [7]. The present method also allows us to deal with a number of the rings mentioned in the previous section.

Hurwitz's theorem can also be used to prove a charming result of O'Meara [9]:

(14) there is a non-zero element $\delta$ in $R$, so that the ring $T = R[\delta^{-1}]$, generated by $R$ and the inverse of $\delta$, is euclidean with respect to the function $N_T$ defined by

$N_T(0) = 0$

$N_T(\beta)$ = number of residue classes of $T$ modulo $\beta$,

$\beta$ in $T$, $\beta \neq 0$.

Here we say that $T$ is euclidean with respect to $N_T$ if for all $\alpha$ and $\beta$ in $T$, $\beta \neq 0$, one can find $\kappa$ and $\rho$ in $T$ so that $\alpha = \kappa\beta + \rho$ and $N_T(\rho) < N_T(\beta)$. It turns out that to prove O'Meara's theorem it is sufficient to take $\delta$ as the product of all the numbers $\omega_i - \omega_j$, $1 \leqslant i < j \leqslant m$, with $m$ as above and $\omega_1, \omega_2, \ldots, \omega_m$ arbitrary distinct elements of $R$.

Actually, it is much easier to find a $\delta$ so that the unique factorisation theorem holds in $R[\delta^{-1}]$. In the case $R = R_0$ one can even choose $\delta$ to be relatively prime to any arbitrarily nominated $\epsilon$ in $R$; that is, so that $\lambda\delta + \mu\epsilon = 1$ for

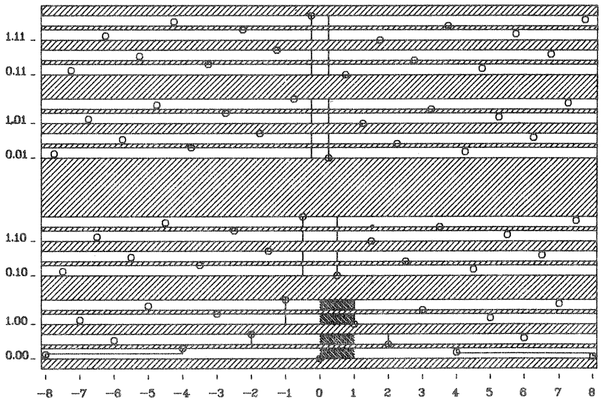

**Figure 2.** The analogue of figure 1 for the ring $T = \mathbb{Z}[\frac{1}{2}] = \{a/b$: $a$ and $b$ are integers, and $b$ is a power of $2\}$. The shaded strips are background, and do not belong to the picture. Projection on the horizontal axis yields the obvious inclusion of $\mathbb{Z}[\frac{1}{2}]$ into $\mathbb{R}$. Projection on the vertical axis yields the inclusion of $\mathbb{Z}[\frac{1}{2}]$ into the field of 2-adic numbers. This field has been embedded topologically in $\mathbb{R}$ by a method which we leave to the reader to find out; the numbers along the vertical axis have been written in binary notation. The set $V$ of elements of norm less than 1 is now bounded by "piecewise linear" hyperbolae. The elements of $\mathbb{Z}[\frac{1}{2}]$ lying on these hyperbolae are exactly the units of the ring: $\pm 1$, $\pm 2^{\pm 1}$, $\pm 2^{\pm 2}, \ldots$ . The shaded region corresponds to the parallelepiped (7). It is contained in $V$, confirming that $\mathbb{Z}[\frac{1}{2}]$ is euclidean with respect to $N_T$.

some $\lambda$, $\mu$ in $R$. Whether one has the same freedom of choice in (14) is an unsolved problem.

The rings $T = R[\delta^{-1}]$, with $\delta$ in $R$, $\delta$ non-zero, have properties which in many respects are analogous to those of the ring $R$ itself. Much of what we have said in this section can, with some modifications, also be said of the rings $T$. Then $p$-adic fields take their place next to that of $\mathbb{R}$ and $\mathbb{C}$, as can be seen in figure 2. In any event, O'Meara's theorem shows that in this wider class of rings there is no lack of examples of euclidean rings. We refer to [8] for the proper generalisation of the theorem of Davenport that we mentioned above.

*The author is indebted to A. K. Lenstra for preparing the drawings.*

### References to § 2

1. E. S. Barnes, H. P. F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms (II), *Acta Math.* 88 (1952), 279–316
2. J. W. S. Cassels, The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms, *Proc. Cambridge Philos. Soc.* 48 (1952), 72–86, 519–520
3. H. J. Godwin, Computations relating to cubic fields, pp. 225–229, in: A. O. L. Atkin, B. J. Birch (eds), *Computers in number theory*, Academic Press, London 1971
4. G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, fourth edition, Oxford University Press, Oxford 1960
5. H. Heilbronn, On Euclid's algorithm in cyclic fields, *Canad. J. Math.* 3 (1951), 257–268
6. A. Hurwitz, *Mathematische Werke*, Zweiter Band, Birkhäuser, Basel 1933
7. H. W. Lenstra, Jr., Euclidean number fields of large degree, *Invent. Math.* 38 (1977), 237–254
8. H. W. Lenstra, Jr., Euclidean ideal classes, Journées Arithmétiques de Luminy, *Astérisque* 61 (1979), 121–131
9. O. T. O'Meara, On the finite generation of linear groups over Hasse domains, *J. Reine Angew. Math.* 217 (1965), 79–108

*H. W. Lenstra, Jr.*
*Mathematisch Instituut*
*Universiteit van Amsterdam*
*Roetersstraat 15*
*1018 WB Amsterdam*
*Netherlands*

*A. J. van der Poorten*
*School of Mathematics and Physics*
*Macquarie University*
*North Ryde*
*NSW 2113 Australia*