Euclidean ideal classes

H.W. LENSTRA, Jr.

Institut des Hautes Etudes Scientifiques
35, rt. de Chartres
91440 - Bures-sur-Yvette (France)

June 1978

IHES/M/78/230

Euclidean ideal classes

H.W. LENSTRA, Jr.

Introduction.

A classical method 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 W 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.

In this paper we consider a variant of this concept, which leads, not to principal ideal rings, but to Dedekind rings with finite cyclic class groups.

We first discuss a special case. Let K be an algebraic number field of finite degree over the field $\mathbb{Q}$ of rational numbers, denote by R the ring of algebraic integers in K, and let the norm $N : R \to \mathbb{N} = \{0,1,2,\ldots\}$ be defined by

$$N(x) = \#(R/Rx) \qquad (x \neq 0),$$

$$N(0) = 0,$$

where $\# S$ denotes the cardinality of S. By multiplicativity, we extend the norm to a function $K \to \mathbb{Q}_{\geq 0}$, which is again denoted by N. It is well known and easy to prove that N, restricted to $R - \{0\}$, is a Euclidean algorithm on R if and only if

(0.1) $\forall x \in K : \exists y \in R : N(x-y) < 1$.

Let $\underline{c}$ be a fractional ideal of R , and consider the following property of $\underline{c}$:

(0.2) $\forall x \in K : \exists y \in \underline{c} : N(x-y) < N(\underline{c})$,

where $N(\underline{c})$ is the ideal norm of $\underline{c}$, defined by $N(\underline{c}) = \# (R/\underline{c})$ if $\underline{c} \subset R$ and extended by multiplicativity to the set of all fractional ideals of R . If $\underline{c}$ is principal, $\underline{c} = Rc$, then $N(\underline{c}) = N(c)$, and dividing by c in (0.2) we see that (0.2) is equivalent to (0.1) . In the general case this argument shows that (0.2) depends only on the ideal class C of $\underline{c}$. If (0.2) holds, we call this ideal class <u>Euclidean for the norm</u> or <u>norm-Euclidean</u>.

As we shall see in (2.2), the ring R has at most one ideal class which is Euclidean for the norm, and if there is one, then it generates the class group. The ring $R = \mathbb{Z}[\sqrt{-5}]$ is an example of a ring having a non-principal norm-Euclidean ideal class, cf. (1.3).

In the general case the definition reads as follows. For unexplained terminology, see section 1.

<u>Definition</u>. Suppose R is a domain, and put

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

Let W be a well-ordered set, $\psi : E \to W$ a map, C an invertible ideal class of R , and $\underline{c} \in C$. We say that ψ is a <u>Euclidean algorithm</u> for C or that C is <u>Euclidean with respect to</u> ψ , if the following condition is satisfied:

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

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 $\underline{b}\,\underline{c}\,z^{-1} \in E$.

To obtain the earlier definition from the new one, in the number field case, take $\psi(\underline{b}) = N(\underline{b})^{-1}$. The inequality $\psi(\underline{b}\,\underline{c}\,z^{-1}) < \psi(\underline{b})$ occurring in (0.3) then simplifies to $N(z) < N(\underline{c})$. Using that $\bigcup_{\underline{b}\in E} \underline{b}\,\underline{c} = K$, and writing $z = x-y$, we then find that (0.3) is equivalent to (0.2) . Hence C is Euclidean with respect to ψ if and only if C is norm-Euclidean.

If C is the principal ideal class we can take $\underline{c} = R$ in the definition. With $\underline{b} = Rb^{-1}$, $x = ab^{-1}$, $r = zb$ condition (0.3) then gives :

$$\text{for all } b \in R\ , b \neq 0\ , \text{ and all } a \in R\ , a \notin Rb\ ,$$
$$\text{there exists } r \in a + Rb \text{ such that } \psi(Rr^{-1}) < \psi(Rb^{-1})\ .$$

Hence, if the principal ideal class is Euclidean with respect to ψ , then the ring R is Euclidean with respect to the map $\varphi : R - \{0\} \to W$ defined by $\varphi(b) = \psi(Rb^{-1})$.

The converse is also true. If R is Euclidean with respect to a map $\varphi : R - \{0\} \to W$, then R is a principal ideal ring, so $E = \{Rb^{-1} : b \in R - \{0\}\}$, and a Euclidean algorithm for the principal ideal class is then given by

$$\psi(\underline{b}) = \varphi(b) \text{ if } \underline{b} = Rb^{-1} ;$$

we remark that φ can be chosen such that this definition does not depend on the choice of b , see [25, prop. 4] .

We conclude that R is Euclidean if and only if the principal ideal class of R is Euclidean.

Many results known about Euclidean rings have immediate generalizations for rings possessing a Euclidean ideal class. The most striking example is the following theorem, which generalizes the classical observation that Euclidean domains are principal ideal domains.

Theorem. Suppose R is a domain, and C is an invertible ideal class of R which admits a Euclidean algorithm. Then R is a Dedekind domain, and the class group of R is a finite cyclic group, generated by C .

For a proof of this theorem, and for other elementary properties of Euclidean ideal classes, we refer to section 1, and to theorem (1.2) in particular. As a rule, we have, in this section, suppressed arguments which are routine verifications or direct generalizations of proofs given by Samuel [25].

Examples given at the end of section 1 show that every positive integer occurs as the class number of a ring having a Euclidean ideal class.

In section 2 we consider rings of arithmetic type, restricting ourselves to maps ψ defined by $\psi(\underline{b}) = N(\underline{b})^{-1}$, where N is a naturally defined ideal norm. Typical examples are given by the rings of integers in algebraic number fields, as discussed above. Our main interest is with rings having two primes at infinity. In particular, we give a complete list of quadratic number fields whose rings of integers have a norm-Euclidean ideal class, see (2.11) and (2.13). Our discussion in this section has the character of a survey, and proofs are mostly omitted. Various open problems are indicated.

The same class of arithmetic rings is considered in section 3, now without any restriction on ψ . If such a ring R has only finitely many units, then each Euclidean ideal class of R is actually norm-Euclidean, and a complete list of examples can be given. If R has infinitely many units the situation is different : in this case every ideal class C generating the ideal class group is Euclidean with respect to a suitable ψ (depending on C) , if certain generalized Riemann hypotheses are satisfied. This is the analogue of the theorem of Weinberger and Queen [28,24] in the classical case.

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

1. *Elementary properties*.

In this paper 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. A *fractional ideal* of R is a subset $\underline{d} \subset K$ with the property that $\underline{d}a = \{xa : x \in \underline{d}\}$ is a nonzero ideal of R for some $a \in K$. A fractional ideal $\underline{d}$ is called *integral* if $\underline{d} \subset R$. We put

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

The *ideal class* $[\underline{d}]$ of a fractional ideal $\underline{d}$ is the set $\{\underline{d}\, a : a \in K^*\}$. Every element of $[\underline{d}]$ is a fractional ideal, and two ideal classes are either the same or disjoint. The class $[R]$ is called the *principal* ideal class. The *product* $\underline{d}\cdot\underline{e}$ of two fractional ideals is the fractional ideal $\{\sum_{i=0}^{n} d_i e_i : n \in \mathbb{N}$, $d_i \in \underline{d}$, $e_i \in \underline{e}$ $(0 \le i \le n)\}$, and ideal classes are multiplied by $[\underline{d}]\cdot[\underline{e}] = [\underline{d}\cdot\underline{e}]$. We call $\underline{d}$ *invertible* if $\underline{d}\cdot\underline{e} = R$ for some $\underline{e}$; if such an

$\underline{e}$ exists, it is uniquely determined by $\underline{d}$, and denoted by $\underline{d}^{-1}$. If $\underline{d}$ is invertible, then so are all elements of $[\underline{d}]$. In that case, $[\underline{d}]$ is called an *invertible ideal class*, and we put $[\underline{d}]^{-1} = [\underline{d}^{-1}]$. The ring R is called a *Dedekind domain* if every fractional ideal of R is invertible, cf. [4, §2]. The set of fractional ideals of a Dedekind domain R is a group with respect to multiplication, and the same is true for the set of ideal classes. The latter group is called the *ideal class group*, or *class group*, of R and denoted by $C\ell(R)$. Its unit element is $[R]$, and its order is called the *class number* of R.

The letter W denotes a well-ordered set, which, for convenience, we assume to consist of ordinal numbers.

(1.1) Lemma. If $\psi : E \to W$ is a Euclidean algorithm for the invertible ideal class C, then for every $\underline{b} \in E$, $\underline{b} \neq R$, there exists $n \in \mathbb{N}$ such that

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

Proof. We use induction on $\psi(\underline{b})$. Let $\underline{c} \in C$. Since $\underline{c}$ is invertible and $\underline{b} \neq R$, we have $\underline{b}\,\underline{c} \neq \underline{c}$, so there exists $x \in \underline{b}\,\underline{c} - \underline{c}$. By the definition given in the introduction, we can find $z \in x + \underline{c}$ such that the fractional ideal $\underline{a} = \underline{b}\,\underline{c}\,z^{-1} \in E$ satisfies $\psi(\underline{a}) < \psi(\underline{b})$. Notice that $[\underline{b}] = C^{-1} . [\underline{a}]$.

If $\underline{a} = R$ then $[\underline{b}]= C^{-1}$, and $\psi(\underline{b}) > \psi(\underline{a}) \geq 0$, so $n = 1$ satisfies our requirements.

If $\underline{a} \neq R$, then by the induction hypothesis there exists $m \in \mathbb{N}$ with $[\underline{a}] = C^{-m}$ and $0 < m \leq \psi(\underline{a})$, so with $n = m+1$ we have $[\underline{b}] = C^{-n}$ and $0 < n \leq \psi(\underline{a}) + 1 \leq \psi(\underline{b})$. This proves (1.1).

The theorem stated in the introduction is contained in theorem (1.2) :

(1.2) Theorem. Suppose R is a domain, and C is an invertible ideal class of R which is Euclidean with respect to $\psi : E \to W$. Then R is a Dedekind domain, and $C\ell(R)$ is a finite cyclic group generated by C. The class number h of R satisfies

$$h \leq \psi(Ra^{-1})$$

for every $a \in R - R^*$, $a \neq 0$.

Proof. Let $\underline{d}$ be any fractional ideal of R, and $x \in \underline{d}$, $x \neq 0$. Then $\underline{d}x^{-1} \in E$, so $[\underline{d}] = [\underline{d}x^{-1}] = C^{-n}$ for some $n \in \mathbb{N}$, by lemma (1.1) (if $\underline{d}x^{-1} = R$ we can take $n = 0$). Hence every ideal class is invertible, so R is Dedekind. We also see that $C\ell(R) = \{C^{-n} : n \in \mathbb{N}\}$. In particular, $C = C^{-n}$ for some $n \in \mathbb{N}$, so the order of C, which equals the class number of R, is finite. If $a \in R - R^*$, $a \neq 0$, then with $\underline{b} = Ra^{-1}$ in lemma (1.1) we find that $[R] = [Ra^{-1}] = C^{-n}$ for some $n \in \mathbb{N}$ with $0 < n \leq \psi(Ra^{-1})$. Therefore the order of C is at most $\psi(Ra^{-1})$. This proves (1.2).

We remark that the theorem remains valid if the invertibility assumption on C is replaced by the weaker condition that

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

for $\underline{c} \in C$.

(1.3) Example. Let $R = \mathbb{Z}[\sqrt{-5}]$, $\underline{c} = (2, 1 + \sqrt{-5})$, $C = [\underline{c}]$, and let N be defined as in the introduction. Define $\psi : E \to \mathbb{N}$ by $\psi(\underline{b}) = N(\underline{b})^{-1}$. The ideal class C is invertible, since $\underline{c} \cdot \frac{1}{2}\underline{c} = R$, and we claim that it is Euclidean with respect to ψ. As we have seen in the introduction, this statement is equivalent to

$$(1.4) \qquad \forall x \in K : \exists y \in \underline{c} : N(x-y) < N(\underline{c}) = 2 .$$

If $K = \mathbb{Q}(\sqrt{-5})$ is considered as a subfield of the field of complex numbers $\mathbb{C}$, then $N(z) = |z|^2$ for $z \in K$, so (1.4) is true if we have

$$\forall x \in \mathbb{C} : \exists y \in \underline{c} : |x-y| < \sqrt{2} .$$

This statement is indeed correct, as may be seen by drawing a picture [5] or by applying Dirichlet's hexagon lemma [7, ch.IX, th. VII]. One readily verifies that $\underline{c}^2$ is principal, but that $\underline{c}$ is not, so we conclude that R is a Dedekind domain with class number two.

(1.5) Remark. It might be argued that in this example we have used, rather than proved, that R is a Dedekind domain, by appealing to the multiplicativity of the ideal norm N. Closer inspection reveals that this is not the case. More generally, suppose that $R/\underline{a}$ has finite length as an R-module for every nonzero ideal $\underline{a} \subset R$, and let for every R-module of finite length M a positive integer $f(M)$ be given such that $f(M')\cdot f(M'') = f(M)$ for every exact R-sequence $0 \to M' \to M \to M'' \to 0$; e.g., $f(M) = \# M$ in the above example. Put $N(\underline{a}) = f(R/\underline{a})$ for $\underline{a}$ an integral ideal of R. Then it is not difficult to prove that for integral ideals $\underline{a}, \underline{b}$ we have

$$N(\underline{a}\,\underline{b}) = N(\underline{a})\cdot N(\underline{b}) \qquad \text{if } \underline{a} \text{ or } \underline{b} \text{ is invertible.}$$

This restricted multiplicativity is all that is needed in (1.3), both for the extension of N to the set of all fractional ideals and for the argument in the introduction leading to (1.4).

(1.6) Proposition. Let the invertible ideal class C be Euclidean with respect to ψ, and $\underline{b} \in E$.

If $\psi(\underline{b}) = \min\{\psi(\underline{d}) : \underline{d} \in E\}$ then $\underline{b} = R$.

If $\psi(\underline{b}) = \min\{\psi(\underline{d}) : \underline{d} \in E , \underline{d} \neq R\}$ then $\underline{b} \in C^{-1}$.

Proof. Assume, without loss of generality, that the image of ψ is a beginning segment of the ordinals. Then (1.6) follows from (1.1), with $\psi(\underline{b}) = 0$ or 1.

(1.7) Corollary. If $\psi : E \to W$ is a map, then there is at most one invertible ideal class C of R which is Euclidean with respect to ψ.

Proof. This is immediate from the second assertion in (1.6).

(1.8) Corollary. Let ψ be a Euclidean algorithm for the invertible ideal class C, and $\underline{a}, \underline{a}' \in E$, $\underline{a} \subset \underline{a}'$. Then $\psi(\underline{a}) \leq \psi(\underline{a}')$, with equality if and only if $\underline{a} = \underline{a}'$.

Proof. Fix $\underline{a} \in E$, and define $\psi_1 : E \to W$ by $\psi_1(\underline{b}) = \psi(\underline{a}\,\underline{b})$. This is readily verified to be a Euclidean algorithm for C, so (1.8) follows by applying the first assertion of (1.6) to ψ_1.

Let $\psi : E \to W$ be a Euclidean algorithm for the invertible ideal class C, and $R' \subset K$ a subring containing R. Then R' is Dedekind, and there is a natural surjective map f from the group of fractional ideals of R to the group of fractional ideals of R', mapping $\underline{a}$ to the R-module generated by $\underline{a}$. Put $E' = \{\underline{b}' : \underline{b}'$ is a fractional ideal of R' with $R' \subset \underline{b}'\} = f[E]$, and define $\psi' : E' \to W$ by $\psi'(\underline{b}') = \min\{\psi(\underline{b}) : \underline{b} \in E , f(\underline{b}) = \underline{b}'\}$. Denote by C' the image of C under the map $C\ell(R) \to C\ell(R')$ induced by f. With these hypotheses and notations, we have :

(1.9) Proposition. The ideal class C' of R' is Euclidean with respect to ψ'.

The proof is routine.

(1.10) Corollary. In the above situation, the following three assertions are equivalent :

(a) R' is a principal ideal domain,

(b) R' is Euclidean,

(c) $C' = [R']$.

Proof. The implications (b) ⇒ (a) and (a) ⇒ (c) are obvious, and (c) ⇒ (b) follows from (1.9), since we have seen in the introduction that the principal ideal class is Euclidean if and only if the ring is Euclidean.

From (1.3) and (1.10) it follows that every principal ideal domain contained in $\mathbb{Q}(\sqrt{-5})$ is Euclidean. This generalizes Wedderburn's observation [27, p.138] that $\mathbb{Z}[\sqrt{-5}, 1/3]$ is Euclidean.

Suppose that C is an invertible Euclidean ideal class of R , and put

$$\Psi = \{\psi : E \to W : \psi \text{ is a Euclidean algorithm for } C\} ,$$

where W is the set of ordinals of cardinality $\leq \# E$. Then Ψ is non-empty, and the map $\theta : E \to W$ defined by

$$\theta(\underline{b}) = \min\{\psi(\underline{b}) : \psi \in \Psi\}$$

is a Euclidean algorithm for C , cf. [25, prop. 9] . It is called the smallest algorithm for C .

(1.11) Proposition. Let $\underline{b} \in E$ be such that $\theta(\underline{b})$ is finite. Then $[\underline{b}] = C^{-\theta(\underline{b})}$.

Proof. We use induction on $\theta(\underline{b})$. If $\theta(\underline{b}) = 0$ then the statement follows from (1.6) . Let $\theta(\underline{b}) = n > 0$, and $\underline{c} \in C$. If for all $x \in \underline{b}\ \underline{c} - \underline{c}$ there would exist $z \in x + \underline{c}$ with $\theta(\underline{b}\ \underline{c}\ z^{-1}) \leq n-2$ then the map $\psi : E \to W$ defined by

$$\psi(\underline{b}) = n-1 \ , \ \psi(\underline{d}) = \theta(\underline{d}) \qquad (\underline{d} \neq \underline{b})$$

would be a Euclidean algorithm for C smaller than θ , contradicting that θ is the smallest one. Hence for some $x \in \underline{b}\ \underline{c} - \underline{c}$ there exists $z \in x + \underline{c}$ with $\theta(\underline{b}\ \underline{c}\ z^{-1}) = n-1$. By the induction hypothesis we have $[\underline{b}\ \underline{c}\ z^{-1}] = C^{-n+1}$, and it follows that $[\underline{b}] = C^{-n}$. This proves (1.11) .

(1.12) Proposition. For $\underline{a}, \underline{b} \in E$ we have $\theta(\underline{a}\ \underline{b}) \geq \theta(\underline{a}) + \theta(\underline{b})$.

Proof. For fixed $\underline{a}$ we can write $\theta(\underline{a}\ \underline{b}) = \theta(\underline{a}) + \chi(\underline{b})$, for some $\chi : E \to W$, by (1.8). By the proof of (1.8), the map χ is a Euclidean algorithm for C . Hence we have $\chi(\underline{b}) \geq \theta(\underline{b})$, and proposition (1.12) follows.

We remark that (1.12) is also valid if the ordinal addition is replaced by Hessenberg addition.

The transfinite construction by which the smallest algorithm for C can be "computed" is easily generalized from the classical case [25, sec.4]. We just mention one consequence.

(1.13) Proposition. Let $\underline{b} \in E$. Then $\theta(\underline{b}) = 1$ if and only if $\underline{p} = \underline{b}^{-1}$ is a non-zero prime ideal of R such that $\underline{p} \in C$ and the natural map $R^* \to (R/\underline{p})^*$ is surjective.

The proof is left to the reader.

(1.14) Corollary. Let C be an invertible Euclidean ideal class of R with smallest algorithm θ, let h denote the class number of R, and let, for $\underline{p}$ a non-zero prime ideal of R, the number $n_{\underline{p}}$ be defined by

$$n_{\underline{p}} = j \quad \text{if } \underline{p} \in C^j, \quad 2 \le j \le h,$$

$$n_{\underline{p}} = 1 \quad \text{if } \underline{p} \in C \text{ and } R^* \to (R/\underline{p})^* \text{ is surjective,}$$

$$n_{\underline{p}} = h+1 \text{ if } \underline{p} \in C \text{ and } R^* \to (R/\underline{p})^* \text{ is not surjective.}$$

Then for every $\underline{a} = \prod_{\underline{p}} \underline{p}^{\operatorname{ord}_{\underline{p}}(\underline{a})} \in E$, with $\operatorname{ord}_{\underline{p}}(\underline{a}) \in \mathbb{Z}_{\le 0}$, we have

$$\theta(\underline{a}) \ge \sum_{\underline{p}} (-\operatorname{ord}_{\underline{p}}(\underline{a}))\cdot n_{\underline{p}} \quad . \tag{1.15}$$

Proof. This follows from (1.11), (1.12) and (1.13).

(1.16) Example. We give a series of examples which shows that every positive integer occurs as the class number of a ring having a Euclidean ideal class.

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

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

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

It is readily verified that R is a ring, and that $\underline{c}$ is an invertible ideal of R with $R/\underline{c} \cong k$. Let $a/b \in R - \{0\}$, with $a,b \in k[t]$ relatively prime; then b is a constant times a power of f, and we claim that

$$\dim_k R/R(a/b) = \deg(b) . \tag{1.17}$$

If $b \in k$ this is clear. If $b \notin k$, then we can write an arbitrary element of R in the form c/b^m, with $c \in k[t]$, $m \in \mathbb{N}$, $m \geq 1$. Choose $d,e \in k[t]$ with $c = d \cdot a + e \cdot b^{m-1}$ and $\deg(d) \leq \deg(b^{m-1})$, then we have $c/b^m = (d/b^{m-1}) \cdot (a/b) + (e/b) \equiv e/b \bmod R(a/b)$. Hence the map $\{e \in k[t] : \deg(e) \leq \deg(b)\} \to R/R(a/b)$ mapping e to the residue class of e/b is surjective, and its kernel is easily seen to be $k \cdot a$. Counting dimensions we find (1.17).

We conclude that $\dim_k R/\underline{a} < \infty$ for every integral ideal $\underline{a}$ of R. Define

$$N(\underline{a}) = 2^{\dim_k R/\underline{a}}$$

and extend N by multiplicativity (cf. remark (1.5)) to the set of all fractional ideals of R. We write $N(x) = N(Rx)$ for $x \in K^*$, and $N(0) = 0$. By (1.17), we have

$$N(x) = 2^{-\mathrm{ord}_f(x) \cdot h} \qquad \text{for } x \in K ,$$

where $\mathrm{ord}_f(x) \in \mathbb{Z} \cup \{\infty\}$ is the number of factors f in x.

Using partial fraction expansions we can write any $x \in K$ in the form $x = (c/f^n) + z$, with $n \in \mathbb{N}$, $c \in k[t]$, $\deg(c) < \deg(f^n)$, $z \in K$, $\mathrm{ord}_f(z) \geq 0$. Then $c/f^n \in \underline{c}$, so with $y = c/f^n$ we see that

$$\forall x \in K : \exists y \in \underline{c} : N(x-y) \leq 1 < 2 = N(\underline{c}) .$$

By an argument given in the introduction this means that the map $\psi : E \to \mathbb{N}$ defined by $\psi(\underline{b}) = N(\underline{b})^{-1}$ is a Euclidean algorithm for $C = [\underline{c}]$. Hence R is a Dedekind domain, and $C\ell(R)$ is generated by C.

We calculate the class number of R. From $N(\underline{c}^h) = N(\underline{c})^h = 2^h = N(R \cdot (1/f))$

(by (1.5) and (1.17)) and $\underline{c}^h \subset \{a/b \in R : \deg(a) \le \deg(b)-h\} = R\cdot(1/f)$ we see that $\underline{c}^h = R\cdot(1/f)$, so the class number of R divides h . Conversely, if $\underline{c}^m = R\cdot x$ is principal, then comparing norms we see that $m = -\mathrm{ord}_f(x)\cdot h$, so m is divisible by h .

We conclude that the class number of R equals h . Since for every positive integer h there exists a field k and an irreducible polynomial $f \in k[t]$ of degree h this proves the claim made at the beginning of (1.16) .

If f is not assumed to be irreducible then similar results are valid. In this case, the class number equals the greatest common divisor of the degrees of the factors of f . This can be proved by similar methods, or by reducing the general case to the case treated above using proposition (1.9), or by applying the following proposition.

(1.18) Proposition. Let k be a field, and K a function field in one variable of genus zero over k , having k as its exact field of constants. Let S be a finite non-empty set of prime divisors of K/k and R the subring $R = \{f \in K : f$ has no poles outside $S\}$ of K . Denote the greatest common divisor of the degrees of all divisors of K/k by δ , and of those in S by δ' .

a) If $\delta = 1$ then the map $\psi : E \to \mathbb{N}$ defined by

$$\psi(\underline{b}) = \dim_k \underline{b}/R$$

is a Euclidean algorithm for the ideal class

$$C = \{\underline{c} : \underline{c} \text{ is a fractional ideal of } R \text{ , and the degree of } \underline{c} \text{ is } 1 \bmod \delta'\} ,$$

and the class number of R equals δ'. Moreover, if k is infinite or $\# S = 1$, then C is the only Euclidean ideal class of R, and ψ is the smallest algorithm for C.

b) If $\delta \neq 1$ then R has no Euclidean ideal class.

The proof of this proposition is completely analogous to the proof given by Samuel in the classical case [25, sec.6].

If k is finite and $\# S \geq 2$ in a), then any ideal class generating $C\ell(R)$ is Euclidean, and ψ is not the smallest algorithm for any of them. This follows from (3.3) and (3.7).

2. Norm-Euclidean ideal classes in global fields.

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 $\mathbb{F}_q$. By P we denote the set of all non-trivial prime divisors of K, and S is a finite non-empty subset of P containing the set S_∞ of archimedean prime divisors of K. For each $\underline{p} \in P$, let $| \,|_{\underline{p}}$ be an absolute value of K corresponding to $\underline{p}$. By R we denote the ring of S-integers in K:

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

This is a Dedekind domain with field of fractions K, whose non-zero prime ideals correspond bijectively with the elements of P-S. If $\underline{a} \subset R$ is a non-zero ideal, then $R/\underline{a}$ is a finite ring, whose cardinality is called the <u>norm</u> of $\underline{a}$ and denoted by $N(\underline{a})$. By multiplicativity we extend N to a group homomorphism from the group of fractional ideals of R to $\mathbb{Q}^*_{>0}$. We put

$N(x) = N(Rx)$ for $x \in K^*$, and $N(0) = 0$. If the absolute values $| \ |_{\underline{p}}$ are suitably normalized, then we have

$$(2.1) \qquad N(x) = \prod_{\underline{p} \in S} |x|_{\underline{p}}$$

for $x \in K$. In the case that K is a number field, and $S = S_\infty$, the ring R consists of the algebraic integers in K, and $N : K \to \mathbb{Q}$ is the absolute value of the field norm.

In this section we are interested in conditions under which R has a norm-Euclidean ideal class, i.e., an ideal class which is Euclidean with respect to the map $\psi : E \to \mathbb{N}$ defined by $\psi(\underline{b}) = N(\underline{b})^{-1} = \# \underline{b}/R$.

(2.2) Proposition. Every norm-Euclidean ideal class of R contains all integral ideals $\underline{c}$ of R for which

$$N(\underline{c}) = \min\{N(\underline{a}) : \underline{a} \text{ is an integral ideal} \neq R\} .$$

The ring R has at most one norm-Euclidean ideal class. If there is one, then it generates the class group, and the class number h of R satisfies

$$(2.3) \qquad h < N(a) \quad \text{for all} \quad a \in R-R^*, \ a \neq 0 .$$

Proof. This is a consequence of (1.6), (1.7) and (1.2), with $\psi : E \to \mathbb{N}$ defined by $\psi(\underline{b}) = N(\underline{b})^{-1}-1$.

If K is a number field of degree n over $\mathbb{Q}$, and $S = S_\infty$, then (2.3) with $a = 2$ yields $h < 2^n$. The inequality (2.3) can often be improved. For example, assuming that R has a norm-Euclidean ideal class, we have

$$(2.4) \qquad h \leq \log N(a)/\log q \qquad \text{for all} \quad a \in R - R^*, \quad a \neq 0 ,$$
$$\text{if } \mathbb{F}_q \subset K ,$$

(2.5) $$h \leq \# \{r : r \text{ is a prime power}, \ 1 < r \leq N(a)\} \quad \text{for all } a \in R-R^*, \ a \neq 0,$$

(2.6) $$h \text{ divides } n \text{ if } K/\mathbb{Q} \text{ is Galois of degree } n \text{ and } S = S_\infty .$$

To prove (2.4) one applies (1.2) with $\psi(\underline{b}) = -\log N(\underline{b})/\log q$, which assumes values in $\mathbb{N}$ if $\mathbb{F}_q \subset K$. The proof of (2.5) depends on a modified version of lemma (1.1) and is left to the reader. We shall not make use of (2.5) in the sequel. To prove (2.6), let $\mathcal{G} = \mathcal{G}a\ell(K/\mathbb{Q})$ and let $C = [\underline{c}]$ be norm-Euclidean. Then for every $\sigma \in \mathcal{G}$ the ideal class $\sigma C = [\sigma\underline{c}]$ is norm-Euclidean, so $\sigma C = C$ by (2.2). Hence $C^n = \prod_{\sigma\in\mathcal{G}} [\sigma\underline{c}] = [RN(\underline{c})] = [R]$, and the class number divides n. This proves (2.6).

As we have seen in the introduction, C is norm-Euclidean if and only if

(2.7) $$\forall x \in K : \exists y \in \underline{c} : N(x-y) < N(\underline{c}),$$

where $\underline{c} \in C$. This property is usually investigated in the completion of K at the primes in S. More precisely, for $\underline{p} \in S$ let $K_{\underline{p}}$ be the $\underline{p}$-adic completion of K, and put $K_S = \prod_{\underline{p}\in S} K_{\underline{p}}$. This is a locally compact topological ring. 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 a discrete subgroup of K_S with $K_S/\underline{a}$ compact. We extend N to a map $K_S \to \mathbb{R}_{\geq 0}$ by

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

cf. (2.1). This is a continuous function satisfying $N(xy) = N(x)N(y)$ for $x, y \in K_S$. For $t \in \mathbb{R}_{>0}$ we put

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

for each t , this is an open neighborhood of 0 in K_S . Clearly, (2.7) is equivalent to

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

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

$$K_S = \underline{c} + V_{N(\underline{c})} . \tag{2.8}$$

(2.9) Problem. Is it true that $K \subset \underline{c} + V_{N(\underline{c})}$ if and only if $K_S = \underline{c} + V_{N(\underline{c})}$?

If F is a compact subset of K_S with $K_S = \underline{c} + F$, then (2.8) is equivalent to

$$F \subset \underline{c} + V_{N(\underline{c})} = \bigcup_{y \in \underline{c}} (y + V_{N(\underline{c})})$$

which by compactness of F is true if and only if

$$F \subset \bigcup_{i=1}^{m} (y_i + V_{N(\underline{c})}) \quad \text{for certain} \quad y_1, y_2, \ldots, y_m \in \underline{c} .$$

Using this remark, and the countability of K , one can show that an affirmative answer to (2.9) implies that the problem whether for an explicitly given pair K,S the ring R has a norm-Euclidean ideal class is effectively decidable. I do not know how to prove this decidability without unproved assumptions.

The following proposition, essentially due to Barnes and Swinnerton-Dyer [3, th.M] is the only known result concerning problem (2.9).

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

We do not give the proof here.

In the case $\# S = 1$ all R having a norm-Euclidean ideal class can be determined. In the number field case they are the rings of algebraic integers in the fields

$$(2.11) \qquad K = \mathbb{Q} \ , \ \mathbb{Q}(\sqrt{-d}) \ , \quad d = 3,4,7,8,11,15,20 \ ,$$

with class number two if $K = \mathbb{Q}(\sqrt{-15})$ or $\mathbb{Q}(\sqrt{-20})$ and class number one otherwise. If K is a function field and $\# S = 1$, then R has a norm-Euclidean ideal class if and only if K has genus zero. By (1.18), the class number then equals the degree of the unique prime in S.

In the case $\# S = 2$, $S = S_\infty$, it has been proved by Davenport [9,10,11; cf.6] that only finitely many R, up to isomorphism, are Euclidean with respect to the norm. This result can be generalized as follows.

(2.12) Proposition. Suppose that $\# S = 2$. Then R has a norm-Euclidean ideal class if and only if

(a) K is one of the fields listed in (2.11) ;

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 finite list mentioned under (b) is not completely known. As we shall see below, it contains at least 107 rings.

The rings with $\# S = 2$ can be divided in five categories :

$S = S_\infty$, and K is real quadratic;

$S = S_\infty$, and K is complex cubic;

$S = S_\infty$, and K is totally complex quartic;

$S = \{\underline{p}_\infty, \underline{p}\}$, with $\underline{p}_\infty$ archimedean and $\underline{p}$ non-archimedean;

K is a function field.

We discuss each of these categories in greater detail.

(2.13) $S = S_\infty$, K is real quadratic, and R is its ring of integers. It is, in this case, an immediate consequence of a theorem of Davenport [9, th.2] that R can only have a norm-Euclidean ideal class if the discriminant Δ of K over $\mathbb{Q}$ satisfies $\Delta < 2^{14} = 16384$. A simpler proof by Cassels [6] yields $\Delta < 2044$, and Ennola [13] improved this to $\Delta < 943$. We remark that the rationality arguments in the proofs of Davenport and Cassels can be replaced by an application of (2.10). These results have been used [8,13] to determine all R , in this category, for which the principal ideal class is norm-Euclidean. They correspond to the sixteen values

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

By similar methods as those used in [13, lemma 11] I found that R has a non-principal norm-Euclidean ideal class if and only if

$$\Delta = 40,\ 60 \ \text{ or } \ 85 .$$

In these cases, we have $h = 2$ by (2.6). We conclude that this category contributes precisely 19 rings to the list in (2.12) (b) .

(2.14) $S = S_\infty$, K is complex cubic, and R is its ring of integers. If R has a norm-Euclidean ideal class, then by a theorem of Davenport [10, th.2] the discriminant Δ of K over $\mathbb{Q}$ satisfies $-\Delta < 5.93 \times 10^{27}$, and Cassels [6] improved this to $-\Delta < 170523$. Taylor [26] lists 52 examples with class number 1, but the list is not claimed to be complete. It would be of interest to obtain examples, in this category, where the class number is larger; it is at most 4, if R has a norm-Euclidean ideal class.

(2.15) $S = S_{\infty}$, K is totally complex quartic, and R is its ring of integers. Suppose that R has a norm-Euclidean ideal class. Then the discriminant Δ of K over $\mathbb{Q}$ is $< 5.21 \times 10^{222}$ by a result of Davenport [11, th.2]. Cassels [6] improved this to $\Delta < 24,845,989$, and an obvious modification of his lemma 15 leads to $\Delta < 20,435,007$. Thirty-two examples with class number one, mainly due to Lakein [17,18,20], are known, and his methods can be used to prove that the ring of integers of $K = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$ has a non-principal norm-Euclidean ideal class and class number 2. Hence this category contributes at least 33 rings to (2.12) (b). Examples with class number larger than six do not exist in this category.

(2.16) $S = \{\underline{p}_{\infty}, \underline{p}\}$, with $\underline{p}_{\infty}$ archimedean and $\underline{p}$ non-archimedean. In this case K is either $\mathbb{Q}$ or an imaginary quadratic number field, and if A is the ring of integers of K, then $R = A[\underline{p}^{-1}]$, where the symbol $\underline{p}$ is also used to denote the maximal ideal of A corresponding to the prime divisor $\underline{p}$ of K. Let Δ be the discriminant of K over $\mathbb{Q}$, denote the characteristic of $A/\underline{p}$ by p, and suppose that R has a norm-Euclidean ideal class. Then Cassels's mode of proof [6] can be used to show that

$$|\Delta| \leq \frac{256}{3} \cdot \left(\frac{p}{p-1}\right)^4 .$$

Hence, leaving aside only finitely many possibilities for R, we have $|\Delta| \leq 85$. For each of the remaining values for Δ one can show, by a different argument, that there are only finitely many possibilities for $\underline{p}$, except if $\Delta \in \{1,-3,-4,-7,-8,-11,-15,-20\}$. In the excepted cases, K is one of the fields (2.11), so A has a norm-Euclidean ideal class. Using (1.9) one then easily proves that the same is true for $A[\underline{p}^{-1}]$, regardless of the choice of $\underline{p}$. This gives an infinity of examples in this category, falling under (2.12) (a). Three examples falling under (2.12) (b) are known; they are

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

and have class number one. The last two are due to G. Cooke (unpublished). There are probably many more examples in this category, and it seems an attractive problem to determine them all. One can show that $h \leq 2$ in all cases.

(2.17) K is a function field. If K has genus zero, then R has a norm-Euclidean ideal class, by (1.18), and for $\# S = 2$ the converse can be proved by a suitable adaptation of Cassels's method [6] . The class number of such a ring R is the g.c.d. of the degrees of the two primes in S .

The function field case of (2.12) can be used to answer a question left open by Armitage [1] : if K is cubic over $\mathbb{F}_p(t)$, with p an odd prime, and the infinite prime of $\mathbb{F}_p[t]$ has precisely two extensions to K , then the integral closure R of $\mathbb{F}_p[t]$ in K is Euclidean with respect to the norm if and only if the discriminant of R over $\mathbb{F}_p[t]$ has degree ≤ 4 .

It is not clear how proposition (2.12) should be formulated such that it has a chance of being valid for higher values of $\# S$, e.g. $\# S = 3$. In the function field case, the ring

$$R = \mathbb{F}_2[X,1/X,1/(X+1),Y]/(Y^2+Y+X^3+X+1)$$

is Euclidean with respect to the norm, it has $\# S = 3$, and its field of fractions has genus one. In the number field case, (2.12) is equivalent to the assertion that there exist, up to isomorphism, only finitely many R with $\# S = 2$ having a norm-Euclidean ideal class for which S is <u>minimal</u> with respect to this property, i.e. for no $S' \subset S$, $S' \neq S$, $S' \supset S_\infty$ does the ring R' of S'- integers have a norm-Euclidean ideal class. But the corresponding assertion for $\# S = 3$ is wrong, since it can be proved that in the case

$$K = \mathbb{Q}(\sqrt{14}) \ , \quad S = S_\infty \cup \{\underline{p}\} \qquad (\underline{p} \text{ non-archimedean})$$

the ring R has a norm-Euclidean ideal class if and only if the prime divisor $\underline{p}$ corresponds to a prime ideal of $\mathbb{Z}[\sqrt{14}]$ which is generated by an element which is <u>not</u> 1 mod 2.

For unbounded $\# S$ an infinity of examples can be deduced from a theorem of O'Meara [23] : 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. It is unknown whether S can be taken to satisfy $S \cap T = \emptyset$, where T is a given finite subset of P with $S_\infty \cap T = \emptyset$.

It may be true that in the case $S = S_\infty$ there are only finitely many R , up to isomorphism, which possess a norm-Euclidean ideal class. There are 318 examples known, 312 with class number one [20,22] and 6 with class number two (see (2.11), (2.13) and (2.15)) . Finiteness results for certain classes of cyclic fields have been proved by Heilbronn [14,15] in the case of class number one. I do not know whether his results carry over to the case of larger class numbers.

3. Other Euclidean algorithms in global fields.

In this section K , S and R have the same meaning as in section 2, except in proposition (3.1) and lemma (3.5) which are more generally valid. By C we denote an ideal class of R . From (1.2) we know that for C to be Euclidean it is necessary that C generates the class group, and in this section we are interested in whether the converse is true. Further, if C is Euclidean, we are interested in its smallest algorithm.

It turns out that the situation much depends on whether $\# S = 1$ or $\# S \geq 2$. Notice that, by the Dirichlet unit theorem, we have $\# S = 1$ if and only if R^* is finite. We discuss both cases in more detail.

First let $\# S = 1$, $S = \{\underline{p}\}$. Then $|x|_{\underline{p}} \geq 1$ for all $x \in R - \{0\}$, with equality if and only if $x \in R^*$. Hence the following proposition applies to our situation, with $v = |\ |_{\underline{p}}$.

<u>(3.1) Proposition</u>. Let R be an arbitrary domain which is no field, with field of fractions K , and let $v : K \to \mathbb{R}_{\geq 0}$ be an absolute value on K with the property

$$v(x) \geq 1 \text{ for all } x \in R - \{0\} \text{ , with equality if and only if } x \in R^*.$$

Suppose that C is an invertible ideal class of R which is Euclidean. Then we have :

(a) if v is archimedean, then K is one of the fields

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

R is the ring of algebraic integers in K , the ideal class

C is the unique generator of $C\ell(R)$, and v belongs to the unique archimedean prime divisor of K;

(b) if v is non-archimedean, then $K = k(t)$ for some field k, with t transcendental over k, the absolute value v is trivial on k, and if $\underline{p}$ denotes the prime divisor of K/k to which v belongs then

$$R = \{x \in K : |x|_{\underline{q}} \leq 1 \text{ for all prime divisors } \underline{q} \neq \underline{p} \text{ of } K/k\} .$$

Moreover, the class number h of R equals the degree of $\underline{p}$ over k, and C consists of the fractional ideals of degree 1 mod h.

We do not give the proof of (3.1) here. It makes use of the theorem of Artin and Whaples [2] to show that K is a number field or a function field. The number field case is then dealt with by the methods of [19, sec. 10], and in the function field case a similar argument, depending on Riemann-Roch, can be applied to show that the genus is zero. Application of (1.18) then concludes the proof.

It follows from (3.1) and (1.18), (2.11) that in the case $\# S = 1$ an ideal class is Euclidean if and only if it is norm-Euclidean. In the function field case the smallest algorithm is described in (1.18), and in the number field case we have the following approximate description.

(3.2) Proposition. Let K be one of the fields listed in (3.1) (a), and put

$$\rho = \tfrac{1}{2} \text{ if } K = \mathbb{Q} ,$$

$$\rho = \frac{1}{3}, \frac{1}{2}, \frac{4}{7}, \frac{3}{4}, \frac{9}{11}, \frac{4}{5}, \frac{9}{10} \text{ if } K = \mathbb{Q}(\sqrt{-d}) ,$$

$d = 3, 4, 7, 8, 11, 15, 20$, respectively.

Let R be the ring of algebraic integers in K, and define $\psi : E \to \mathbb{N}$ by

$$\psi(\underline{b}) = (\text{greatest integer} \le \log N(\underline{b})/\log \rho) ,$$

for $\underline{b} \in E$, with N as defined in the introduction. Then ψ is a Euclidean algorithm for the unique ideal class C which generates $C\ell(R)$. Moreover, if θ is the smallest Euclidean algorithm for C, then there exists a real number s such that

$$\theta(\underline{b}) \le \psi(\underline{b}) \le \theta(\underline{b}) + s \quad \text{for all } \underline{b} \in E .$$

The proof uses the methods of [19, sec.10].

It follows from (3.1) (a) that if R is the ring of integers in an imaginary quadratic number field of discriminant Δ, $\Delta = -19$ or $\Delta < -20$, then R has no Euclidean ideal class, even if $C\ell(R)$ is cyclic, as is the case for

$$-\Delta = 19,\ 23,\ 24,\ 31,\ 35,\ 39,\ 40,\ 43,\ 47$$

and probably infinitely many others.

Next we suppose that $\# S \ge 2$. We have, in this case, the following proposition, which generalizes the theorem of Weinberger and Queen [28,24] in the classical case, cf. [21].

(3.3) Proposition. Let K be a global field, S a finite set of prime divisors of K containing S_∞ such that $\# S \ge 2$, and R the ring of S-integers in K. Further, 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 class group of R

is Euclidean.

It follows from (3.3) that the rings $\mathbb{Z}[(1+\sqrt{65})/2]$ and $\mathbb{Z}[\zeta_{23}]$, which have no norm-Euclidean ideal classes, do have Euclidean ideal classes if the Riemann hypotheses are true. If no unproved hypotheses are assumed then all known Euclidean classes in number rings are actually norm-Euclidean. Changing this situation should be easier than proving the Riemann hypotheses.

The proof of (3.3) yields in fact a Euclidean algorithm for C. Assume that C generates $C\ell(R)$, put $h = \# C\ell(R)$, and let, for $\underline{p}$ a non-zero prime ideal of R, the number $m_{\underline{p}}$ be defined by

$$m_{\underline{p}} = h+j \quad \text{if } \underline{p} \in C^j,\ 2 \le j \le h,$$

$$m_{\underline{p}} = h+1 \quad \text{if } \underline{p} \in C \text{ and } R^* \to (R/\underline{p})^* \text{ is surjective,}$$

$$m_{\underline{p}} = 2h+1 \quad \text{if } \underline{p} \in C \text{ and } R^* \to (R/\underline{p})^* \text{ is not surjective,}$$

so $m_{\underline{p}} = n_{\underline{p}} + h$ with $n_{\underline{p}}$ as in (1.14). Then the map $\psi : E \to \mathbb{N}$ defined by

$$(3.4) \qquad \psi(\underline{b}) = \sum_{\underline{p}} (-\operatorname{ord}_{\underline{p}}(\underline{b}))\cdot m_{\underline{p}}, \quad \text{for } \underline{b} = \prod_{\underline{p}} \underline{p}^{\operatorname{ord}_{\underline{p}}(\underline{b})} \in E,$$

is a Euclidean algorithm for C, under the hypotheses of (3.3). The proof makes use of the following lemma, which rephrases the definition of a Euclidean algorithm in terms of integral ideals.

<u>(3.5) Lemma</u>. Let R be an arbitrary Dedekind domain. If $\underline{a}$, $\underline{b}$, $\underline{f}$ are integral ideals of R, let $\underline{a} \equiv \underline{b} \bmod \underline{f}$ express that $\underline{a}\,\underline{b}^{-1} = Ra$ for some $a \in 1 + \underline{f}\,\underline{b}^{-1}$. Let $\psi : E \to W$ be a map, C an ideal class of R, and put $\varphi(\underline{a}) = \psi(\underline{a}^{-1})$ if $\underline{a}$ is an integral ideal of R. Then ψ is a Euclidean algorithm for C if and only if for all integral ideals $\underline{a}$, $\underline{f}$ of R for which

$$\underline{a} \not\subset \underline{f},\ \underline{a} \in C^{-1}\cdot[\underline{f}],$$

there exists $\underline{b} \equiv \underline{a} \bmod \underline{f}$ such that $\varphi(\underline{b}) < \varphi(\underline{f})$.

The proof is left to the reader.

The congruence notion defined in the lemma coincides, in the global field case, with ray class congruence if $\underline{a}$ and $\underline{b}$ are coprime with $\underline{f}$, except that no conditions at the primes in S are imposed on a . If $\underline{a}$ and $\underline{f}$ are not necessarily coprime, $\underline{a} + \underline{f} = \underline{d}$, then an integral ideal $\underline{b}$ satisfies $\underline{a} \equiv \underline{b} \bmod \underline{f}$ if and only if $\underline{b} + \underline{f} = \underline{d}$ and $\underline{a}\,\underline{d}^{-1} \equiv \underline{b}\,\underline{d}^{-1} \bmod \underline{f}\,\underline{d}^{-1}$.

Using the lemma, one finds that to prove that ψ is a Euclidean algorithm for C it suffices to establish the existence of prime ideals $\underline{p}$ in certain ray classes for which the map $R^* \to (R/\underline{p})^*$ is surjective. Here the unit group R^* is infinite, since $\# S \geq 2$. This problem can be dealt with by an analogue of Artin's conjecture on primes with prescribed primitive roots which is discussed in [21]. The validity of this conjecture is a consequence of the Riemann hypotheses we assumed [16].

The map ψ defined by (3.4) does not assume the value 1 and is therefore not the smallest algorithm for C . It is a natural question to ask whether the map $\chi : E \to \mathbb{N}$ defined by

$$\chi(\underline{b}) = \sum_{\underline{p}} (-\mathrm{ord}_{\underline{p}}(\underline{b}))\cdot n_{\underline{p}} \quad , \tag{3.6}$$

with $n_{\underline{p}} = m_{\underline{p}} - h$ as in (1.14), is a Euclidean algorithm for C . If it is one, then it is the smallest one, by (1.14). The answer, modulo the Riemann hypotheses, is affirmative, except in a very special case, which can be completely characterized :

<u>(3.7) Proposition</u>. Let the hypotheses and notations be as in (3.3), and let C be a generator of $C\ell(R)$, with smallest algorithm θ . Then equality holds in (1.15), i.e., θ equals the map χ defined by (3.6), except if for some prime ideal $\underline{\ell}$ of R the following conditions are satisfied :

(3.8) K is a totally complex number field, R is its ring of integers (so $S = S_\infty$) , $C\ell(R)$ has order 2 and is generated by $[\underline{\ell}]$, we have $\underline{\ell}^2 = R\cdot 2$, the natural map $R^* \to (R/\underline{\ell})^*$ is surjective, for every $u \in R^*$ there exists $x \in R$ with $x^2 \equiv u \bmod \underline{\ell}^2$, and for some $v \in R^*$ the extension $K(\sqrt{2v})/K$ is totally unramified.

If (3.8) holds, then θ is given by

$$\theta(\underline{b}) = \chi(\underline{b}) + (-\mathrm{ord}_{\underline{\ell}}(\underline{b})) \qquad \text{if } \mathrm{ord}_{\underline{\ell}}(\underline{b}) \text{ is even,}$$

$$\theta(\underline{b}) = \chi(\underline{b}) + (-\mathrm{ord}_{\underline{\ell}}(\underline{b})) -1 \qquad \text{if } \mathrm{ord}_{\underline{\ell}}(\underline{b}) \text{ is odd,}$$

for $\underline{b} \in E$, with χ defined by (3.6).

The proof of (3.7) again uses the techniques of [21] .

Examples in which (3.8), with $v = 1$, is satisfied are the rings of integers of the fields $K = \mathbb{Q}((-5 + 5^{1/2})^{1/2})$ and $K = \mathbb{Q}((-6)^{1/2}, \cos(2\pi/9))$.

References.

1. J.V. Armitage, Euclid's algorithm in certain algebraic function fields, Proc. London Math. Soc. (3) 7 (1957), 498-509.

2. E. Artin, G. Whaples, Axiomatic characterization of fields by the product formula for valuations, Bull. Amer. Math. Soc. 51 (1945), 469-492; pp. 202-225 in : The collected papers of Emil Artin, Addison-Wesley, Reading, 1965.

3. E.S. Barnes, H.P.F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms (II), Acta Math. 88 (1952), 279-316.

4. N. Bourbaki, Algèbre commutative, Ch. 7, Hermann, Paris 1965.

5. 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.

6. 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.

7. J.W.S. Cassels,An introduction to the geometry of numbers, Springer, Berlin 1959.

8. H. Chatland, H. Davenport, Euclid's algorithm in real quadratic fields, Canad. J. Math. 2 (1950), 289-296; pp. 366-373 in [12].

9. H. Davenport, Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields, Proc. London Math. Soc. (2) 53 (1951), 65-82; pp. 344-361 in [12].

10. H. Davenport, Euclid's algorithm in cubic fields of negative discriminant, Acta Math. 84 (1950), 159-179; pp. 374-394 in [12].

11. H. Davenport, Euclid's algorithm in certain quartic fields, Trans. Amer. Math. Soc. 68 (1950), 508-532; pp. 404-428 in [12].

12. The collected works of Harold Davenport, vol. I, Academic Press, London 1977.

13. V. Ennola, On the first inhomogeneous minimum of indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields, Ann. Univ. Turku Ser. A I 28 (1958), 58 pp.

14. H. Heilbronn, On Euclid's algorithm in cubic self-conjugate fields, Proc. Cambridge Philos. Soc. 46 (1950), 377-382.

15. H. Heilbronn, On Euclid's algorithm in cyclic fields, Canad. J. Math. 3 (1951), 257-268.

16. C. Hooley, On Artin's conjecture, J. Reine Angew. Math. 225 (1967), 209-220.

17. E.E. Kummer, Letter to Kronecker dated 2 Oct. 1844, pp. 87-91 in : E.E. Kummer, Collected papers, vol.I, Springer, Berlin 1975.

18. R.B. Lakein, Euclid's algorithm in complex quartic fields, Acta Arith. 20 (1972), 393-400.

19. H.W. Lenstra, Jr., Lectures on Euclidean rings, Bielefeld 1974.

20. H.W. Lenstra, Jr., Euclidean number fields of large degree, Invent. Math. 38 (1977), 237-254.

21. H.W. Lenstra, Jr., On Artin's conjecture and Euclid's algorithm in global fields, Invent. Math. 42 (1977), 201-224.

22. H.W. Lenstra, Jr., Quelques exemples d'anneaux euclidiens, C.R. Acad. Sci. Paris, 286 (1978), 683-685.

23. O.T.O'Meara, On the finite generation of linear groups over Hasse domains, J. Reine Angew. Math. 217 (1965), 79-108.

24. C. S. Queen, Arithmetic Euclidean rings, Acta Arith. 26 (1974), 105-113.

25. P. Samuel, About Euclidean rings, J. Algebra 19 (1971), 282-301.

26. E.M. Taylor, Euclid's algorithm in cubic fields with complex conjugates, J. London Math. Soc. 14 (1976), 49-54.

27. J.H.M. Wedderburn, Non-commutative domains of integrity, J. Reine Angew. Math. 167 (1932), 129-141.

28. P.J. Weinberger, On Euclidean rings of algebraic integers, Proc. Symp. Pure Math. 24 (Analytic number theory), 321-332, Amer. Math. Soc. 1973.