Astérisque

H. W. JUN. LENSTRA

Euclidean ideal classes

Astérisque, tome 61 (1979), p. 121-131

<http://www.numdam.org/item?id=AST_1979__61__121_0>

Société Mathématique de France
Astérisque 61 (1979) p. 121-131

EUCLIDEAN IDEAL CLASSES

par

H.W. Lenstra, jr

Introduction

A classical method, due to Euclid, Stevin and Gauss, to establish that a given commutative ring R is a principal ideal ring consists in showing that R is Euclidean, i.e. that there exists a map φ from $R - \{0\}$ to a well-ordered set, usually $\mathbb{N} = \{0, 1, 2, \ldots\}$, such that for all $a, b \in R$, $b \neq 0$, $a \notin Rb$, there exist $q, r \in R$ such that $a = qb + r$ and $\varphi(r) < \varphi(b)$. Such a map φ is said to be a Euclidean algorithm on R, and R is called Euclidean with respect to φ.

A case of special interest in number theory is the following. Let K be a global field, i.e. a finite extension of $\mathbb{Q}$ or a function field in one variable over a finite field $\mathbb{F}_q$. Denote by P the set of all non-trivial prime divisors of K, and let $S \subset P$ be a finite non-empty subset containing the set S_∞ of archimedean prime divisors of K. For R we take the ring of S-integers in K:

$$R = \{x \in K: |x|_{\underline{p}} \leq 1 \text{ for all } \underline{p} \in P - S\},$$

where $|\ |_{\underline{p}}$, for $\underline{p} \in P$, denotes an absolute value of K corresponding to $\underline{p}$. For $x \in R - \{0\}$, the norm $N(x)$ is the cardinality of the finite ring R/Rx. One is interested in conditions under which the norm N is a Euclidean algorithm on R. Most of the literature on the subject (see [8] for references) restricts to the case that K is a number field, and $S = S_\infty$. Then R is the ring of algebraic integers in K, and N is the absolute value of the field norm $K \to \mathbb{Q}$ (restricted to $R - \{0\}$).

Let the norm N be extended to K by multiplicativity and $N(0) = 0$. Then it is easily seen that N is a Euclidean algorithm on R if and only if

(0.1) for all $x \in K$ there exists $y \in R$ such that $N(x-y) < 1$.

In this paper we investigate a similar property in which the role of the ring R is played by a fractional ideal $\underline{c}$ of R. If $\underline{a} \subset R$ is a non-zero ideal, we define $N(\underline{a})$ to be the cardinality of $R/\underline{a}$, and we extend the definition of $N(\underline{a})$ to fractional ideals by multiplicativity. We are interested in the following property of a fractional ideal $\underline{c}$:

(0.2) for all $x \in K$ there exists $y \in \underline{c}$ such that $N(x-y) < N(\underline{c})$.

For $\underline{c} = R$ this clearly reduces to (0.1). If $\underline{c}$ is principal, $\underline{c} = Rc$, then $N(\underline{c}) = N(c)$ and dividing by c we see that (0.2) and (0.1) are equivalent. Generally, this argument shows that whether or not (0.2) is satisfied only depends on the ideal class $[\underline{c}]$ of $\underline{c}$. If it is satisfied, we say that the ideal class $[\underline{c}]$ is Euclidean for the norm or norm-Euclidean. So the principal ideal class is Euclidean for the norm if and only if N is a Euclidean algorithm on R.

Here is an example of a non-principal Euclidean ideal class. Let $K = \mathbb{Q}(\sqrt{-5})$, $R = \mathbb{Z}[\sqrt{-5}]$ (so $S = S_\infty$) and $\underline{c} = (2, 1 + \sqrt{-5})$. Then $N(\underline{c}) = 2$, and $N(x) = |x|^2$ for $x \in K$ if K is considered as a subfield of $\mathbb{C}$. Drawing a picture (cf. [2]) one finds that

for all $x \in \mathbb{C}$ there exists $y \in \underline{c}$ such that $|x-y| < \sqrt{2}$,

so (0.2) holds. But (0.1) doesn't, because R is no principal ideal ring.

The main result about Euclidean ideal classes is the following theorem.

(0.3) Theorem The ring R has at most one ideal class which is Euclidean for the norm. If there is one, then it generates the ideal class group of R.

In particular, if the principal ideal class is Euclidean, then the class group is trivial and R is a principal ideal ring, as we knew already.

A generalization of theorem (0.3), in an algebraic setting, is proved in section 1. By means of examples we show that the class number can be arbitrarily

large.

Section 2 is devoted to the arithmetic rings discussed above. We shall see in this section that the ring of integers of a quadratic number field K has a non-principal norm-Euclidean ideal class if and only if the discriminant of K over $\mathbb{Q}$ is one of

$$-20, -15, 40, 60, 85,$$

see (2.1) and (2.5). In all five cases, the class number is two (cf. (1.8)).

1. Elementary properties

In this section R is a domain, i.e. a commutative ring, without zero-divisors, with a unit element different from zero. The group of units of R is denoted by R^*, and K denotes its field of fractions. An ideal class of R is a set of the form $\{\underline{d}a: a \in K^*\}$ where $\underline{d} \subset R$ is a non-zero ideal and $\underline{d}a = \{xa: x \in \underline{d}\}$. An element of an ideal class is called a fractional ideal of R. The unique ideal class containing a given fractional ideal $\underline{a}$ is denoted by $[\underline{a}]$. Fractional ideals are multiplied in the usual way, and ideal classes are multiplied by $[\underline{a}].[\underline{b}] = [\underline{a}.\underline{b}]$. If the set $Cl(R)$ of ideal classes of R is a group with respect to this multiplication, then R is called a Dedekind domain, $Cl(R)$ its class group, and the order of $Cl(R)$ its class number. We put

$$E = \{\underline{b}: \underline{b} \text{ is a fractional ideal of } R, \text{ and } \underline{b} \supset R\}.$$

(1.1) Definition Let W be a well-ordered set, $\psi: E \to W$ a map, C an ideal class of R, and $\underline{c} \in C$. We say that ψ is a Euclidean algorithm for C, or that C is Euclidean with respect to ψ, if

(1.2) for all $\underline{b} \in E$ and all $x \in \underline{b}.\underline{c} - \underline{c}$ there exists $z \in x + \underline{c}$ such that $\psi(\underline{b}cz^{-1}) < \psi(\underline{b})$.

We call C Euclidean if there exists a Euclidean algorithm for C.

It is readily verified that the definition does not depend on the choice of

$\underline{c}$ in C, and that, in the given circumstances, we have $z \neq 0$ and $\underline{bc}z^{-1} \in E$.

In the arithmetic case discussed in the introduction we take $\psi(\underline{b}) = N(\underline{b})^{-1}$. The inequality in (1.2) then simplifies to $N(z) < N(\underline{c})$. Using that $\bigcup_{\underline{b} \in E} \underline{bc} = K$, and writing $z = x - y$, we then find that (1.2) is equivalent to (0.2). So C is Euclidean with respect to ψ if and only if it is Euclidean for the norm.

(1.3) Exercise Show that a domain R is Euclidean if and only if the principal ideal class $[R]$ is Euclidean.

In the sequel we suppose that $C = [\underline{c}]$ satisfies the condition

$$\{x \in K: x\underline{c} \subset \underline{c}\} = R. \tag{1.4}$$

This condition is satisfied if $\underline{c}$ is invertible, e.g. if R is Dedekind. If (1.4) does not hold, then in our conclusions R should be replaced by the ring $\{x \in K: x\underline{c} \subset \underline{c}\}$.

In the following lemma we assume that W contains $\mathbb{N}$ as a beginning segment.

(1.5) Lemma Let C satisfy (1.4) and be Euclidean with respect to ψ. Then for every $\underline{b} \in E$, $\underline{b} \neq R$, there exists $n \in \mathbb{N}$ such that

$$[\underline{b}.\underline{c}^n] = [R], \quad 0 < n \leq \psi(\underline{b}).$$

Proof by induction on $\psi(\underline{b})$. From $\underline{b} \neq R$ and (1.4) we find that there exists an element $x \in \underline{bc} - \underline{c}$, and (1.2) then gives us $\underline{a} = \underline{bc}z^{-1} \in E$ with $\psi(\underline{a}) < \psi(\underline{b})$. If $\underline{a} = R$, then $[\underline{bc}] = [R]$ and we can take $n = 1$. If $\underline{a} \neq R$, then by the induction hypothesis $[\underline{ac}^m] = [R]$ for some $m \leq \psi(\underline{a})$, and we can take $n = m + 1$. This proves (1.5).

(1.6) Theorem Let R be a domain, and C a Euclidean ideal class of R satisfying (1.4). Then R is a Dedekind domain with a finite cyclic class group, generated by C.

Proof We may clearly assume that $R \neq K$. Then $Cl(R) = \{[\underline{b}]: \underline{b} \in E, \underline{b} \neq R\}$, so (1.5) shows that every ideal class has an inverse $[\underline{c}^n]$. Therefore R is Dedekind, and $Cl(R) = \{[\underline{c}]^{-n}: n = 1, 2, 3, \ldots\}$. In particular $[R] = [\underline{c}]^{-n}$

for some $n > 0$, so $[\underline{c}]$ has finite order. This proves (1.6).

(1.7) Exercise Let $a \in R - R^*$, $a \neq 0$. Prove that $\#Cl(R) \leq \psi(Ra^{-1})$.

Suppose $\underline{b} \in E$, $\underline{b} \neq R$ is such that $\psi(\underline{b})$ is smallest possible. Then the ideal $\underline{a}$ in the proof of (1.5) must be equal to R, so $n = 1$ and $C = [\underline{b}]^{-1}$. Hence there is at most one ideal class, satisfying (1.4), which is Euclidean with respect to a given ψ. This remark, and theorem (1.6), prove theorem (0.3).

(1.8) Exercise Let K be a Galois extension of degree n of $\mathbb{Q}$, and suppose that its ring of integers has a norm-Euclidean ideal class. Prove that the class number of K divides n.

Many results known about Euclidean rings (cf. [13]) have immediate generalizations for rings possessing a Euclidean ideal class. We list some of them as exercises. Assume, for (1.9) - (1.14), that C satisfies (1.4) and is Euclidean with respect to ψ.

(1.9) Exercise Let $\underline{a}, \underline{b} \in E$. Prove that $\psi(\underline{ab}) \geq \psi(\underline{b})$, with equality if and only if $\underline{a} = R$.

(1.10) Exercise Let $R' \subset K$ be a subring containing R. Prove that R' has a Euclidean ideal class. Prove that R' is Euclidean if and only if R' is a principal ideal domain. Deduce that $\mathbb{Z}[\sqrt{-5}, 1/3]$ is Euclidean (cf. [15]).

In the following exercises we put

(1.11) $$\theta(\underline{b}) = \min\{\psi(\underline{b}): \psi: E \to W \text{ is a Euclidean algorithm for } C\}$$

where W is the set of ordinals of cardinality $\leq \#E$. This map is called the smallest Euclidean algorithm for C; the terminology is easily justified.

(1.12) Exercise Prove that $\theta(\underline{ab}) \geq \theta(\underline{a}) + \theta(\underline{b})$ for $\underline{a}, \underline{b} \in E$.

(1.13) Exercise Let $\underline{b} \in E$ be such that $\theta(\underline{b})$ is finite. Prove that $\underline{b} \in C^{-\theta(\underline{b})}$.

(1.14) Exercise Prove that $\theta(\underline{b}) = 1$ if and only if $\underline{b}^{-1} = \underline{p}$ is a maximal ideal of R such that $\underline{p} \in C$ and the natural map $R^* \to (R/\underline{p})^*$ is surjective.

(1.15) Example Let k be a field, $K = k(t)$ a simple transcendental extension of k, and $f \in k[t]$ an irreducible polynomial. Denote by h the degree of f. Put

$$R = \{a/b \in K: a, b \in k[t], \ b \text{ is a power of } f, \ \deg a \leq \deg b\},$$

$$\underline{c} = \{a/b \in R: \deg a < \deg b\}.$$

Then R is a ring, and $\underline{c}$ is an invertible R-ideal, satisfying (1.4). For a non-zero ideal $\underline{a} \subset R$, put $d(\underline{a}) = \dim_k R/\underline{a}$, and extend the definition to all fractional ideals by $d(\underline{a}\underline{a}^{-1}) = d(\underline{a}) - d(Ra)$. Then $d(\underline{c}) = 1$, and more generally $d(\underline{a}\underline{c}) = d(\underline{a}) + 1$ for all $\underline{a}$; this follows from the invertibility of $\underline{c}$. An easy calculation gives

$$d(Rx) = -\mathrm{ord}_f(x).h \quad \text{for} \quad x \in K^*,$$

where ord_f is the normalized exponential valuation of K corresponding to f.

We claim that $C = [\underline{c}]$ is Euclidean with respect to the map $\psi: E \to \mathbb{N}$ defined by $\psi(\underline{b}) = -d(\underline{b})$. This assertion is equivalent to

for all $x \in K$ there exists $y \in \underline{c}$ such that $d(R(x-y)) < d(\underline{c})$

(cf. (0.2)). To prove it, use the partial fraction expansion of x to write $x = (c/f^n) + z$, with $n \in \mathbb{N}$, $c \in k[t]$, $\deg c < \deg f^n$, $z \in K$, $\mathrm{ord}_f(z) \geq 0$, and choose $y = c/f^n$. Then $d(R(x-y)) = d(Rz) = -\mathrm{ord}_f(z).h \leq 0 < 1 = d(\underline{c})$, as required.

We conclude that R is Dedekind, and that $\mathrm{Cl}(R)$ is generated by C. We calculate the class number. If $\underline{c}^n = Rx$, then $n = d(\underline{c})^n = d(Rx) = -\mathrm{ord}_f(x).h$ so n is divisible by h. Also $\underline{c}^h = Rf^{-1}$, so the class number equals h.

Thus we see that every positive integer occurs as the class number of a ring having a Euclidean ideal class.

If we take $k = \mathbb{F}_q$, then R is of the arithmetic type described in the introduction, and $N(x) = q^{d(x)}$. Hence, in our example, C is also Euclidean for the norm.

2. Arithmetic rings

In this section we let the notations be as in the introduction. In particular, K is a global field, and R is its ring of S-integers.

In the case $\#S = 1$ all examples of Euclidean ideal classes are easily determined.

(2.1) Proposition Let $\#S = 1$, and let C be an ideal class of R. Then C is Euclidean if and only if C is Euclidean for the norm, and if and only if

(a) R is the ring of integers in one of the fields

$$\mathbb{Q},\ \mathbb{Q}(\sqrt{-d}),\ d = 3,\ 4,\ 7,\ 8,\ 11,\ 15,\ \text{or}\ 20$$

and C is the unique generator of $Cl(R)$;

or (b) R is one of the rings described in (1.15), with k finite and $C = [\underline{c}]$.

The proof is similar to the proof in the classical case (cf. [7, sec. 10]). There is an analogous result for function fields over infinite fields of constants.

The class numbers of the rings in (a) are 1, 1, 1, 1, 1, 1, 2, 2, respectively.

(2.2) Proposition Suppose that $\#S \geq 2$, and if K is a number field, assume that for every squarefree integer n the ζ-function of the field $K(\zeta_n, R^{*1/n})$, with ζ_n denoting a primitive n-th root of unity, satisfies the generalized Riemann hypothesis. Then every ideal class C which generates the ideal class group of R is Euclidean.

This proposition generalizes the theorem of Weinberger and Queen in the classical case [16, 12]. The proof of (2.2) uses the methods of [9]. It also yields an explicit description of the map θ defined by (1.11); in most, but not all, cases it is the smallest function having the properties indicated in exercises (1.12), (1.13) and (1.14).

In the rest of this section we are exclusively interested in ideal classes which are Euclidean for the norm.

Let K_S denote the locally compact topological ring

$$K_S = \prod_{\underline{p} \in S} K_{\underline{p}},$$

where $K_{\underline{p}}$ is the $\underline{p}$-adic completion of K. We regard K as being embedded in K_S along the diagonal. Then K is dense in K_S, and every fractional ideal $\underline{a}$ of R is discrete in K_S, with $K_S/\underline{a}$ compact. The norm is extended to a map $N: K_S \to \mathbb{R}_{\geq 0}$ by

$$N(x) = \prod_{\underline{p} \in S} |x_{\underline{p}}|_{\underline{p}}, \quad \text{for} \quad x = (x_{\underline{p}})_{\underline{p} \in S} \in K_S,$$

where the $|\ |_{\underline{p}}$ are normalized in the usual way which makes the formula valid for $x \in K$. For $t \in \mathbb{R}_{>0}$, put

$$V_t = \{z \in K_S : N(z) < t\}.$$

This is an open neighborhood of 0 in K_S. Clearly, the ideal class $C = [\underline{c}]$ is Euclidean for the norm if and only if

$$K \subset \underline{c} + V_{N(\underline{c})} = \{x + y : x \in \underline{c},\ y \in V_{N(\underline{c})}\}.$$

It seems that in all cases in which this condition is known to be satisfied we actually have

$$K_S = \underline{c} + V_{N(\underline{c})}.$$

It is unknown whether both properties are in fact equivalent. The only known result in this direction is:

(2.3) Proposition Suppose that $\#S \leq 2$, and $t \in \mathbb{R}_{>0}$. Then $K \subset \underline{c} + V_t$ implies that $K_S = \underline{c} + V_{t+\varepsilon}$ for every $\varepsilon \in \mathbb{R}_{>0}$; if $\#S = 1$ or K is a function field this is also true for $\varepsilon = 0$.

For the proof, cf. [1, theorem M].

In the case $\#S = 2$, $S = S_\infty$, Davenport [4, nrs 70, 76, 82] proved that only finitely many R, up to isomorphism, are Euclidean with respect to the norm. This result can be generalized as follows.

(2.4) Proposition Suppose that $\#S = 2$. Then R has an ideal class which is

Euclidean for the norm if and only if

(a) K is one of $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-d})$, $d = 3, 4, 7, 8, 11, 15, 20$;

or (b) R belongs, up to isomorphism, to a certain finite list of number rings;

or (c) K is a function field of genus zero.

The proof makes use of (2.3) and of ideas of Cassels [3].

The finite list mentioned under (b) is not completely known. It contains at least 107 rings, as we shall see below. We distinguish four cases.

(2.5) $S = S_\infty$, K is real quadratic, and R its ring of integers. This case is completely settled. The principal ideal class is norm-Euclidean if and only if the discriminant of K over $\mathbb{Q}$ has one of the following sixteen values:

$$5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73, 76,$$

cf. [4, nr 74]. By similar methods one can show that there is a non-principal norm-Euclidean ideal class if and only if the discriminant is one of

$$40, 60, 85.$$

In these three cases, the class number is two.

(2.6) $S = S_\infty$, K is complex cubic, and R its ring of integers. If R has a norm-Euclidean ideal class then $-\Delta < 170523$ and $h \leq 4$, where Δ denotes the discriminant of K over $\mathbb{Q}$ and h the class number. The fifty-two known examples all have class number one [14]. It would be of interest to find examples with larger class numbers in this category.

(2.7) $S = S_\infty$, K is totally complex quartic, and R its ring of integers. Here we may restrict attention to fields with $\Delta < 20{,}435{,}007$ and $h \leq 6$. There are thirty-two known K's with $[R]$ norm-Euclidean, see [8] for references. The only other known example in this category is $K = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$: it has class number two, and the non-principal ideal class is Euclidean for the norm.

(2.8) $S = S_\infty \cup \{\underline{p}\}$, K is a complex quadratic field not mentioned in (2.4)(a), and $\underline{p}$ is a non-archimedean prime of K. The three rings

$$R = \mathbb{Z}[\sqrt{-19}, 1/2],\ \mathbb{Z}[\sqrt{-6}, 1/2],\ \mathbb{Z}[\sqrt{-6}, 1/(1+4\sqrt{-6})]$$

are Euclidean with respect to the norm; the last two are due to G. Cooke (unpublished). Other examples of norm-Euclidean ideal classes are not known in this category, but should not be hard to find. It seems an attractive problem to determine them all. It can be shown that they all have $h \leq 2$.

For higher values of $\#S$ no result comparable to (2.4) is known.

We finish with three unsolved problems.

(2.9) Problem A theorem of O'Meara [11] states that for any global field K there exists a finite subset $S \subset P$, $S \neq \emptyset$, $S \supset S_\infty$, such that the ring R of S-integers is Euclidean with respect to the norm. Can one take S to satisfy $S \cap T = \emptyset$, where T is a given finite subset of P with $S_\infty \cap T = \emptyset$?

(2.10) Problem Do there, in the case $S = S_\infty$, exist infinitely many non-isomorphic rings R with a norm-Euclidean ideal class? See [8, 10] for 312 examples with class number one, and (2.1), (2.5), (2.7) for six examples with class number two.

(2.11) Problem Heilbronn [5, 6] has shown that in certain classes of cyclic number fields there are only finitely many whose ring of integers is Euclidean with respect to the norm. Do his results carry over to rings with a norm-Euclidean ideal class?

Acknowledgement

Research for this paper was supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

References

1. E.S. BARNES, H.P.F. SWINNERTON-DYER, The inhomogeneous minima of binary

quadratic forms (II), Acta Math. 88 (1952),279-316.

2. E. CAHEN, Sur une note de M. Fontené relative aux entiers algébriques de la forme $x + y\sqrt{-5}$, Nouv. Ann. Math. (4) 3 (1903), 444-447.
3. 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.
4. The collected works of HAROLD DAVENPORT, vol. I, Academic Press, London 1977.
5. H. HEILBRONN, On Euclid's algorithm in cubic self-conjugate fields, Proc. Cambridge Philos. Soc. 46 (1950), 377-382.
6. H. HEILBRONN, On Euclid's algorithm in cyclic fields, Canad. J. Math. 3 (1951), 257-268.
7. H.W. LENSTRA, Jr., Lectures on Euclidean rings, Bielefeld 1974.
8. H.W. LENSTRA, Jr., Euclidean number fields of large degree, Invent. Math. 38 (1977), 237-254.
9. H.W. LENSTRA, Jr., On Artin's conjecture and Euclid's algorithm in global fields, Invent. Math. 42 (1977),201-224.
10. H.W. LENSTRA, Jr., Quelques exemples d'anneaux euclidiens, C. R. Acad. Sci. Paris 286 (1978), 683-685.
11. O.T. O'MEARA, On the finite generation of linear groups over Hasse domains, J. Reine Angew. Math. 217 (1965), 79-108.
12. C.S. QUEEN, Arithmetic Euclidean rings, Acta Arith. 26 (1974), 105-113.
13. P. SAMUEL, About Euclidean rings, J. Algebra 19 (1971), 282-301.
14. E.M. TAYLOR, Euclid's algorithm in cubic fields with complex conjugates, J. London Math. Soc. 14 (1976), 49-54.
15. J.H.M. WEDDERBURN, Non-commutative domains of integrity, J. Reine Angew. Math. 167 (1932), 129-141.
16. P.J. WEINBERGER, On Euclidean rings of algebraic integers, Proc. Symp. Pure Math. 24 (Analytic number theory), 321-332, Amer. Math. Soc. 1973.

Permanent adress

Mathematical Institut
Roetersstraat 15
1018 WB AMSTERDAM
Netherlands

Hendrik Lenstra
Institut des Hautes Études Scientifiques
35, route de Chartres
91440 Bures-sur-Yvette.