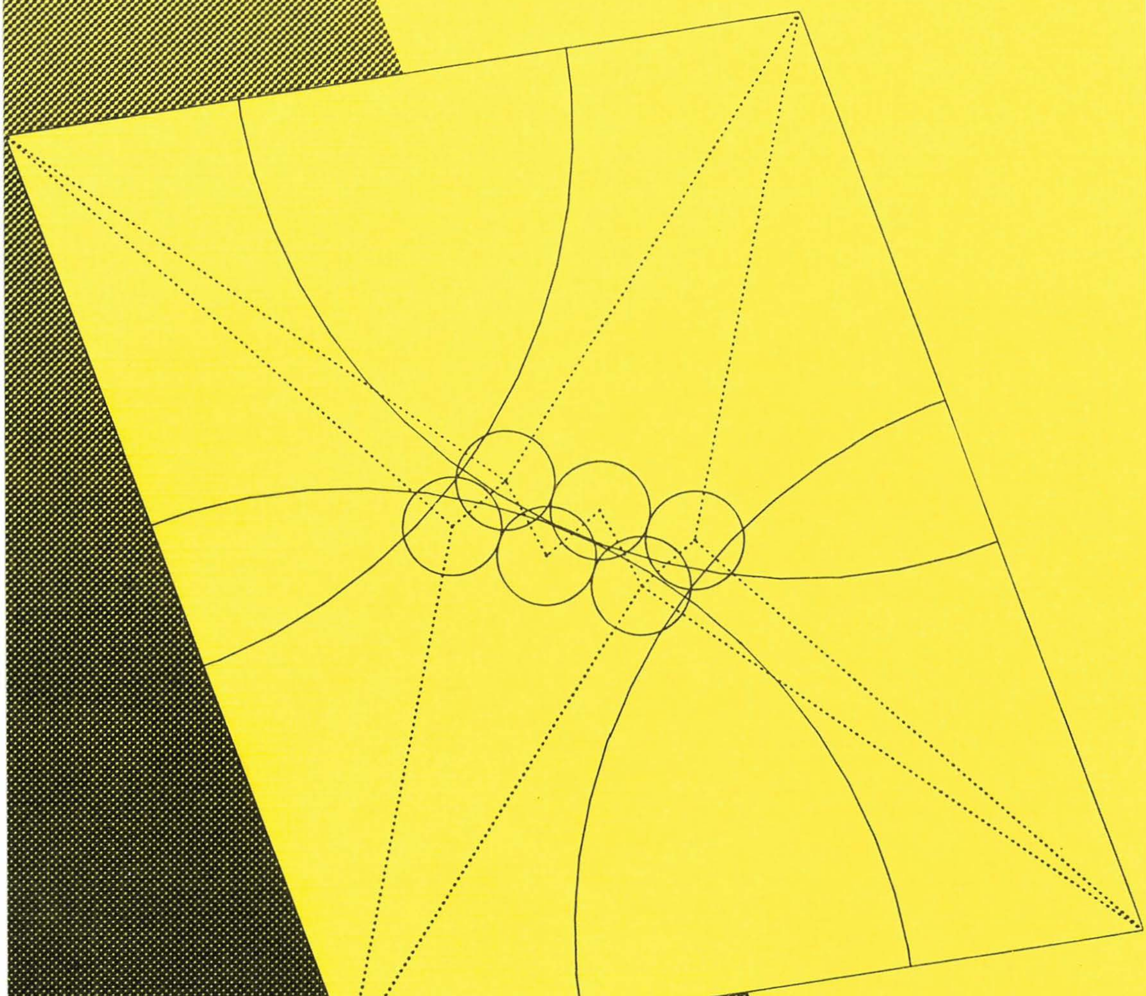
Euclidean rings with two infinite primes

F.J. van der Linden



Euclidean rings with two infinite primes

Euclidean rings with two infinite primes

Academisch proefschrift

ter verkrijging van de graad van
doctor in de Wiskunde en Natuurwetenschappen
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
dr. D.W. Bresters
hoogleraar in de Faculteit
der Wiskunde en Natuurwetenschappen
in het openbaar te verdedigen
in de Aula der Universiteit
(tijdelijk in de Lutherse kerk, ingang Singel 411, hoek Spui)
op woensdag 23 mei 1984 des namiddags te 4.00 uur

door

Franciscus Jozef van der Linden

geboren te Muiden

1984
Centrum voor Wiskunde en Informatica, Amsterdam

PROMOTOR: PROF. DR. H.W. LENSTRA JR.

CONTENTS

INTRODUCTION

§(0.1) The Euclidean algorithm

An *algebraic number field* is a finite extension of the field of rational numbers $\mathbb{Q}$. One of the subjects of algebraic number theory is to generalize classical number theory, which deals with the ring $\mathbb{Z}$ of ordinary integers, to subrings of algebraic number fields K. Of particular interest is the *ring of integers* $\mathcal{O} = \mathcal{O}(K)$ of the field K. This ring $\mathcal{O}$ is the integral closure of $\mathbb{Z}$ in K, i.e. it consists of those $\alpha \in K$ for which there exists a *monic* polynomial $f \in \mathbb{Z}[X]$ with $f(\alpha) = 0$.

The ring $\mathcal{O}$ has much in common with $\mathbb{Z}$, but there are differences. For instance, the ring $\mathbb{Z}$ has unique factorization, which does not hold in general for rings of integers of algebraic number fields. However there are fields for which the ring $\mathcal{O}$ does have unique factorization.

The proof that $\mathbb{Z}$ has unique factorization depends on an algorithm given by Euclid (~ 300 B.C.) [Eu] book VII prop. 1,2. This algorithm calculates the *greatest common divisor* gcd(a,b) of two elements $a,b \in \mathbb{Z}$. It consists of repeatedly using division with remainder:

(0.1) For any $a,b \in \mathbb{Z}$ with $b \neq 0$ there exist $q,r \in \mathbb{Z}$ such that $a = qb + r$ and $|r| < |b|$.

In general if in a ring $\mathcal{O}$ we have division with remainder, analogously to (0.1), we can construct an algorithm to compute the greatest common divisor of two elements of $\mathcal{O}$. This algorithm is called a *Euclidean algorithm.* If a ring has a Euclidean algorithm we can prove that it has unique factorization.

In order to generalize (0.1) we define a generalization of the absolute value: the *norm* $N(\alpha)$ of an element $\alpha \in \mathcal{O}$ is defined by

(0.2) $$N(\alpha) = \#\mathcal{O}/\alpha\mathcal{O} \quad \text{if } \alpha \neq 0; \; N(0) = 0,$$

where # denotes the cardinality. If $K = \mathbb{Q}$, then $\mathcal{O} = \mathbb{Z}$, and the norm is equal to the usual absolute value. By multiplicativity we extend the norm to all of K.

We call $\mathcal{O}$ a *Euclidean* ring (for the norm) if the following condition is satisfied.

(0.3) For any $a,b \in \mathcal{O}$, with $b \neq 0$, there exist $q,r \in \mathcal{O}$ such that $a = qb + r$ and $N(r) < N(b)$.

From (0.1) we see that $\mathbb{Z}$ is a Euclidean ring.

The first rings that were proven to be Euclidean were among the *cyclotomic* rings. These rings are the rings of integers $\mathcal{O} = \mathbb{Z}[\zeta_n]$ of the fields $\mathbb{Q}(\zeta_n)$. Here ζ_n is a primitive n-th root of unity, i.e. $\zeta_n^n = 1$ and $\zeta_n^i \neq 1$ for $0 < i < n$. For example by taking $n = 1$ we recover the ring $\mathbb{Z}$. Cyclotomic rings were encountered in the 19-th century in the study of higher degree reciprocity laws.

Gauss was the first who proved that certain cyclotomic rings different from $\mathbb{Z}$ are Euclidean. In 1832 he published a paper on biquadratic reciprocity in which he proved that $\mathbb{Z}[i]$ is Euclidean ([G3] §§41-45), where $i = \sqrt{-1} = \zeta_4$. He also proved that $\mathbb{Z}[\zeta_3]$ is Euclidean, c.f. Gauss' Nachlass [G2], where $\zeta_3 = \frac{1}{2}(-1 + \sqrt{-3})$. In 1844 Kummer [K] proved that $\mathbb{Z}[\zeta_5]$ and $\mathbb{Z}[\zeta_7]$ are Euclidean. We refer to section (0.6) for more details about the determination of Euclidean cyclotomic rings.

§(0.2) Euclidean rings of integers in quadratic, cubic and quartic fields

Apart from cyclotomic rings, other rings of integers were investigated as well. In particular attention was paid to the rings of integers of quadratic fields. The study of these fields was a natural development in the investigation of binary quadratic forms.

Any quadratic number field is of the form $K = \mathbb{Q}(\sqrt{\Delta})$ for some $\Delta \in \mathbb{Z}$. This Δ is uniquely determined by K if we require that $\Delta \equiv 0,1 \bmod 4$, that Δ is not divisible by the square of an integer > 2, and that $\Delta \equiv 8,12 \bmod 16$ if Δ is even. The unique Δ that satisfies these restrictions is called the *discriminant* of the field. In section (3.1) we will give the precise connection between quadratic fields and binary quadratic forms of the same discriminant Δ, in the case that $\Delta < 0$.

The ring of integers of the quadratic field of discriminant Δ is equal to $\mathcal{O} = \mathbb{Z}[\frac{1}{2}(\Delta + \sqrt{\Delta})]$. If Δ is positive we can embed $K = \mathbb{Q}(\sqrt{\Delta})$ into $\mathbb{R}$. In this case K is called a *real* quadratic field. If Δ is negative $K = \mathbb{Q}(\sqrt{\Delta})$ is called an *imaginary* quadratic field.

The determination of Euclidean rings of integers of imaginary quadratic fields is easy. In particular the rings with $\Delta = -3$ or $\Delta = -4$, which are equal to the cyclotomic rings $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[\zeta_4]$, are Euclidean as we have seen in section (0.1). In a supplement to the book of Dirichlet, Dedekind showed that $\mathbb{Z}[\frac{1}{2}(\Delta + \sqrt{\Delta})]$ is Euclidean for $\Delta \in \{-3,-4,-7,-8,-11, 5,8,12,13\}$, cf. [D3] supp. XI §159. In fact he gives the proof only for $\Delta = -4$ and states that for the other rings the proof is analogous. He also asserts that the ring of integers of $\mathbb{Q}(\sqrt{-19})$ is not Euclidean but that it does have unique factorization. In 1927 Dickson proved that the only Euclidean rings of integers of imaginary quadratic fields are those that Dedekind listed, i.e. $\Delta \in \{-3,-4,-7,-8,-11\}$, cf. [Di] Kap. VIII §93 Satz 7.

We will now turn our attention to real quadratic fields. Also in this case all Euclidean rings of integers have been determined but it was much harder to establish this. In section (0.6) we describe the steps that led to this determination. Finally in 1948 Chatland and Davenport [CD] proved that for positive Δ the ring $\mathbb{Z}[\frac{1}{2}(\Delta + \sqrt{\Delta})]$ is Euclidean if and only if Δ assumes one of the following values:

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

In fact they stated that $\mathbb{Z}[\frac{1}{2}(97 + \sqrt{97})]$ is also Euclidean, following an erroneous statement by Rédei [Ré3]. The error was later corrected by Barnes and Swinnerton-Dyer [BSD1].

Davenport showed that the method of Chatland and himself could also be applied to certain classes of cubic and quartic fields [Da2; Da3; Da4; Da5], namely, the cubic fields with exactly one embedding in $\mathbb{R}$ and the quartic fields with no embedding in $\mathbb{R}$. Davenport proved that there are, up to isomorphism, only finitely many such fields for which the ring of integers is Euclidean.

The *discriminant* $\Delta(K)$ of an algebraic number field K will be defined in section (3.2). It is an important invariant of the field, which generalizes the discriminant of a quadratic number field. In general the field K is not uniquely determined by $\Delta(K)$ and the degree, as it is for quadratic fields. However, there are only finitely many fields with a given discriminant, even if the degree is not specified. Davenport established an upper bound for the absolute value of the discriminant of a cubic or quartic field of one of the types mentioned above that has a Euclidean ring of integers.

Using a different method, Cassels [C1] obtained in 1951 an improvement of Davenport results. This implied a drastic reduction of the amount of work needed to determine all Euclidean rings of integers of real quadratic fields. Also the discriminant bounds for the special classes of cubic and quartic fields were improved. However in these cases the bounds are still too large to allow a complete determination of all Euclidean rings. A description of Cassels' method is given in section (5.3).

§(0.3) Euclidean rings of functions

It has often been observed that function fields of curves defined over finite fields are in many ways analogous to algebraic number fields. The role of the ring of integers is played by certain subrings of these function fields. In 1957 Armitage [Ar1] showed that Davenport's results can be generalized to several rings of this type.

Armitage considered the integral closure $\mathcal{O}$ of the polynomial ring $\mathbb{F}_p[t]$ in certain quadratic and cubic extensions of $\mathbb{F}_p(t)$, with p an odd prime number. For quadratic extensions he determined in which cases the ring $\mathcal{O}$ is Euclidean. For cubic extensions he derived partial results.

There is a more natural way to describe these function fields and their subrings. This is also the description that Armitage used in his later work [Ar2]. We give this description here.

The fields Armitage considered are examples of *function fields in one variable* with a finite field $\mathbb{F}_q$ as field of constants. A function field in one variable with $\mathbb{F}_q$ as field of constants is a finitely generated field of transcendence degree 1 over $\mathbb{F}_q$, having $\mathbb{F}_q$ as it largest finite subfield. For most assertions in this section about function fields in one variable we refer to [Cv;De], for the connection between function fields in one variable and curves we refer to [Ha] ch I §6 and for the definition of curves over arbitrary fields we refer to [Se] ch VI §1; [We2] ch VII §1; [We3] p. 3.

Let K be a function field in one variable with $\mathbb{F}_q$ as field of constants. The field K is the *function field* of a non-singular projective curve C defined over $\mathbb{F}_q$. For an extension field F of $\mathbb{F}_q$ we denote by $C(F)$ the set of points of C defined over F. Each element of K can be regarded as a function: $C(F) \to F \cup \{\infty\}$.

We give two examples to illustrate this. First, the field $\mathbb{F}_q(t)$ is the function field of the projective line $\mathbb{P}^1$ over $\mathbb{F}_q$. For each extension field F over $\mathbb{F}_q$ the curve $\mathbb{P}^1(F)$ is equal to $F \cup \{\infty\}$. Next we consider the (elliptic) function field $\mathbb{F}_2(t,u)$ with $u^2+u = t^3+t+1$. For an extension field F of $\mathbb{F}_2$ the curve $C(F)$ is equal to $\{(u:t:z) \in \mathbb{P}^2(F) : u^2z+uz^2 = t^3+tz^2+z^3\}$. In particular $C(\mathbb{F}_2)$ consists only of the point $(1:0:0)$.

Let K be a function field in one variable with constant field $\mathbb{F}_q$ corresponding to the curve C. Let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$ and let G be the Galois group of $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$. The *prime* of K corresponding to an element P of $C(\overline{\mathbb{F}}_q)$ is the set $p = \{\sigma P : \sigma \in G\}$. The cardinality of a prime p is called the *degree* of p, notation: $\deg(p)$. It is equal to the minimal positive integer n, such that $P \in C(\mathbb{F}_{q^n})$.

Let f be an element of K and let F be an extension field of $\mathbb{F}_q$. We regard f as a function $f : C(F) \to \mathbb{P}^1(F) = F \cup \{\infty\}$. Let p be a prime of K and suppose that all elements of p are in F. We say that f has a zero or a pole of order n in p if it has such a zero or pole in some element of p. Because $0, \infty \in \mathbb{P}^1(F)$ are already defined over $\mathbb{F}_q$ this definition does not depend on the choice of the element in p.

Let S be a non-empty set of primes of K. We define a ring A_S by

(0.4) $$A_S = \{f \in K : f \text{ has no poles in } p \text{ for } p \notin S\}.$$

For example, if $K = \mathbb{F}_q(t)$ and $S = \{\infty\}$ we get $A_S = \mathbb{F}_q[t]$; if $S = \{0,\infty\}$ we get $A_S = \mathbb{F}_q[t,t^{-1}]$. For another example we take $K = \mathbb{F}_2(t,u)$, with $u^2 + u = t^3+t+1$. Above we have seen that the corresponding curve $C(\mathbb{F}_2)$ has only one point. Hence K has a unique prime ∞ of degree 1. We have $A_{\{\infty\}} = \mathbb{F}_2[t,u]$. Let α be a generator of $\mathbb{F}_4$ over $\mathbb{F}_2$. There are 4 points in $C(\mathbb{F}_4) - C(\mathbb{F}_2)$: $(\alpha:0:1)$, $(\alpha+1:0:1)$, $(\alpha:1:1)$ and $(\alpha+1:1:1)$. They give rise to two primes of degree 2 in K: $p = \{(\alpha:0:1), (\alpha+1:0:1)\}$ and $q = \{(\alpha:1:1), (\alpha+1:1:1)\}$. It can be shown that the elements of $\mathbb{F}_2[t,u] \subset K$ that have a zero at p form the ideal generated by t. This can be used to show that $A_{\{\infty,p\}} = \mathbb{F}_2[t,u,t^{-1}]$. In section (1.4) we return to this example.

The rings Armitage considered are all of the form A_S, with $\#S \leq 2$. A quadratic or cubic extension of $\mathbb{F}_p(t)$ is a function field of a curve that is a double or triple covering of the projective line $\mathbb{P}^1$. For the rings that Armitage considered the set S always consists of all primes lying over $\infty \in \mathbb{P}^1(\mathbb{F}_p)$.

The *genus* $g(K)$ of a function field K is an invariant that is analogous to the discriminant of a number field. It will be defined in section (3.2). It can be shown that a function field K with finite field of constants $\mathbb{F}_q$ has genus equal to 0 if and only if $K \simeq \mathbb{F}_q(t)$, cf. [De] §39.

We may use Hurwitz' theorem [Ha] ch.IV §2 cor.2.4 to compute the genus of extension fields of $\mathbb{F}_p(t)$. This computation tells us that the rings A_S that Armitage considered are Euclidean only in the cases that $g(K) = 0$ and $\gcd(\deg(\mathfrak{p}) : \mathfrak{p} \in S) = 1$. Thus Armitage's results are consequences of the following theorem that will be proven in this thesis, cf. theorems (0.18) and (0.19).

THEOREM (0.5). *Let* K *be a function field in one variable with finite field of constants. Let* S *be a set of* 1 *or* 2 *primes of* K. *Then* A_S *is Euclidean if and only if* $g(K) = 0$ *and* $\gcd(\deg(\mathfrak{p}) : \mathfrak{p} \in S) = 1$.

The proof will be given in sections (4.1) and (5.4). In the case that $\#S = 1$ all Euclidean rings are isomorphic to $\mathbb{F}_q[t]$ as we will see below. If the ring A_S has unique factorization we have $\gcd(\deg(\mathfrak{p}) : \mathfrak{p} \in S) = 1$, cf. [S] prop.16, hence the condition in (0.5) is a natural one.

In section (1.4) we show that we cannot expect a theorem as (0.5) for $\#S \geq 3$: whether or not a ring is Euclidean does not only depend on the genus and the degrees of the primes in S.

In the case that $g(K) = 0$ we give an explicit description of the rings A_S. As we remarked above we have $K \simeq \mathbb{F}_q(t)$. We show that there is a natural $1-1$ correspondence:

$$\{\text{primes of } K\} \leftrightarrow \{\text{monic irreducible polynomials in } \mathbb{F}_q[t]\} \cup \{\infty\}.$$

Let $\mathfrak{p}$ be a prime of K not equal to $\{\infty\}$. We have to construct a monic irreducible $f_\mathfrak{p}$ in $\mathbb{F}_q[t]$. Because K is the function field of $\mathbb{P}^1$ and $\mathbb{P}^1(\overline{\mathbb{F}}_q) = \overline{\mathbb{F}}_q \cup \{\infty\}$ we may regard $\mathfrak{p}$ as a conjugacy class under $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ of elements of $\overline{\mathbb{F}}_q$. For $f_\mathfrak{p}$ we take the minimal polynomial of some element of $\mathfrak{p}$. This does not depend on the choice of this element. We have $\deg(\mathfrak{p}) = \deg(f_\mathfrak{p})$ the correspondence between primes $\neq \{\infty\}$ and monic irreducible polynomials is bijective.

Let p be a prime of K and let $\alpha \in \mathbb{F}_q(t)$. First suppose that $p \neq \{\infty\}$. Then α has a pole in p if and only if α can be written as $\frac{h}{g}$ with $h,g \in \mathbb{F}_q[t]$, $f_p \nmid h$ and $f_p \mid g$. The element α has a pole at $\{\infty\}$ if and only if $\alpha = \frac{h}{g}$ with $\deg(h) > \deg(g)$. Thus, by using (0.4) we get the following description of A_S.

(0.6) (a) $A_S = \{\frac{h}{g} : g,h \in \mathbb{F}_q[t],\ g = \prod_{p \in S-\{\infty\}} f_p^{n(p)}$ for some $n(p) \in \mathbb{Z}_{\geq 0}\}$.

if $\{\infty\} \in S$;

(b) $A_S = \{\frac{h}{g} : g,h \in \mathbb{F}_q[t], \deg(h) \leq \deg(g)$ and $g = \prod_{p \in S} f_p^{n(p)}$ for some $n(p) \in \mathbb{Z}_{\geq 0}\}$

if $\{\infty\} \notin S$.

As promised after (0.5) we show that for $\#S = 1$ in (0.5) we have $A_S \simeq \mathbb{F}_q[t]$. If $S = \{\{\infty\}\}$ we have $A_S = \mathbb{F}_q[t]$ by (0.6)(a). If $S = \{p\}$ with $p \neq \{\infty\}$ we have $f_p = t-\alpha$ for some $\alpha \in \mathbb{F}_q$. Then $A_S = \mathbb{F}_q[\frac{1}{t-\alpha}] \simeq \mathbb{F}_q[t]$ by (0.6)(b).

As is common usage we will call a function field with $\mathbb{F}_q$ as field of constants a function field over $\mathbb{F}_q$.

§(0.4) Valuations

In this section we describe the analogy between the rings of integers of algebraic number fields and the rings A_S given by (0.4). We state this analogy in terms of *valuations*. For the proofs of the assertions about valuations given in this section we refer to the standard books on algebraic number theory, e.g. [BS; CF; H1; Iy; La2; W].

Let K be a field. A *valuation* on K is a function $\varphi : K \to \mathbb{R}_{\geq 0}$ satisfying the following conditions.

(0.7) $\varphi(\alpha) = 0 \Longleftrightarrow \alpha = 0$;

$\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ for $\alpha,\beta \in K$;

there exists a constant $C \in \mathbb{R}$ such that

$\varphi(\alpha) \leq 1 \Rightarrow \varphi(1+\alpha) \leq C$.

By taking $C = 2$ we find that the ordinary absolute value is a valuation on every subfield of $\mathbb{C}$.

If we can take $C = 1$ in (0.7) the valuation is called *non-archimedean.* The other valuations are called *archimedean.*

Every positive power of a valuation is again a valuation. Two valuations φ_1 and φ_2 are called *equivalent* if there exists an $r \in \mathbb{R}_{>0}$ with $\varphi_1^r = \varphi_2$.

Each valuation φ renders K into a topological field, with $\{\{\alpha \in K : \varphi(\alpha) < \varepsilon\} : \varepsilon \in \mathbb{R}_{>0}\}$ as a basis for the neighbourhoods of 0. Two valuations are equivalent if and only if they give rise to the same topology on K. Every field has a *trivial valuation*, given by $\varphi(\alpha) = 1$ whenever $\alpha \neq 0$. This endows K with the discrete topology.

An equivalence class of non-trivial valuations is called a *prime* of K. Two equivalent valuations are both archimedean or both non-archimedean. Accordingly we may call a prime archimedean or non-archimedean. Below we will see that the non-archimedean primes of $\mathbb{Q}$ are in 1-1 correspondence to prime numbers. The only archimedean prime of $\mathbb{Q}$ is the equivalence class of the usual absolute value. Also we will see that the primes as defined here are in 1-1 correspondence to the primes as defined in section (0.3).

Let p be a non-archimedean prime of K, and let $\varphi \in p$ be a valuation. We define the *valuation ring* $\mathcal{O}_p$ of p by

(0.8) $$\mathcal{O}_p = \{x \in K : \varphi(x) \leq 1\}.$$

This is a subring of K that does not depend on the choice of $\varphi \in p$. The ring $\mathcal{O}_p$ has exactly one maximal ideal, which we also denote by p:

(0.9) $$p = \{x \in K : \varphi(x) < 1\}.$$

Let K be a function field in one variable with finite field of constants. Let p be a prime of K as defined in section (0.3). It gives rise to a valuation φ of K, as follows. Choose $\gamma \in \mathbb{R}$ with $0 < \gamma < 1$. If $f \in K^*$ we define

$$\varphi(f) = \gamma^n \text{ if } f \text{ has a zero of order } n \text{ at } p;$$
$$\varphi(f) = \gamma^{-n} \text{ if } f \text{ has a pole of order } n \text{ at } p;$$
$$\varphi(f) = 1 \text{ if } f \text{ has no zero or pole at } p;$$
$$\varphi(0) = 0.$$

The function φ is a non-archimedean valuation of K. For example if $K = \mathbb{F}_q(t)$ and $p = \{\infty\}$ then $\varphi(f) = \gamma^{\deg(f)}$ for all $f \in \mathbb{F}_q[t] - \{0\}$. A different choice of γ gives an equivalent valuation. All non-trivial valuations of K are of this form and different primes give rise to non-equivalent valuations, cf. [ZS] ch.VII §4^{bis}; [La1] ch.II §1 ex.2. Hence we may identify both notions of primes of K.

Using (0.8) we get a new description of the rings A_S defined in (0.4), as follows:

$$(0.10) \qquad A_S = \bigcap_{p \notin S} \mathcal{O}_p.$$

For example if $K = \mathbb{F}_q(t)$, $S = \{\{\infty\}\}$ then A_S consists of those $f \in K$ that have no poles outside $\{\infty\}$, i.e. $A_S = \mathbb{F}_q[t]$, accordingly to (0.6) (a).

Because S consists of the primes where the elements of A_S may have poles we call S the set of *primes at infinity* of A_S.

Now we consider the primes of an algebraic number field K. Such a field admits archimedean valuations, in contrast to function fields with a finite field of constants.

As we remarked above every embedding of K in $\mathbb{C}$ gives rise to an archimedean valuation induced by the ordinary absolute value on $\mathbb{C}$. Two different embeddings give rise to the same prime if and only if they are complex conjugate. Each archimedean prime is derived from an embedding of K in $\mathbb{C}$, cf. [W] 1-8. The set of archimedean primes of K will be denoted by S_∞. If a prime in S_∞ corresponds to an embedding with image in $\mathbb{R}$ we call it a *real* prime. The other archimedean primes are called *complex* primes. Let r be the number of real primes and let s be the number of complex primes of K. If the degree $[K:\mathbb{Q}]$ equals n there are exactly n embeddings of K into $\mathbb{C}$, hence $r + 2s = n$ and $\frac{1}{2}n \leq \#S_\infty \leq n$.

The non-archimedean primes of K correspond to non-zero prime ideals of $\mathcal{O}$ as follows. Let p be a prime ideal of $\mathcal{O}$ and let $\gamma \in \mathbb{R}$ be fixed such that $0 < \gamma < 1$. For $\alpha \in \mathcal{O} - \{0\}$ there exists a unique $n \in \mathbb{Z}_{\geq 0}$ such that $\alpha \in p^n - p^{n+1}$. We take $\varphi(\alpha) = \gamma^n$. By multiplicativity we extend φ to K^*, and we take $\varphi(0) = 0$. Then φ is a non-archimedean valuation of K. A different choice of γ gives an equivalent valuation. In this way we get a bijection between the set of non-zero prime ideals of $\mathcal{O}$ and the set of non-archimedean primes of K, cf. [La2] ch.II §1. When no confusion arises we denote the prime ideals of $\mathcal{O}$ and the corresponding primes of K by the same letter.

Using the valuation of K we get a characterization of $\mathcal{O}$ by

$$(0.11) \qquad \mathcal{O} = \bigcap_{p \notin S_\infty} \mathcal{O}_p.$$

Notice the similarity with (0.10).

By a *global field* we mean either an algebraic number field or a function field in one variable with finite field of constants. The set of archimedean primes of a global field K will be denoted by S_∞. The set S_∞ is empty if and only if K is a function field. The similarity between (0.10) and (0.11) suggests the following definition. Let $S \supset S_\infty$ be a non-empty set of primes of the global field K. We define a subring A_S of K by

$$(0.12) \qquad A_S = \bigcap_{p \notin S} \mathcal{O}_p .$$

We will call S the set of *primes at infinity* for A_S. Rings of integers of algebraic number fields are examples of rings of this form. In this case the set of primes at infinity is equal to S_∞.

If K is a number field and $S \neq S_\infty$ we encounter rings that we did not consider before. For example if $K = \mathbb{Q}$ there is one archimedean prime, denoted by ∞. If we take $S = \{2,\infty\}$ we get

$$A_S = \mathbb{Z}[\tfrac{1}{2}] = \{\frac{a}{2^n} \in \mathbb{Q} : a \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\}.$$

Let p be a non-archimedean prime of the global field K. The residue class field $\mathcal{O}_p/p$ is a finite field. Its cardinality is called the *norm* of p:

$$(0.13) \qquad Np = \#\mathcal{O}_p/p.$$

If the prime p is not in S it corresponds to a prime ideal $p \cap A_S$ of A_S. We will denote this prime ideal by p too if no confusion arises. Every prime ideal $\neq 0$ of A_S is of this form and different primes correspond to different prime ideals. We have $\#A_S/p = Np$.

The *norm* of an A_S-ideal a is defined by

$$(0.14) \qquad Na = \#A_S/a.$$

This definition agrees with the definition of the norm of a prime $p \notin S$. The norm of an element $\alpha \in A_S$ is given by

(0.15) $N(\alpha) = N(\alpha A_S)$ if $\alpha \neq 0$;
$N(0) = 0.$

This agrees with (0.2). By multiplicativity we can extend the norm to all of K. Notice that for different choices of S we get different norm functions. Because we usually deal with only one set S this will not lead to confusion.

We give some examples. If $K = \mathbb{Q}$ and $S = S_\infty$ we have $A_S = \mathbb{Z}$. In this case the norm function is equal to the ordinary absolute value. If we take $S = \{\infty, 2\}$ we get $A_S = \mathbb{Z}[\frac{1}{2}]$. Each element of $\mathbb{Q}^*$ can be written as $\frac{a}{b}2^r$ with $a,b,r \in \mathbb{Z}$ and a,b odd. For $S = \{\infty, 2\}$ we have $N(\frac{a}{b}2^r) = |\frac{a}{b}|$.

If $K = \mathbb{F}_q(t)$ and $S = \{\infty\}$ we have $A_S = \mathbb{F}_q[t]$. In this case the norm is given by $N(f) = q^{\deg(f)}$ if $f \in \mathbb{F}_q[t]$.

Finally suppose that $K = \mathbb{F}_q(t,u)$ with $u^2 + u = t^3 + t + 1$. If S consists of the unique prime of degree 1 we have $A_S = \mathbb{F}_q[t,u]$, cf. section (0.3). Let $f \neq 0$ be an element of A_S. We may write $f = g + u \cdot h$. with $g,h \in \mathbb{F}_q[t]$. the norm of f is equal to $\max\{q^{2\deg(g)}, q^{3+2\deg(h)}\}$, where we take $\deg(0)$ to be $-\infty$.

§(0.5) The main theorems

We consider a ring A_S as defined by (0.12). It is called *Euclidean* if the following condition holds. cf. (0.1), (0.3):

(0.16) For any $a,b \in A_S$, with $b \neq 0$, there exist $q,r \in A_S$ such that $a = qb + r$ and $N(r) < N(b)$.

In the determination of Euclidean subrings of global fields we may restrict our attention to rings of the form A_S. In fact other subrings with the same quotient field cannot be Euclidean, cf. [W] 4-1-1.

The rings that were considered by Davenport and Armitage, cf. sections (0.2) and (0.3), all have $\#S = 2$. In this thesis we consider all rings with $\#S \leq 2$. We distinguish the different cases with $\#S \leq 2$ according to the set S_∞ of archimedean primes in S. This gives the following complete list:

(0.17) If $\#S = 1$:

(F) K is a function field, $S = \{p\}$;

(#1) $K = \mathbb{Q}$, $S = S_\infty$;

(#2) $K = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta < 0$, $S = S_\infty$.

If $\#S = 2$:

(F) K is a function field, $S = \{p,q\}$;

(#1) $K = \mathbb{Q}$, $S = \{\infty,p\}$;

(#2$^+$) $K = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta > 0$, $S = S_\infty$ consists of two real primes;

(#2$^-$) $K = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta < 0$, $S = \{\infty,p\}$;

(#3) $[K : \mathbb{Q}] = 3$, $S = S_\infty$ consists of one real and one complex prime;

(#4) $[K : \mathbb{Q}] = 4$, $S = S_\infty$ consists of two complex primes.

Throughout this thesis we will use the symbols at the left to distinguish between the different cases. In (0.17) the letters p and q always denote non-archimedean primes. If S_∞ consists of one prime we denote it by ∞.

In this thesis we investigate whether a given ring of the form A_S, with $\#S \leq 2$, is Euclidean. The following two theorems state what we shall prove.

<u>THEOREM (0.18)</u>. *Suppose that* $\#S = 1$. *Then the ring* A_S *is Euclidean if and only if we are in one of the following cases:*

(F) K *has genus* 0 *and* $S = \{p\}$, *with* p *a prime of degree* 1;

(#1) $K = \mathbb{Q}$;

(#2) $K = \mathbb{Q}(\sqrt{\Delta})$ *with* $\Delta \in \{-3,-4,-7,-8,-11\}$.

For the case (F) we have $g(K) = 0$ and $\deg(p) = 1$ if and only if $A_S \simeq \mathbb{F}_q[t]$. The 'if' part of (F) can be found in [vdW] §17. The 'only if' part will be proven in section (4.1). The results about the cases (#1) : $A_S = \mathbb{Z}$ and (#2) : $A_S = \mathbb{Z}[\frac{1}{2}(\Delta + \sqrt{\Delta})]$ were already proven by Euclid, Dedekind and Dickson, cf. sections (0.1) and (0.2).

<u>THEOREM (0.19)</u>. *Suppose that* $\#S = 2$. *Then the ring* A_S *is Euclidean if and only if we are in one of the following cases:*

(F) K *has genus* 0 *and* $S = \{p,q\}$ *with* $\gcd(\deg(p), \deg(q)) = 1$;

(#1) $K = \mathbb{Q}$;

(#2$^+$) $K = \mathbb{Q}(\sqrt{\Delta})$ *with* $\Delta \in \{5,8,12,13,17,21,24,28,29,33,37,41,44,57,73,76\}$;

(#2$^-$) $K = \mathbb{Q}(\sqrt{\Delta})$, $S = \{\infty,p\}$ *with* $\Delta \in \{-3,-4,-7,-8,-11\}$ *and any non-archimedean* p, *or* $\Delta \in \{-15,-20\}$ *and any non-archimedean* p *that is non-principal as an* $O(K)$*-ideal, or* (Δ, Np) *is one of the 38 pairs listed in table 1;*

(#3) K *is contained in a finite list of fields, all of which have discriminant* $0 > \Delta(K) \geq -170520$;

(#4) K *is contained in a finite list of fields, all of which have discriminant* $0 < \Delta(K) \leq 230202117$.

TABLE 1. Euclidean rings A_S in imaginary quadratic number fields $\mathbb{Q}(\sqrt{\Delta})$, with $S = S_\infty \cup \{p\}$.

Δ	Np	Δ	Np
−19	4	−39	2
−23	2, 3, 13, 29, 31, 41, 47, 71, 73, 127, 131, 163, 193, 233, 239, 257, 353, 443, 481	−40	2
		−47	2, 3
		−55	2
		−71	2, 3
−24	2, 5, 29	−79	2
−31	2, 5, 7	−87	2
−35	5, 7	−111	2

The proof of (0.19) occupies the greater part of this thesis. In section (1.3) we state two theorems (1.9) and (1.10) that are supplements to (0.18) and (0.19). In that section we also mention where the proofs of the different parts of (0.19) are to be found.

§(0.6) History of the determination of Euclidean rings

Euclid proved that $\mathbb{Z}$ is Euclidean. The next ring that was proven to be Euclidean was $\mathbb{R}[X]$. The proof was given by Simon Stevin in problème LIII of [Sv]. After this the first rings that were proven to be Euclidean were cyclotomic rings. Gauss was the first who proved that two of these rings, viz. $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[i] = \mathbb{Z}[\zeta_4]$, are Euclidean, cf. [G3] §§41-45; [G2]. In his paper on quadratic forms over $\mathbb{Z}[i]$ of 1842 Dirichlet also gave a proof that $\mathbb{Z}[i]$ is Euclidean, [D1] §2. In 1844, in two letters to Kronecker [K], Kummer proved that $\mathbb{Z}[\zeta_5]$ is Euclidean and that his method would apply to $\mathbb{Z}[\zeta_7]$ as well. Sixty-five years later, before these letters were published, Ouspensky [O] also proved that $\mathbb{Z}[\zeta_5]$ is Euclidean. A proof that $\mathbb{Z}[\zeta_8]$ is Euclidean was given in 1850 by Eisenstein [Ei]. Since for odd n we have $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_{2n}]$ this shows that $\mathbb{Z}[\zeta_n]$ is Euclidean for all $n \leq 8$.

Until 1975 no other cyclotomic rings were proven to be Euclidean. In that year Masley [M1] proved that $\mathbb{Z}[\zeta_{12}]$ is Euclidean. This was the last cyclotomic ring with degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq 4$ to be treated. In the same year Lenstra [L2] proved that $\mathbb{Z}[\zeta_n]$ is Euclidean for $n \in \{7,9,11,15,20\}$. The last two cyclotomic rings that are proven to be Euclidean are $\mathbb{Z}[\zeta_{16}]$ an $\mathbb{Z}[\zeta_{24}]$. The proof for $\mathbb{Z}[\zeta_{16}]$ was given by Ojala [Oj] in 1977 and the proof for $\mathbb{Z}[\zeta_{24}]$ was given by Lenstra [L4] in 1978. These results show that $\mathbb{Z}[\zeta_n]$ is Euclidean whenever the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is at most 10.

There are however more cyclotomic rings that have unique factorization. In fact Masley and Montgomerey [MM] proved in 1976 that for $n \not\equiv 2 \bmod 4$ the ring $\mathbb{Z}[\zeta_n]$ has unique factorization if and only if $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq 20$ or $n \in \{35,45,84\}$. Among these there are possibly more rings that can be proven to be Euclidean. In chapter 10 we give a list of all cyclotomic rings that may be Euclidean, cf. (10.5).

Now we will turn our attention to rings of integers of quadratic fields. These rings are mentioned in (0.18)(#2) and (0.19)(#2$^+$). Several methods for determining the Euclidean rings among them are important for the rest of this thesis. In section (0.2) we mentioned that the Euclidean rings of integers of imaginary quadratic fields were determined by Dedekind and Dickson ([D3] sup XI §159; [Di] Kap. VIII §93 satz 7). For the rest of this section we only consider *real* quadratic fields.

The proof that the rings asserted to be Euclidean are in fact Euclidean constituted the easiest part of the work. The proof given by Hardy and Wright in [HW] §14.8 are models for most other proofs. Hardy and Wright's arguments are essentially those of Oppenheim [Op]. Remak [R1; R2] supplies pictures illustrating the method. In section (5.5) two proofs of this sort are given.

The first values of Δ for which a proof was given that $\mathbb{Z}[\frac{1}{2}(\Delta + \sqrt{\Delta})]$ is Euclidean are 5,8,12 and 13. This was done by Dedekind [D3] Sup XI

§159, as we have seen in section (0.2). In 1933 Perron [P] proved that we may enlarge this list of Δ's with 17,21,24,28,29 and 44. Oppenheim [Op] and Remak [R2] proved independently in 1934 that also 33,37 and 41 are values of Δ for which the ring is Euclidean. The proof that the ring is Euclidean for $\Delta = 57$ was supplied by Hofreiter [Ho] and for $\Delta = 76$ by Berg [Be]. These proofs were given in 1935. A more detailed proof for $\Delta = 76$ was given by Behrbohm and Rēdei [BR]. The list of (0.19) (#2^+) was completed by Rēdei [Rē3] who proved in 1942 that also for $\Delta = 73$ the ring is Euclidean. In the same paper Rēdei stated, without proof, that for $\Delta = 97$ the ring is Euclidean as well. Later Barnes and Swinnerton-Dyer [BSD1] showed that this statement is false: the ring is not Euclidean.

The proof that the other rings are not Euclidean was much harder. It proceeded in several stages. Using the theory of genera of Gauss, cf. [G1] §§230-287; [D3] sup IV; [H1] ch. 26 §8, Behrbohm and Rēdei [BR] showed that $\mathbb{Z}[\frac{1}{2}(\Delta+\sqrt{\Delta})]$ has unique factorization only if Δ has at most two different prime factors. In particular this restriction on Δ must hold for Euclidean rings.

The first proofs that rings are not Euclidean are of an *arithmetical* kind. As we will see below these proofs were not as successful as the *geometrical* proofs that were supplied later.

The arithmetical proofs all run as follows. Let Δ be a discriminant for which it is to be proved that $\mathcal{O} = \mathbb{Z}[\frac{1}{2}(\Delta+\sqrt{\Delta})]$ is not Euclidean. For the special choice of $b = \sqrt{\Delta} \in \mathcal{O}$ the existence of $a \in \mathcal{O}$ such that the division of (0.3) is impossible is proven. In many cases this element a is constructed from quadratic residues mod Δ with special properties. Prime and composite Δ and Δ in different residue classes mod 24 have to be treated seperately. The existence of the quadratic residues with the required properties is proven for large Δ with analytic methods. For certain small Δ they are explicitly constructed. The proof, given by Hardy and Wright in [HW] §14.9 thm. 249 for $\Delta \not\equiv 1 \bmod 4$ is of this form. They used the proof of Berg [Be].

Oppenheim [Op] used in 1934 the arithmetical method to show that for $\Delta \in \{53,92,124\}$ the ring is not Euclidean. Independently in 1935 Fox Keston [F] and Berg [Be] proved that for even Δ the Euclidean rings are those that are listed in (0.19)(#2^+). In the same year Hofreiter [Ho] showed that there does not exist a Euclidean ring with (composite) $\Delta \equiv 21 \bmod 24$ and $\Delta > 21$. Also for $\Delta = 77$ he proved that the ring is not Euclidean. The rings with composite discriminant $\Delta \equiv 5,13 \bmod 24$ were treated by Behrbohm and Rédei [BR]. They showed that there are no Euclidean rings in this case. Also they showed that for prime $\Delta \equiv 5 \bmod 24$ the only Euclidean rings occur for $\Delta = 5$ and $\Delta = 29$.

In 1938 Erdös and Chao Ko [ECK] proved that there exists an upper bound on Δ for Euclidean rings with prime $\Delta \equiv 13 \bmod 24$. In the same year Heilbronn [He] proved the existence of an upper bound on Δ for all Euclidean rings $\mathbb{Z}[\frac{1}{2}(\Delta+\sqrt{\Delta})]$. These upper bounds were not explicitly computed, but at least it followed that there are only finitely many rings of this form. Schuster [Sc] computed such upper bounds for the remaning cases with composite Δ, except for $\Delta \equiv 1 \bmod 24$. He proved that for composite odd Δ the ring can be Euclidean only if $\Delta = 33$, $\Delta = 57$, or $\Delta \equiv 1 \bmod 24$ and $\Delta > 10000$.

Using the method of Erdös and Chao Ko, Brauer [Br] computed an upper bound equal to 3300000 for prime $\Delta \equiv 13 \bmod 24$. If in addition 5,7,11 or 13 is a quadratic residue mod Δ he got better bounds. With the help of his mother and his wife he computed for the remaining $\Delta \equiv 13 \bmod 24$ with $109 < \Delta < 3300000$ that the ring $\mathbb{Z}[\frac{1}{2}(\Delta+\sqrt{\Delta})]$ is not Euclidean. So in this case only $\Delta = 61$ and $\Delta = 109$ remained uncertain.

From now on also geometrical methods were used. In the long run they were more effective than the arithmetical methods. A geometrical proof may be described as follows. In most proofs that rings are Euclidean one uses geometrical methods to show that (0.3) holds for pairs (a,b) in several sets, which are described in geometrical terms. Because these sets cover all pairs (a,b) the rings is Euclidean, cf. section (5.5). Suppose that for a given ring there remain sets of (a,b) for which this proof of (0.3) does not work, even when it is refined. Then by a limiting process we may find a pair (a,b) for which the division in (0.3) is impossible. Proofs of this kind will be used in chapter 5. The application of this method suggests us to look whether there exists $a \in \mathcal{O}$ such that the division in (0.3) is impossible for $b = \eta \pm 1$, where η is a fundamental unit of $\mathcal{O}$, cf. sections (1.1), (5.1), (7.1).

Rédei was the first who used a geometrical method. He proved in 1941 that for $\Delta = 61$ and $\Delta = 109$ the ring is not Euclidean. Also for composite $\Delta \equiv 1 \bmod 24$ and prime $\Delta \equiv 17 \bmod 41$, $\Delta > 41$ he showed that the rings are not Euclidean, cf. [Ré1; Ré2; Ré3].

Using the arithmetical method Hua [Hu] managed in 1944 to prove that there exists an absolute upper bound equal to e^{250} for the discriminant of Euclidean rings. Independently of Rédei he proved, together with

Min [HM] that for prime $\Delta \equiv 17 \bmod 24$, $\Delta > 137$ the ring is not Euclidean. Together with Shih [HS] he proved that the ring is not Euclidean for $\Delta = 61$.

In 1947 Inkeri [In] used a geometrical method to prove that the only unknown Euclidean rings must have $\Delta > 5000$. Davenport [Da1, Da5] used in 1948 a geometrical method to show that all Euclidean rings have $\Delta < 16384$. Apparently unaware of Inkeri's work Chatland [Ch] used Davenport's results to show that a Euclidean ring must have $\Delta \leq 601$. In a joint paper with Davenport [CD] he finished the determination, not using Inkeri's results.

As we have seen above the geometrical method was more successful in supplying upper bounds and finishing the proof than the arithmetical approach was. In fact most authors using the geometrical method proved many results already known with less effort. For example in the papers of Cassels [C1] and Ennola [E] we find a proof not relying on restrictions obtained by arithmetical means. The fact that the geometrical and the arithmetical methods are of a different nature can be illustrated as follows. If we generalize the methods for higher degree number fields it turns out that the arithmetical methods are applicable for extensions of $\mathbb{Q}$ in which at least one prime is totally ramified, cf. [Ci], and the geometrical methods apply for fields with $\#S_\infty \leq 2$.

CHAPTER I EUCLIDEAN IDEAL CLASSES

§(1.1) Elementary properties of the ring A_S.

In this chapter we study the subrings A_S of global fields K defined in (0.12). Usually we only deal with one ring of this form. In this case we will denote A_S by A.

A finitely generated, non-zero A-submodule of K is called a *fractional ideal* of A. Any non-zero A-ideal is a fractional ideal, and conversely for any fractional ideal $\mathfrak{a}$ of A there exists $\alpha \in K^*$ such that $\alpha\mathfrak{a}$ is a non-zero A-ideal. From now on we will call the non-zero A-ideals the *integral* A-ideals, reserving the word 'ideal' for fractional ideals. It can be shown that the set I of fractional A-ideals forms a group with respect to the usual ideal product. The unit element of I equals A and the inverse of a fractional ideal $\mathfrak{a}$ equals $\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subset A\}$. The ideal group I is freely generated by the set of non-zero prime ideals of A, cf. [La2] ch. I §6, thm. 2.

A fractional ideal of the form αA for some $\alpha \in K^*$ is called a *principal ideal*. The set P of all principal ideals is a subgroup of I. The quotient group $Cl(A) = I/P$ is called the *class group* of A. It is a finite group, cf. [W] 5-3-11. The order h(A) of Cl(A) is called the *class number* of A. The residue classes of I mod P are called the *ideal classes* of A. The ideal class of $\mathfrak{a}$ will be denoted by $[\mathfrak{a}]$.

If K is a number field and $S = S_\infty$, i.e. $A = \mathcal{O}$, then Cl(A) and h(A) are equal to the class group Cl(K) and the class number h(K) of K respectively.

Let $\mathfrak{p}$ be a prime of a global field K. The field K is not complete in the topology determined by $\mathfrak{p}$, cf. section (0.4). The completion of K in this topology will be denoted by $K_\mathfrak{p}$. This is a field, and each field of this form will be called a *local field*. By continuity we extend each valuation in $\mathfrak{p}$ to a valuation of $K_\mathfrak{p}$. The only archimedean local fields are $\mathbb{R}$ and $\mathbb{C}$, cf. [W] 1-8. If $\mathfrak{p}$ corresponds to an embedding of K in $\mathbb{R}$ we have $K_\mathfrak{p} \simeq \mathbb{R}$, then we call $\mathfrak{p}$ a *real* prime. If $\mathfrak{p}$

corresponds to a pair of complex conjugate embeddings of K in $\mathbb{C}$ we have $K_p \simeq \mathbb{C}$, then we call p a *complex* prime.

For a non-archimedean local field K_p, the valuation ring will be denoted by $\tilde{O}_p$, and its maximal ideal by $\tilde{p}$, cf. (0.8) and (0.9). The residue class field $\tilde{O}_p/\tilde{p}$ is isomorphic to the field O_p/p. In particular we have $Np = \#\tilde{O}_p/\tilde{p}$, cf. (0.13). We have $K = \bigcup_{n\in\mathbb{Z}} \tilde{p}^n$. We define the *order function* ord_p on K_p by

(1.1) $$\mathrm{ord}_p(x) = n \quad \text{if} \quad x \in \tilde{p}^n - \tilde{p}^{n+1}; \qquad \mathrm{ord}_p(0) = \infty$$

Using the multiplicativity of the valuations, cf. (0.7), we derive that every valuation in p is of the form $\gamma^{\mathrm{ord}_p(\cdot)}$ for some γ with $0 < \gamma < 1$. The *normalized valuation* $|\cdot|_p$ on K_p is defined as follows.

(1.2) (a) If p is non-archimedean then $|x|_p = Np^{-\mathrm{ord}_p(x)}$;

(b) If p is real, then $|x|_p = |x|$, the usual absolute value on $\mathbb{R}$;

(c) If p is complex, then $|x|_p = |x|^2$, the *square* of the usual absolute value on $\mathbb{C}$.

For all p the field K is a subfield of K_p, hence the normalized valuations are also defined on K. These normalized valuations satisfy a *product formula* ([W] prop. 5-1-2; [Iy] ch. III §6.2 cor.; [H1] ch. 20 IV), which reads as follows. For all $\alpha \in K$, $\alpha \neq 0$ we have $|\alpha|_p = 1$ for all but finitely many p and

(1.3) $$\prod_p |\alpha|_p = 1,$$

where the product runs over all primes of K. We use this product formula to get an expression for the norm, different from its definition, cf. (0.2), (0.15). For each principal fractional ideal αA of A we have

(1.4) $$\alpha A = \prod_{p\notin S} p^{\mathrm{ord}_p(\alpha)}.$$

Using the multiplicativity of the norm we get from (1.2)(a), (1.4) and (1.3):

(1.5) $$N(\alpha) = \prod_{p\notin S} |\alpha|_p^{-1} = \prod_{p\in S} |\alpha|_p.$$

The equality $N(\alpha) = \prod_{p\in S}|\alpha|_p$ even holds trivially for $\alpha = 0$.

As an analogue of (1.4) we define for an arbitrary A-ideal $\mathfrak{a}$ the order at a prime $p \notin S$ by

$$(1.6) \qquad \mathfrak{a} = \prod_{p\notin S} p^{\operatorname{ord}_p(\mathfrak{a})}.$$

Suppose that K is a number field, and $S = S_\infty$. The classical definition of the norm of an element is given by

$$(1.7) \qquad \mathcal{N}(\alpha) = \prod \varphi(\alpha)\ ,$$

where the product runs over the different embeddings $\varphi : K \to \mathbb{C}$, cf. [vdW] §47. Combining (1.2)(b), (c) and (1.5) we see that $\mathcal{N}(\alpha)$ equals $N(\alpha)$ up to sign.

From the definition of the norm (0.15) we derive that the unit group A^* of A equals the set of elements of A with norm equal to 1. By the Dirichlet-Hasse unit theorem ([CF] ch. II §18; [W] 5-3-10; [La2] ch.V §1, p. 105) the group A^* is isomorphic to $W \times \mathbb{Z}^{s-1}$, where $s = \#S$ and W equals the group of *roots of unity* of K. In particular when $\#S = 2$ the quotient A^*/W is isomorphic to $\mathbb{Z}$. In this case any unit $\eta \in A^*$ that generates A^* mod W is called a *fundamental unit* of A.

§(1.2) The definition of Euclidean ideal class

In this section we generalize the notion of 'Euclidean ring' to that of 'ring with Euclidean ideal class'. Below we will see that the rings of integers of $\mathbb{Q}(\sqrt{-15})$ and $\mathbb{Q}(\sqrt{-20})$ have a Euclidean ideal class. In section (2.2) we will see that this explains the occurrence of the Euclidean rings with $\Delta \in \{-15,-20\}$ in (0.19) ($\#2^-$)

The definition of a Euclidean ideal class is due to Lenstra [L5]. We shall recall this definition to our special case, i.e. to subrings of the form A_S of a global field, and for the norm function.

Let $\mathfrak{a}$ be an A-ideal. We call $\mathfrak{a}$ a *Euclidean ideal* (for the norm) if the following condition is satisfied.

(1.8) For each $\alpha \in K$ there exists $\gamma \in \mathfrak{a}$ such that $N(\alpha-\gamma) < N\mathfrak{a}$.

Because the norm is multiplicative this condition only depends on the ideal class of $\mathfrak{a}$. The ideal class of a Euclidean ideal will be called a *Euclidean ideal class*. By comparing (0.16) and (1.8) we see that A is a Euclidean ring if and only if the principal ideal class $[A]$ is Euclidean. This shows that the notion of 'Euclidean ideal class' is only novel for non-principal classes. As an illustration we show that the rings of integers of the fields $\mathbb{Q}(\sqrt{-15})$ and $\mathbb{Q}(\sqrt{-20})$ have a non-principal Euclidean ideal class.

If $K = \mathbb{Q}(\sqrt{-15})$ we have $\mathcal{O} = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-15})]$. We show that $\mathfrak{a} = \mathbb{Z}\cdot 2 + \mathbb{Z}\cdot\frac{1}{2}(1+\sqrt{-15})$ is a Euclidean ideal. The norm of $\mathfrak{a}$ equals 2. We denote the archimedean prime of K by ∞. Through the embedding $K \subset \mathbb{C} = K_\infty$

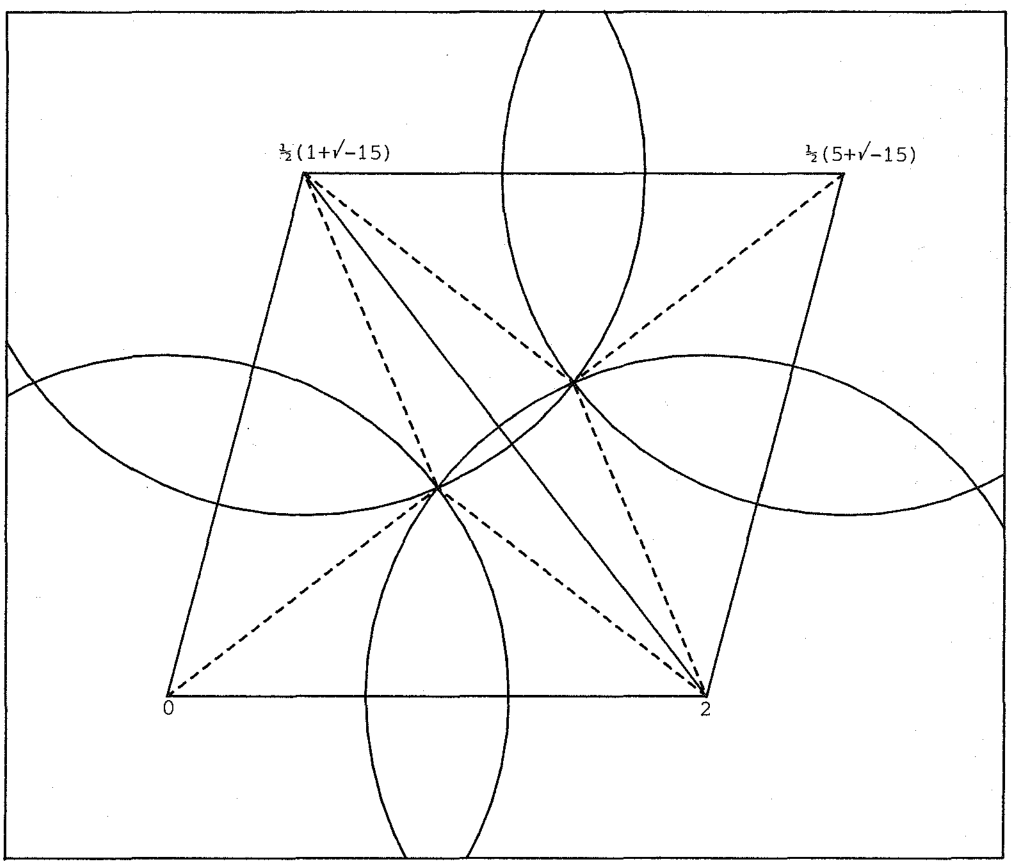


fig. 1

the norm equals $|\cdot|_\infty$, the square of the usual absolute value on $\mathbb{C}$, cf. (1.2) (c) and (1.5). The embedding $K \subset \mathbb{C}$ turns $\mathfrak{a}$ into a lattice of $\mathbb{C}$ for which the parallelogram with vertices 0, 2, $\frac{1}{2}(5+\sqrt{-15})$ and $\frac{1}{2}(1+\sqrt{-15})$ is a fundamental domain, see fig. 1. Let r be the radius of the circle through 0, 2 and $\frac{1}{2}(1+\sqrt{-15})$. It follows easily that for every $\alpha \in K$ there exists $\gamma \in \mathfrak{a}$ with $|\alpha - \gamma| \le r^2$. Since $r^2 = \frac{8}{5} < 2 = N\mathfrak{a}$, cf. (3.4), we derive that $\mathfrak{a}$ is Euclidean.

For $K = \mathbb{Q}(\sqrt{-20})$, we have $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. A similar argument as above shows that the ideal $\mathfrak{a} = \mathbb{Z}\cdot 2 + \mathbb{Z}(1+\sqrt{-5})$ is Euclidean, see fig. 2. In this case for every $\alpha \in K$ there exists $\gamma \in \mathfrak{a}$ such that $N(\alpha-\gamma) \le \frac{9}{5} < 2 = N\mathfrak{a}$.

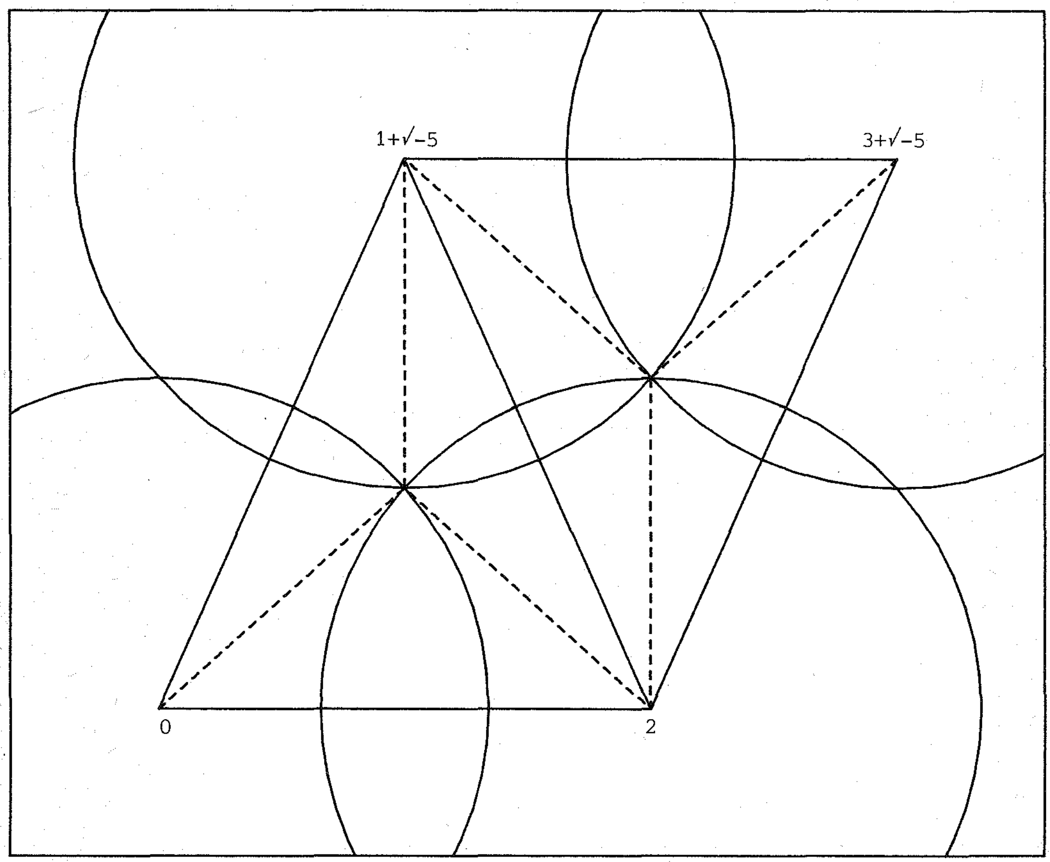


fig. 2

§(1.3) Rings with a Euclidean ideal class

In the course of proving (0.18) and (0.19) we will also obtain results on rings with a non-principal Euclidean ideal class. These results are stated in the following two theorems.

THEOREM (1.9). *Suppose that* $\#S = 1$. *Then the ring* A_S *has a non-principal Euclidean ideal class if and only if we are in one of the following cases:*

(F) K *has genus* 0, $S = \{p\}$ *with* $\deg(p) = h > 1$; *in this case the class group* $Cl(A_S)$ *is cyclic of order* h;

(#2) $K = \mathbb{Q}(\sqrt{\Delta})$ *with* $\Delta \in \{-15,-20\}$, $S = S_\infty$; *in this case the class number* $h(A_S) = h(K)$ *equals* 2.

In case (F) the structure of A_S is given by (0.6) (b), because $\deg(\infty) = 1$ we do *not* have $\infty \in S$. Theorems (0.18) (F) and (1.9) (F) show that for function fields and $\#S = 1$ the ring A has a Euclidean ideal class if and only if K has genus equal to 0, i.e. $K \simeq \mathbb{F}_q(t)$. The proof will be given in section (4.1).

The 'if' part of (1.9)(#2) was already proved in section (1.2). The 'only if' part will be dealt with in section (4.2).

THEOREM (1.10). *Suppose that* $\#S = 2$. *Then the ring* A_S *has a non-principal Euclidean ideal class if and only if we are in one of the following cases:*

(F) K *has genus* 0, $S = \{p,q\}$ *with* $\gcd(\deg(p),\deg(q)) = h > 1$; *in this case the class group* $Cl(A_S)$ *is cyclic of order* h;

($\#2^+$) $K = \mathbb{Q}(\sqrt{\Delta})$ *with* $\Delta \in \{40,60,85\}$, $S = S_\infty$; *in this case the class number* $h(A_S)$ *equals* 2;

($\#2^-$) $K = \mathbb{Q}(\sqrt{\Delta})$, $S = \{\infty,p\}$ *for* $\Delta \in \{-15,-20\}$ *and any* p *that is principal as an* $\mathcal{O}(K)$*-ideal, or for* (Δ, Np) *as listed in table* 2; *in this case the class number* $h(A_S)$ *equals* 2;

(#3) K *is contained in a finite list of fields, all of which have discriminant* $0 > \Delta(K) \geq -170520$; *in this case the class group is cyclic and* $2 \leq h(A_S) = h(K) \leq 4$;

(#4) K *is contained in a finite list of fields, all of which have discriminant* $0 < \Delta(K) \leq 230202117$; *in this case the class group is cyclic and* $2 \leq h(A_S) = h(K) \leq 6$.

TABLE 2. Subrings A_S of imaginary quadratic fields $\mathbb{Q}(\sqrt{\Delta})$, with $S = \{\infty, p\}$, which have a non-principal ideal class.

Δ	Np
-24	7
-35	4, 11
-56	2
-68	2
-84	2
-136	2

In case (F) the structure of A_S is given by (0.6) (b). Again we cannot have $\infty \in S$. The combination of (0.19) (F) and (1.10) (F) shows that when K is a function field and $\#S = 2$ the ring A_S has a Euclidean ideal class if and only if the genus of K equals 0.

We indicate where the proofs of (0.19) and (1.10) can be found. For case (F) the 'if' part will be proved in theorem (4.4). The 'only if' part will be proved in theorem (5.19)(F). The facts about the class group follow from theorem (4.6).

Case (#1) of (0.19) is a direct consequence of (0.18) (#1) and (2.8). For part (#2^+) the result of (0.19) was proven by Chatland and Davenport [CD], cf. section (0.6). The result of (1.10) will be proven in section (5.5).

The part of case (#2^-) which asserts that for $\Delta \in \{-3,-4,-7,-8,-11, -15,-20\}$ any subring A_S with $\#S = 2$ has a Eulicean ideal class will be proven in section (2.2). The rest of the proofs for this case occupies the chapters 5-9.

The discriminant bounds in the cases (#3) and (#4) will be derived in (5.19) (#3) and (#4). The fact that $Cl(A_S)$ is cyclic will be proven in (2.5). The bounds on the class number will be derived in section (10.1). In the rest of chapter 10 we derive further conditions that rings with a Euclidean ideal class in the cases (#3) or (#4) must satisfy.

It is easily checked that in case (#2^-) with $\Delta \in \{-15,-20\}$ the ring A_S is principal if and only if Np is *not* a quadratic residue mod 5, including $Np = 5$ when $\Delta = -15$.

§(1.4) Large sets of infinite primes

For $^\#S > 2$ the obvious generalizations of (0.18), (0.19), (1.9) and (1.10) do not hold. We give two examples to support this.

First we consider number fields. In this section we call a ring A_S *minimal* if it has a Euclidean ideal class and $A_{S'}$ has no Euclidean ideal class for any proper subset S' of S, containing S_∞. From (0.18), (0.19), (1.9) and (1.10) we deduce that for $^\#S \le 2$ the number of minimal A_S is finite up to isomorphism. This does not hold for $^\#S \le n$ with $n \ge 3$ as is shown by the following example.

The ring of integers $\mathcal{O} = \mathbb{Z}[\sqrt{14}]$ of $K = \mathbb{Q}(\sqrt{56})$ is a principal ideal domain but it is not Euclidean. This can be proven by checking (0.16) for $b = 2$ and $a = 1+\sqrt{14}$ as follows. If $\mathcal{O}$ is Euclidean there must be $U,V \in \mathbb{Z}$ with $U \equiv V \equiv 1 \bmod 2$ and $N(U+V\sqrt{14}) < 4$. Since $N(U+V\sqrt{14}) = |U^2-14V^2|$ we must have $U^2-14V^2 \in \{\pm1,\pm3\}$. By reducing mod 4 we see that $U^2-14V^2 \in \{1,-3\}$ is not possible. By reducing mod 7 we see that $U^2-14V^2 \in \{-1,3\}$ is not possible. Hence $\mathcal{O}$ is not Euclidean (see also (0.19) ($\#2^+$)). Now we consider the rings A_S with $S = S_\infty \cup \{p\}$ for some non-archimedean prime p of K. If p, as an $\mathcal{O}$-ideal, is generated by an element $\pi \not\equiv 1 \bmod 2$ then the ring A_S is Euclidean. This can be derived from the fact that the so called second inhomogeneous minimum of X^2-14Y^2 is smaller than 1, cf. [BSD1; BSD2]. By the Čebotarev-density theorem, cf. [Č], [La2] ch. VIII §4; [CF] ch. VIII §2 thm. 4, there are infinitely many prime ideals p for which $\pi \not\equiv 1 \bmod 2$. Hence for $K = \mathbb{Q}(\sqrt{56})$ there are already infinitely many minimal rings with $^\#S = 3$.

Now we consider function fields. For $^\#S \le 2$ we found that whether a ring has a Euclidean ideal class only depends on the genus of the field, i.e. $g(K) = 0$. This does not hold for $^\#S = 3$ any more. We give an example of a field with genus equal to 1 and for which A_S has a Euclidean ideal class for some, but not all sets S with $^\#S = 3$.

We take $K = \mathbb{F}_2(t,u)$ with $u^2+u = t^3+t+1$. We encountered this field already in section (0.2) and (0.4). It can be shown that the genus of K is equal to 1. We saw that K has only one prime ∞ of degree 1 and that $A_{\{\infty\}} = \mathbb{F}_2[t,u]$. It is a principal ideal domain, cf. [Q] thm. 3. Let p and q be the two primes of degree 2 of K. As $\mathbb{F}_2[t,u]$-ideals they are generated by t and $t+1$ respectively. From [L1] thm. (16.1) we conclude that A_S is Euclidean for $S = \{p,q,\infty\}$.

Let $\mathfrak{r}$ be the prime of K that as an $\mathbb{F}_2[t,u]$-ideal is generated by t^2+t+1. It is a prime of degree 4. Put $S=\{\mathfrak{p},\mathfrak{r},\infty\}$. We show that the principal ideal domain A_S, cf. (2.7), is not Euclidean. Every unit ε of A_S is a product of powers of t and of t^2+t+1, hence $\varepsilon\equiv 1 \bmod \mathfrak{q}$, where $\mathfrak{q}$ is regarded as an A_S-ideal. Because $\mathbb{F}_2[t,u]$ does not contain an element of norm 2 the ring A_S does not contain an element of norm 2 either. Let $\alpha\in A_S$ be such that $\alpha\equiv u \bmod \mathfrak{q}$. Then $\alpha\not\equiv 1 \bmod \mathfrak{q}$ so α is not a unit of A_S, and $N(\alpha)\neq 1$. Also $N(\alpha)\neq 2$ as we just have seen Hence $N(\alpha)\geq 4=N\mathfrak{q}$. This shows that A_S is not Euclidean.

CHAPTER 2 PROPERTIES OF RINGS WITH EUCLIDEAN IDEAL CLASSES

In this chapter we investigate the properties of the class group of a ring with a Euclidean ideal class. We denote by S a non-empty set of primes of K defined by (0.12). If no confusion arises we simply write A instead of A_S.

Most results of this chapter can also be found in [L5].

§(2.1) Connections with the class group

As we have seen in section (1.2) the existence of a Euclidean ideal class of A does not imply that $h(A) = 1$. In this section we show that a ring A has at most one Euclidean ideal class. Also we find that a Euclidean ideal class generates the class group.

LEMMA (2.1). *Suppose that* $[\mathfrak{c}]$ *is a Euclidean ideal class of* A. *Then for every integral* A*-ideal* $\mathfrak{a} \neq A$ *there exists an integral* A*-ideal* $\mathfrak{b}$ *with* $[\mathfrak{a}] = [\mathfrak{b}\mathfrak{c}]$, $N\mathfrak{b} < N\mathfrak{a}$ *and* $\mathfrak{a} + \mathfrak{b} = A$.

PROOF. By the strong approximation theorem ([CF], ch.II, §15) there exists $y \in \mathfrak{c}\mathfrak{a}^{-1}$ with $y \notin \mathfrak{c}$ such that $yA + \mathfrak{c} = \mathfrak{c}\mathfrak{a}^{-1}$. Because $\mathfrak{c}$ is Euclidean there exists $x \in y + \mathfrak{c}$ with $N(x) < N\mathfrak{c}$. If we take $\mathfrak{b} = x\mathfrak{a}\mathfrak{c}^{-1}$ we get $[\mathfrak{a}] = [\mathfrak{b}\mathfrak{c}]$, $N\mathfrak{b} < N\mathfrak{a}$ and $\mathfrak{a} + \mathfrak{b} = A$. □

COROLLARY (2.2). *Let* $[\mathfrak{c}]$ *be a Euclidean ideal class of* A. *Then for every integral* A*-ideal* $\mathfrak{a} \neq A$ *there exists* $n \in \mathbb{Z}$ *with* $0 < n < N\mathfrak{a}$ *and* $[\mathfrak{a}] = [\mathfrak{c}]^n$.

PROOF. Use induction on $N\mathfrak{a}$ in lemma (2.1). □

COROLLARY (2.3). *Let* $[\mathfrak{c}]$ *be a Euclidean ideal class of* A. *Then every integral* A*-ideal* $\mathfrak{a}$ *with* $N\mathfrak{a} = \min\{N\mathfrak{b} : \mathfrak{b}$ integral A-ideal, $\mathfrak{b} \neq A\}$ *is contained in* $[\mathfrak{c}]$.

PROOF. For any integral $\mathfrak{a} \neq A$ with minimal norm, the ideal $\mathfrak{b}$ of (2.1) must be equal to A. □

COROLLARY (2.4). *Each ring* A *has at most one Euclidean ideal class.*

PROOF. If $\mathfrak{a} \neq A$ is an integral ideal of minimal norm then by (2.3) the Euclidean ideal class must be equal to $[\mathfrak{a}]$. □

We combine the results above to get the following theorem.

THEOREM (2.5). *Let* $[\mathfrak{c}]$ *be a Euclidean ideal class of the ring* A. *Then* $[\mathfrak{c}]$ *is a generator of* Cl(A). *Moreover the class number* h(A) *satisfies*

$$h(A) < \min\{N(\alpha) : \alpha \in A,\ \ N(\alpha) > 1\}.$$

PROOF. Corollary (2.2) implies that $[\mathfrak{c}]$ is a generator of Cl(A). If $\alpha \in A$ with $N(\alpha) > 1$ we derive from (2.2) that $[A] = [\alpha A] = [\mathfrak{c}]^n$ for some n with $0 < n < N(\alpha)$. Hence the order of $[\mathfrak{c}]$, which equals h(A), is less than $N(\alpha)$. □

This theorem gives a new proof of the fact that a Euclidean ring is a principal ideal domain, because in that case the generator of the class group is trivial.

§(2.2) Enlarging the set of infinite primes

Throughout this section we consider two non-empty sets of primes $S \subset S'$ of K that contain S_∞. We denote $A_S = A$ and $A_{S'} = A'$. We show that when A has a Euclidean ideal class then also A' has a Euclidean ideal class. The ideal groups of A and A' will be denoted by I and I', and the norms with respect to A and A' by N and N', respectively.

The group I is generated as a free abelian group by the primes of K not in S and similarly the group I' is generated by the primes not in S'. There is a natural surjection $\varphi : I \to I'$, defined by $\varphi(\mathfrak{a}) = \mathfrak{a}A'$ for any $\mathfrak{a} \in I$. The kernel of φ is generated by the primes in $S' - S$. For an ideal $\mathfrak{a} \in I$ that does not contain prime factors in S' we have

$$N\mathfrak{a} = N'\varphi(\mathfrak{a}). \tag{2.6}$$

Since φ maps principal ideals to principal ideals it induces an exact sequence

$$(2.7)\qquad 0 \to \langle [p] \in \mathrm{Cl}(A) : p \in S' - S\rangle \to \mathrm{Cl}(A) \xrightarrow{\overline{\varphi}} \mathrm{Cl}(A') \to 0.$$

THEOREM (2.8). *Let* A *and* A' *be as defined above, and let* $[c]$ *be a Euclidean ideal class of* A. *Then* $\overline{\varphi}([c])$ *is a Euclidean ideal class of* A'.

PROOF. We have to show that for any $x \in K$ there exists $\xi \in \varphi(c)$ such that $N'(x-\xi) < N'\varphi(c)$. Using the strong approximation theorem ([CF], ch.II, §15) we find $y \in \varphi(c)$ such that

$$|x-y|_p \le Np^{-\mathrm{ord}_p(c)} \quad \text{for all} \quad p \in S' - S.$$

Since c is Euclidean, there exists $\gamma \in c$ with

$$N(x-y-\gamma) < Nc.$$

Because c is a subset of $\varphi(c)$ we have $\xi = y+\gamma \in \varphi(c)$. Since both

$$|x-y|_p \le Np^{-\mathrm{ord}_p(c)} \quad \text{and} \quad |\gamma|_p \le Np^{-\mathrm{ord}_p(c)} \quad \text{for} \quad p \in S'-S$$

we have

$$|x-\xi|_p \le Np^{-\mathrm{ord}_p(c)} \quad \text{for all} \quad p \in S' - S.$$

Using the product formula for the norm (1.5) we get

$$N'(x-\xi) = N(x-\xi) \prod_{p \in S'-S} |x-\xi|_p <$$

$$< Nc \prod_{p \in S'-S} Np^{-\mathrm{ord}_p(c)} = N'\varphi(c). \quad \square$$

The 'if' part of case $(\#2^-)$ of (0.19) and (1.10) for $\Delta \in \{-3,-4,-7,-8,-11,-15,-20\}$ now follows from case (#2) of (0.18) and (1.9). The value of the class number follows from the exact sequence (2.7). Also the 'if' part of case (F) of (0.19) and (1.10) now follows from case (F) of (0.18) and (1.9). The value of $h(A)$ in this case will be computed in section (4.1).

§(2.3) Restrictions on the class number

In this section we derive upper bounds for the class number of a ring with a Euclidean ideal class. For number fields and $S = S_\infty$ a trivial upper bound can be derived from (2.5). If $[K:\mathbb{Q}] = n$ we find that $h(\mathcal{O}) = h(K) < N(2) = 2^n$ if $\mathcal{O}$ has a Euclidean ideal class. A better upper bound is given by the following proposition.

PROPOSITION (2.9). *Let* $S \supset S_\infty$ *be a non-empty set of primes of the global field* K. *Let* $A = A_S$ *be the corresponding ring. Suppose that* $[c]$ *is a Euclidean ideal class of* A. *Let* P *denote the set of prime powers* $\neq 1$ *that occur as the norm of an integral* A-*ideal. Then for every integral* A-*ideal* $a \neq A$ *we have* $[a] = [c]^n$ *for some* $n \in \mathbb{Z}$ *with* $0 < n \leq \#\{q \in P : q \leq Na\}$. *Moreover*

$$h(A) \leq \#\{q \in P : q \leq N(\alpha) \text{ for all } \alpha \in A \text{ with } N(\alpha) > 1\}.$$

PROOF. For the first assertion we use induction on Na. First suppose that Na is a prime power. This includes the initial step. By (2.1) there exists an integral ideal b with $[a] = [bc]$ and $Nb < Na$. By induction we have $[b] = [c]^n$ for some n with $0 \leq n \leq \#\{q \in P : q \leq Nb\}$. Notice that we must include $n = 0$ for the case that $b = A$. Since Na is a prime power we have $n+1 \leq \#\{q \in P : q \leq Na\}$, and $[a] = [c]^{n+1}$, which proves the first assertion in this case.

If Na is not a prime power it is not a prime ideal. Hence there exists a decomposition $a = a_1 \cdot a_2$ in integral ideals with $Na_i < Na$. By induction we have $[a_i] = [c]^{n_i}$ for some $n_i \in \mathbb{Z}$ with

$$0 < n_i \leq \#\{q \in P : q \leq Na_i\}.$$

This shows that $[a] = [c]^{n_1+n_2}$. We will prove that $n_1 + n_2 \leq$ $\leq \#\{q \in P : q \leq Na\}$.

Let p be a prime number and let E_i be the set of p-powers in P that are $\leq Na_i$, for $i = 1,2$. The contribution of p-powers to n_i is exactly $\# E_i$. Let q_0 be the largest element of E_2. Every p-power of the form q, with $q \in E_2$, or of the form qq_0, with $q \in E_1$, is less than Na, and all these p-powers, which are in P, are different. So the contribution of p-powers to $\#\{q \in P : q \leq Na\}$ is at least

$\#E_1 + \#E_2$, which proves the first assertion.

The second assertion follows by taking for a an integral ideal αA such that $\alpha \in A$ is of least norm > 1. □

COROLLARY (2.10). *Let* K *be a function field over* $\mathbb{F}_q$. *Suppose that the subring* $A = A_S$ *has a Euclidean ideal class, then*

$$h(A) \leq \min\{\frac{\log N(\alpha)}{\log q} : \alpha \in A \text{ with } N(\alpha) > 1\}.$$

PROOF. Every element of P is a q-power. □

In section (4.1) we find that we have equality in (2.10) in the case that $g(K) = 0$.

Now suppose that K/K_0 is a Galois extension with group G. We call a set of primes of K G-*invariant* if for all $\sigma \in G$ we have $S = \{\sigma p : p \in S\}$. Analogously we call a prime p of K G-*invariant* if for all $\sigma \in G$ we have $\sigma p = p$.

PROPOSITION (2.11). *Suppose that* $K/\mathbb{Q}$ *is a Galois extension with group* G. *Let* $S \supset S_\infty$ *be a* G-*invariant set of primes of* K. *If* $A = A_S$ *has a Euclidean ideal class* $[c]$ *then* $h(A)$ *divides* $n = [K : \mathbb{Q}]$.

PROOF. From the definition (1.8) we derive that under G-action the Euclidean ideals are permuted. So the action of G on the class group is trivial by (2.3) and (2.4). So

$$[c]^n = \prod_{\sigma \in G} [\sigma c] = [Nc \cdot A] = [A],$$

i.e. $h(A) | n$. □

As an example we will compute an upper bound for the class numbers of subrings of quadratic number fields with a Euclidean ideal class. This bound is best possible.

PROPOSITION (2.12). *Let* K *be a quadratic number field and let* $S \supset S_\infty$ *be a set of primes of* K. *If* $A = A_S$ *has a Euclidean ideal class we have* $h(A) \leq 2$.

PROOF. Let q be the smallest prime power such that there exists an ideal $a \in A$ with $Na = q$ (if q does not exist then S consists of all primes of K, i.e. $A = K$ and $h(A) = 1$). Since a is an ideal of minimal norm, the Euclidean ideal class must be equal to $[\mathfrak{a}]$. Let p be the prime number dividing q, then $q = p$ or $q = p^2$. If $N(pA) = q$ we must have $pA = \mathfrak{a}$, so $\mathfrak{a}$ is principal, and $h(A) = 1$. In the other case we must have $N\mathfrak{a} = p$ and $N(pA) = p^2$. Then $pA = \mathfrak{a} \cdot \mathfrak{a}'$ for some ideal $\mathfrak{a}'$ of norm p. By the minimality of $N\mathfrak{a}$ and by (2.3) we have $[\mathfrak{a}] = [\mathfrak{a}']$. Hence $[pA] = [\mathfrak{a}]^2$, which shows that $h(A)|2$. □

Another proof can be given using (2.11) as follows. Let σ be the non-trivial automorphism of K. Take $S' = S \cup \sigma[S]$, then $A' = A_{S'}$ has a Euclidean ideal class by (2.8) and $h(A')|2$ by (2.11). The proposition is proven when we show that the map $\overline{\varphi}$ in (2.7) is an isomorphism. The kernel of $\overline{\varphi}$ is generated by the ideal classes of primes $\mathfrak{p} \in S' - S$. If $\mathfrak{p} \in S' - S$, then $\sigma\mathfrak{p} \in S$, which shows that $\mathfrak{p} = N\mathfrak{p} \cdot A$, i.e. $\mathfrak{p}$ is principal in A. Hence $\overline{\varphi}$ is an isomorphism. □

LEMMA (2.13). *Suppose that* $[K : \mathbb{Q}] = 2$ *and* $S = S_\infty \cup \{\mathfrak{p}\}$ *for some non-archimedean* $\mathfrak{p}$.
If $\Delta \equiv 1 \bmod 8$ *and* $N\mathfrak{p} = 2$ *we have* $h(A) = 1$.
If $\Delta \equiv 5 \bmod 24$ *and* $N\mathfrak{p} \neq 4$ *we have* $h(A) = 1$.
If $\Delta \equiv 13, 21 \bmod 24$ *and* $N\mathfrak{p} = 3$ *we have* $h(A) = 1$.

PROOF. In all cases the integral ideal of minimal norm > 1 is generated by 2 or 3 and thus it is principal. □

For fields of degrees 3 and 4 we can use similar arguments as in (2.12) to get upper bounds for the class numbers. However in these cases the bound depends on the size of S. In section (10.1) we get $h(A) \leq 4$ in the case (#3) and $h(A) \leq 6$ in the case (#4). These bounds are derived by similar means as the first proof of (2.12). Notice that from (2.9) with $\alpha = 2$ we derive $h \leq 6$ in case (#3) and $h \leq 10$ in case (#4) which is worse than the bounds given above.

CHAPTER 3 TOOLS FROM TOPOLOGICAL ALGEBRA AND THE GEOMETRY OF NUMBERS

In this chapter we state several results from topological algebra and the geometry of numbers that are needed in the rest of this thesis. Most of these results are not new and we often refer to standard texts for the proofs.

§(3.1) Ideals in subrings of imaginary quadratic fields

In this section we deal with the connection between the ideal classes of the ring of integers of an imaginary quadratic field, and equivalence classes of positive definite binary quadratic forms, cf. [BS] Kap.II §7. With the use of the map φ, as given by (2.7), this also leads to a description of the ideal classes of all subrings A_S of imaginary quadratic fields.

Let $K = \mathbb{Q}(\sqrt{\Delta})$ be an imaginary quadratic field and let $\mathfrak{a}$ be an $\mathcal{O}(K)$-ideal. Throughout this section we imagine K to be embedded in its completion at infinity $\mathbb{C}$. The norm on K with respect to $\mathcal{O}(K)$ then equals $|\cdot|_\infty$, the square of the usual absolute value on $\mathbb{C}$. The ideal $\mathfrak{a}$ is as an additive group free of rank 2 over $\mathbb{Z}$. Let $\{\alpha,\beta\}$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Then $N(x\alpha + y\beta) = (ax^2 + bxy + cy^2)N\mathfrak{a}$ for $x,y \in \mathbb{Q}$, where a, b, c are integers determined by $N(\alpha) = aN\mathfrak{a}$, $N(\beta) = cN\mathfrak{a}$ and $2a \cdot \mathrm{Re}(\alpha/\beta) = b$. The quadratic form $ax^2 + bxy + cy^2$ is positive definite and its *discriminant* $b^2 - 4ac$ is equal to Δ, cf. [BS] Kap.II §7. We will denote this form by the triple (a,b,c). For a different choice of α,β we may get a different quadratic form. However for every ideal we will make a choice such that the quadratic form is uniquely defined. First we take α to be an element of minimal norm in $\mathfrak{a} - \{0\}$. Then we choose β such that β/α lies in the *modular region*, cf. fig. 3, i.e.

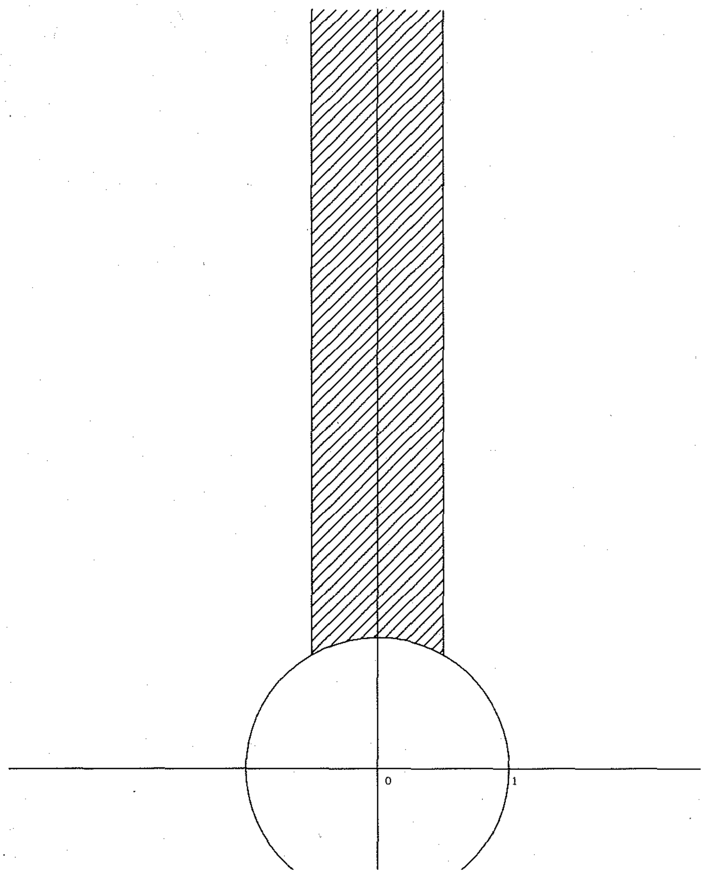


fig. 3

$\operatorname{Im}(\beta/\alpha) > 0$;

$-\frac{1}{2} < \operatorname{Re}(\beta/\alpha) \le \frac{1}{2}$;

$\operatorname{Re}(\beta/\alpha) \ge 0 \quad \text{if} \quad N(\alpha) = N(\beta)$.

The third requirement may be established by replacing the pair (α,β) by $(\beta,-\alpha)$, when necessary. With this choice of α,β the quadratic form satisfies

(3.1) $$-a < b \le a \le c ;$$
$$b \ge 0 \quad \text{if} \quad a = c ,$$

i.e. it is *reduced*, cf. [G1] §§171,172.

LEMMA (3.2). *Let* K *be an imaginary quadratic field of discriminant* Δ *and let* $\mathcal{O}$ *be its ring of integers. There is a bijection between the class group* $\mathrm{Cl}(\mathcal{O})$ *and the set of reduced quadratic forms of discriminant* Δ. *This bijection is given by*

$$[\mathbb{Z} + \mathbb{Z}\,\frac{b+\sqrt{\Delta}}{2a}] \leftrightarrow (a,b,c),$$

where c *equals* $\frac{b^2-\Delta}{4a}$.

PROOF. cf. [BS] Kap.II §7 Satz 4; [L7] §§2,3. □

Using (3.1) in combination with $\Delta = b^2 - 4ac$ we find that $a \le \sqrt{\frac{|\Delta|}{3}}$. So the class number $h(\mathcal{O})$ can be calculated by considering the finitely many possibilities $|b| \le a \le \sqrt{\frac{|\Delta|}{3}}$. In the 19th century this was already done for several values of Δ, cf. [G1] §303; [Ca].

The group structure on $\mathrm{Cl}(\mathcal{O})$ can also be described in terms of quadratic forms, cf. [Sh;L7]. Below we often use the quadratic forms for a description of the class group. In particular we will use this description to determine for every $\mathcal{O}$-ideal $\mathfrak{a}$ and every $\alpha \in K$ the minimum of $N(\gamma)$ for $\gamma \in \alpha + \mathfrak{a}$ and those γ for which this minimum is attained. For this we define the *covering radius* $\rho(\mathfrak{a})$ of the ideal $\mathfrak{a}$ to be equal to

$$(3.3) \qquad \rho(\mathfrak{a}) = \frac{a \cdot c \cdot (a - |b| + c)}{|\Delta|}$$

if $\mathfrak{a}$ corresponds to the reduced form (a,b,c). The following theorem expresses that $\rho(\mathfrak{a})$ measures the minimal radius of discs with centres at $\mathfrak{a}$ that cover $\mathbb{C}$.

THEOREM (3.4). (Dirichlet 'hexagon lemma', cf. [D2] §3,4; [C2] ch.IX thm.VII, p.234.) *Let* K *be an imaginary quadratic field of discriminant* Δ *and let* $\mathfrak{a}$ *be an* $\mathcal{O}(K)$*-ideal. Then for every* $\xi \in \mathbb{C}$ *there exists* $\alpha \in \mathfrak{a}$ *such that* $|\xi - \alpha|_\infty \le \rho(\mathfrak{a})N\mathfrak{a}$. *The inequality is best possible and there exist elements* ξ *of* K *for which the equality sign is needed. Finally the ideal* $\mathfrak{a}$ *is Euclidean if and only if* $\rho(\mathfrak{a}) < 1$.

PROOF. Let (a,b,c) be the reduced quadratic form corresponding to $\mathfrak{a}$. Let $\{\alpha\ \beta\}$ be a basis of $\mathfrak{a}$ such that $N(\alpha) = a \cdot N\mathfrak{a}$, $N(\beta) = c \cdot N\mathfrak{a}$ and $\beta = \frac{b+\sqrt{\Delta}}{2a}\alpha$. When necessary we reflect the plane in the line $\mathbb{R}\alpha$ to get $b \ge 0$. Let η be the centre of the circle through 0, α and β, i.e.

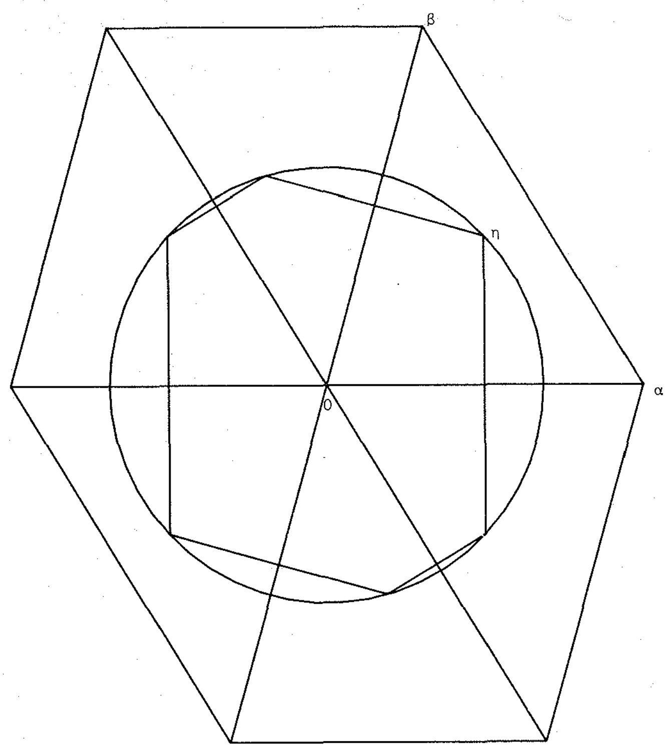


fig. 4

$$\eta = (\tfrac{1}{2} + \frac{2c-b}{2|\Delta|}\sqrt{\Delta})\alpha ,$$

which is an element of K. Let H be the closed hexagon (or rectangle in a degenerate case) with vertices η, $\beta-\eta$, $-\alpha+\eta$, $-\eta$, $-\beta+\eta$ and $\alpha-\eta$, cf. fig. 4. It is equal to the set of those elements $x \in \mathbb{C}$ such that $|x|_\infty \le |x-\gamma|_\infty$ for all $\gamma \in \mathfrak{a}$.

Take $\xi \in \mathbb{C}$. Let $\gamma \in \xi + \mathfrak{a}$ be such that $|\gamma|_\infty$ is minimal. Then γ is in H. Because $|\eta|_\infty = |\beta-\eta|_\infty = |\alpha-\eta|_\infty = \rho(\mathfrak{a})N\mathfrak{a}$ we see that $|\gamma|_\infty \le \rho(\mathfrak{a})N\mathfrak{a}$. Also we see that equality is attained at points of $\pm\eta+\mathfrak{a}$, which are all in K. This shows that $\mathfrak{a}$ is Euclidean if and only if $\rho(\mathfrak{a}) < 1$. □

§(3.2) Different, discriminant and genus

As we remarked in section (0.2) the discriminant of an algebraic number field is an important invariant of the field. For function fields the invariant which plays the same role is the genus of the field. In this section we define these invariants. First we have to define differents.

Let $L_{\mathcal{P}}/K_{\mathfrak{p}}$ be an extension of non-archimedean local fields with valuation rings $\tilde{\mathcal{O}}_{\mathcal{P}}$ and $\tilde{\mathcal{O}}_{\mathfrak{p}}$ (cf. section (1.1)) and let Tr: $L_{\mathcal{P}} \to K_{\mathfrak{p}}$ be the trace function. The set

$$\mathfrak{a} = \{\alpha \in L_{\mathcal{P}} : \mathrm{Tr}(\alpha\tilde{\mathcal{O}}_{\mathcal{P}}) \subset \tilde{\mathcal{O}}_{\mathfrak{p}}\}$$

is a fractional $\tilde{\mathcal{O}}_{\mathcal{P}}$-ideal. The *relative (local) different* $\mathcal{D}(L_{\mathcal{P}}/K_{\mathfrak{p}})$ is defined as the inverse of this ideal: $\mathcal{D}(L_{\mathcal{P}}/K_{\mathfrak{p}}) = \mathfrak{a}^{-1}$, which is an integral ideal.

Let K be a number field and let $\mathfrak{p}$ be a non-archimedean prime of K. Let p be the prime number such that $\mathfrak{p}|p$. The *different* $\mathcal{D}(K_{\mathfrak{p}})$ is defined as the local different $\mathcal{D}(K_{\mathfrak{p}}/\mathbb{Q}_p)$. Let $S \supset S_\infty$ be a set of primes of K and let $A = A_S$ be the corresponding subring of K. If $\mathfrak{p} \notin S$ we define the *local different* of A with respect to $\mathfrak{p}$ as the ideal $\mathcal{D}_{\mathfrak{p}} = \mathfrak{p}^n$, where n is defined by $\mathcal{D}(K_{\mathfrak{p}}) = \tilde{\mathfrak{p}}^n$. Because $\mathcal{D}_{\mathfrak{p}} = A$ for all but finitely many $\mathfrak{p} \notin S$ (cf. [Iy] ch.III §6.4, p.240) we may define the *different* of A by

(3.5) $$\mathcal{D}(A) = \prod_{\mathfrak{p} \notin S} \mathcal{D}_{\mathfrak{p}}.$$

If $S = S_\infty$, i.e. $A = \mathcal{O}$, the ideal $\mathcal{D}(A)^{-1}$ consists of those elements $\alpha \in K$ such that $\mathrm{Tr}(\alpha\mathcal{O}) \subset \mathbb{Z}$, where $\mathrm{Tr} : K \to \mathbb{Q}$ is the trace map, cf. [Iy] Ap.1 §2.1.

The *discriminant* $\Delta(K)$ is defined to be the integer $(-1)^s N(\mathcal{D}(\mathcal{O}))$, where s is equal to the number of complex archimedean primes of K. The sign $(-1)^s$ accounts for the archimedean primes, for which the different is not defined. It can be shown that $\Delta(K) = (\det(\sigma_i(\alpha_j))_{i,j=1}^n)^2$, where $\{\alpha_j\}_{j=1}^n$ is a basis of $\mathcal{O}$ over $\mathbb{Z}$ and where σ_i runs over all embeddings $K \to \mathbb{C}$, cf. [Iy] Ap.1 §§2.2,2.3.

Now suppose that K is a function field over $\mathbb{F}_q$. Choose $t \in K$ such that $K/\mathbb{F}_q(t)$ is a finite separable extension. For each prime $\mathfrak{p}$ of K we choose a prime element $t_{\mathfrak{p}}$ of $\tilde{\mathcal{O}}_{\mathfrak{p}}$. Then $K_{\mathfrak{p}} \simeq \mathbb{F}_{q^n}((t_{\mathfrak{p}}))$, the field of formal Laurent series in t_p over $\mathbb{F}_{q^n}$, with $n = \deg(p)$, cf. [Iy] ch.II §4.4 thm.4.9. Define

$$(3.6) \qquad \mathcal{D}_t = \{x \in K : x \in (\frac{dt}{dt_p})^{-1}\tilde{\mathcal{O}}_p \quad \text{for all } p\}.$$

This is the 'linear system of a differential divisor' of K. It is a finite dimensional vector space over $\mathbb{F}_q$. The dimension of $\mathcal{D}_t$ over $\mathbb{F}_q$ is called the *genus* $g(K)$ of K:

$$(3.7) \qquad \#\mathcal{D}_t = q^{g(K)}.$$

This dimension is independent of the choice of t, cf. (4.1) or [Iy] ch.III §6.4 pp.240, 243.

§(3.3) Local duality

In this section we investigate the structure of a local field K_p as a topological group. The following possibilities occur for the field K_p, cf. [Iy] ch.II §§3.1, 5.4, 5.5:

(3.8)

(a) If K_p is archimedean, then $K_p \simeq \mathbb{R}$ or $K_p \simeq \mathbb{C}$.

(b) If K_p is non-archimedean of characteristic 0, then K_p is a finite extension of the field $\mathbb{Q}_p$, for some prime number p.

(c) If K_p is non-archimedean of positive characteristic, then its valuation ring $\tilde{\mathcal{O}}_p$ is equal to $\mathbb{F}_q[[t]]$, the ring of formal power series over some finite field $\mathbb{F}_q$. Here t is a prime element of $\tilde{\mathcal{O}}_p$. The field K_p is its quotient field $\mathbb{F}_q((t))$, the field of formal Laurent series in t over $\mathbb{F}_q$.

As an additive topological group the field K_p is locally compact. Its dual in the sense of Pontrjagin is isomorphic to K_p itself, cf. Tate's thesis [CF] ch.XV; see also [Iy] ch.III thm.3.2. Such an isomorphism is not canonical, but we make a fixed choice by defining a non-degenerate inner product $< , >_p : K_p \times K_p \to \mathbb{R}/\mathbb{Z}$. Each element $\alpha \in K_p$ then corresponds to the character $<\alpha, \cdot>_p : K_p \to \mathbb{R}/\mathbb{Z}$. The inner product $< , >_p$ is defined as follows:

(3.9)

(a) Suppose that K_p is archimedean of characteristic 0. Let $Tr: K_p \to \mathbb{R}$ be the trace map, i.e. if $K_p = \mathbb{R}$ then $Tr = id$ and if $K_p = \mathbb{C}$ then $Tr(z) = 2Re(z)$. We define the inner product by

$$\langle x,y\rangle_p = (-Tr(xy) \bmod \mathbb{Z}) \in \mathbb{R}/\mathbb{Z} .$$

(b) Suppose K_p is a finite extension of $\mathbb{Q}_p$. Let $Tr: K_p \to \mathbb{Q}_p$ be the trace map. The composition of the natural maps

$$\mathbb{Q}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z} \hookrightarrow \mathbb{R}/\mathbb{Z}$$

will be denoted by λ. We define the inner product by

$$\langle x,y\rangle_p = \lambda \circ Tr(xy).$$

(c) Suppose $K_p = \mathbb{F}_q((t_p))$, where q is a power of the prime number p. Let $Tr: \mathbb{F}_q \to \mathbb{F}_p$ be the trace map and let $res_p: K_p \to \mathbb{F}_q$ be the residue map, which sends every element of K_p to its coefficient at t_p^{-1}. We embed $\mathbb{F}_p$ in $\mathbb{R}/\mathbb{Z}$ by $\lambda(a \bmod p) = \frac{a}{p} \in \mathbb{R}/\mathbb{Z}$ for each $(a \bmod p) \in \mathbb{F}_p$. We define an inner product by

$$\langle x,y\rangle_p = \lambda \circ Tr \circ res_p(xy)$$

In (3.9)(c) the inner product depends on the choice of t_p.

As a topological group, each local field has a Haar measure, which is defined up to a multiplicative constant. Let G be a locally compact group with Haar measure μ and dual group $\hat{G}$. The duality between G and $\hat{G}$ will be denoted by an inner product $\langle\ ,\ \rangle: G \times \hat{G} \to \mathbb{R}/\mathbb{Z}$, where we have $\langle x,\hat{x}\rangle = \hat{x}(x)$ for all $x \in G$ and all characters $\hat{x}: G \to \mathbb{R}/\mathbb{Z}$ in $\hat{G}$. For each $\mathbb{C}$-valued $f \in L^1(G)$ the *Fourier transform* $\hat{f}$ on $\hat{G}$ is defined by

(3.10) $$\hat{f}(\hat{x}) = \int f(x) \exp(2\pi i\langle x,\hat{x}\rangle)\, d\mu, \quad \text{for } \hat{x} \in \hat{G}.$$

The dual measure $\hat{\mu}$ of μ on $\hat{G}$ is the unique Haar measure on $\hat{G}$ such that for each $\mathbb{C}$-valued $f \in L^1(G)$ for which $\hat{f} \in L^1(\hat{G})$ we have

$$(3.11) \qquad f(x) = \int \hat{f}(\hat{x}) \exp(-2\pi i \langle x,\hat{x}\rangle) d\hat{\mu},$$

cf. [Iy] ch.III §1.3.

Multiplying μ by a constant corresponds to dividing $\hat{\mu}$ by the same constant, i.e. $(c\mu)^\wedge = c^{-1}\hat{\mu}$. Hence for each local field K_p there is a unique Haar measure μ_p that is self dual with respect to the inner product $\langle\ ,\ \rangle_p$. It can be shown, cf. [Iy] ch.III §3.2, that μ_p is fixed by the following properties.

(3.12)

(a) If $K_p = \mathbb{R}$, then μ_p is the Haar measure for which $\mu_p([0,1]) = 1$.

If $K_p = \mathbb{C}$, then μ_p is the Haar measure for which $\mu_p(\{x+iy \in \mathbb{C} : 0 \le x \le 1,\ 0 \le y \le 1\}) = 2$.

(b) If K_p is non-archimedean of characteristic 0, then μ_p is the Haar measure for which $\mu_p(\tilde{\mathcal{O}}_p) = N(\mathcal{D}(K_p))^{-\frac{1}{2}}$, where $\mathcal{D}(K_p)$ is the local different.

(c) If $K_p = \mathbb{F}_q((t_p))$, then μ_p is the Haar measure for which $\mu_p(\tilde{\mathcal{O}}_p) = 1$.

§(3.4) Global duality

Let S be a non-empty set of primes of K. We denote by K_S the restricted direct product of the K_p, for $p \in S$, with respect to the open sets $\tilde{\mathcal{O}}_p$, cf. [Iy] ch.III §4.1:

$$(3.13) \qquad K_S = \{x \in \prod_{p\in S} K_p : x_p \in \tilde{\mathcal{O}}_p \text{ for all but finitely many } p \in S - S_\infty\},$$

where we denote the K_p-coordinate of x by x_p. Notice that for finite S we have $K_S = \prod_{p\in S} K_p$.

By giving a system of neighbourhoods of 0 we give K_S the structure of a topological group. A typical member of this system is $\prod_{p\in S} U_p$, where U_p is a neighbourhood of 0 in K_p, and $U_p = \tilde{\mathcal{O}}_p$ for all but finitely many $p \in S$. If S consists of all primes of K we have $K_S = A_K$, the *adèle ring* of K, cf. [Iy] ch.III §4.3.

We embed K into K_S along the diagonal. The strong approximation theorem ([CF] ch.II §15) shows that the image of K is dense in K_S whenever S is not the set of all primes of K. By continuity we may extend the norm on K with respect to A_S to K_S if S is finite. It is given by

$$N(x) = \prod_{p \in S} |x_p|_p$$

The dual of K_S in the sense of Pontrjagin is isomorphic to K_S itself. As in the previous section we may fix the isomorphism by giving a non-degenerate inner product $\langle\ ,\ \rangle_S$ on K_S. This inner product is defined as follows, cf. [Iy] ch.III §4.2:

$$\langle x,y\rangle_S = \sum_{p \in S} \langle x_p,y_p\rangle_p. \tag{3.14}$$

This definition makes sense because $\langle x_p,y_p\rangle_p = 0$ for all but finitely many $p \in S$. The self-dual Haar measure with respect to this inner product is given by

$$\mu_S = \prod_{p \in S} \mu_p. \tag{3.15}$$

§(3.5) Lattices

Let $S \supset S_\infty$ be a non-empty set of primes of K. In the next section we will show that the embedding of K into K_S turns every A_S-ideal into a lattice of K_S. Here we call a subgroup Γ of a locally compact abelian group G a *lattice* if it satisfies the following conditions:

(3.16)
- Γ is discrete in G;
- Γ is cocompact in G, i.e. G/Γ is compact.

Let $\hat{G}$ denote the dual group of G, and suppose that μ and $\hat{\mu}$ are dual Haar measures on G and $\hat{G}$ respectively.

For a lattice Γ of G we define the *polar* lattice $\Gamma^\perp$ as the annihilator of Γ in $\hat{G}$, i.e.

$$(3.17) \qquad \Gamma^{\perp} = \{x \in \hat{G} : \langle x,y\rangle = 0 \quad \text{for all} \quad y \in \hat{G}\}.$$

For each $\bar{x} \in G/\Gamma$ and each $y \in \Gamma^{\perp}$ the value of $\langle x,y\rangle$ does not depend on the choice of $x \in \bar{x}$. So we may write $\langle\bar{x},y\rangle = \langle x,y\rangle$ for $x \in \bar{x} \in G/\Gamma$. In fact this induces an isomorphism between the Pontrjagin dual of Γ and $\hat{G}/\Gamma$. Because $\Gamma^{\perp\perp} \simeq \Gamma$ we find that the polar lattice $\Gamma^{\perp}$ of Γ is indeed a lattice.

The group G/Γ has a unique Haar measure $\bar{\mu}$ corresponding to μ. It is characterized by $\bar{\mu}(\bar{B}) = \mu(B)$ for every measurable set B of G, which maps injectively onto $\bar{B} \subset G/\Gamma$. The *determinant* $\nu(\Gamma)$ of a lattice Γ is given by

$$(3.18) \qquad \nu(\Gamma) = \bar{\mu}(G/\Gamma),$$

which is defined because G/Γ is compact. The determinant depends on the choice of μ.

<u>LEMMA (3.19)</u>. *Let* Γ *be a lattice of* G, *and let* $\Gamma^{\perp}$ *be its dual. If* $\nu(\Gamma)$ *and* $\nu(\Gamma^{\perp})$ *are defined with respect to a pair of dual measures we have* $\nu(\Gamma)\nu(\Gamma^{\perp}) = 1$.

<u>PROOF</u>. For the proof we introduce several measures. These are:

The counting measure μ_{Γ} on Γ and its dual measure $\hat{\mu}_{\Gamma}$ on $\hat{G}/\Gamma^{\perp}$;

the counting measure $\mu_{\Gamma^{\perp}}$ on $\Gamma^{\perp}$ and its dual measure $\hat{\mu}_{\Gamma^{\perp}}$ on G/Γ.

The measure μ is equal to the product measure $\mu_{\Gamma} \cdot \bar{\mu}$, i.e. for a measurable f on G we have

$$\int_G f\, d\mu = \int_{G/\Gamma} \Big(\int_{x\Gamma} f\, d\mu_{\Gamma}\Big) d\bar{\mu}.$$

By considering the Fourier transform of a constant function on G/Γ we find that $\hat{\mu}_{\Gamma^{\perp}}(G/\Gamma) = 1$, hence $\hat{\mu}_{\Gamma^{\perp}} = \nu(\Gamma)^{-1}\bar{\mu}$ and $\mu_{\Gamma} \cdot \hat{\mu}_{\Gamma^{\perp}} = \nu(\Gamma)^{-1}\mu$. Analogously we have $\mu_{\Gamma^{\perp}} \cdot \hat{\mu}_{\Gamma} = \nu(\Gamma^{\perp})^{-1}\hat{\mu}$. Since $\mu_{\Gamma} \cdot \hat{\mu}_{\Gamma^{\perp}}$ is dual to $\mu_{\Gamma^{\perp}} \cdot \hat{\mu}_{\Gamma}$, cf. [Iy] ch.III §(1.3), p.187, we find that $\nu(\Gamma)\nu(\Gamma^{\perp}) = 1$. □

§(3.6) Ideals as lattices

In this section we study a special kind of lattice in K_S, i.e. the A_S-ideals, where $S \supset S_\infty$ is a non-empty set of primes of K.

LEMMA (3.20). *Any* A_S*-ideal* a *becomes a lattice in* K_S *via the embedding* $a \subset K \subset K_S$.

PROOF. It suffices to consider the case that $a = A = A_S$, because for arbitrary a there exists $\alpha_1, \alpha_2 \in K^*$ such that $\alpha_1 A \subset a \subset \alpha_2 A$. Let T be a finite non-empty subset of S, containing S_∞. The set

$$U = \{x \in K_S : |x|_p < 1 \text{ if } p \in T, \ |x|_p \leq 1 \text{ if } p \in S - T\}$$

is an open subset of K_S. By (1.5) we have $1 \leq N(x) = \prod_{p \in S} |x|_p$ for any $x \in A$ with $x \neq 0$. Hence $U \cap A = \{0\}$, which proves the discreteness of A.

Now we prove the compactness of K_S/A. Consider the surjection $\varphi: \mathbb{A}_K/K \to K_S/A$, given as follows. Let $\bar{\alpha}$ be an element of $\mathbb{A}_K/K$. By the strong approximation theorem ([CF] ch.II §15) there exists $\alpha = (\alpha_p)_p \in \bar{\alpha}$ with $|\alpha_p|_p \leq 1$ for $p \notin S$. We define $\varphi(\bar{\alpha}) = (\alpha_p)_{p \in S} \bmod A$. This does not depend on the choice of α. The map φ is continuous and surjective. Since $\mathbb{A}_K/K$ is compact, cf. [CF] ch.II §14; [W] §5-2, we derive that K_S/A is compact. □

In section (3.4) we have seen that K_S is self-dual with inner product $\langle\ ,\ \rangle_S$. Hence the polar of a lattice in K_S is again a lattice in K_S. Below we determine the polar of $A = A_S$ and its determinant with respect to the measure μ_S, cf. (3.15). From the definition of the norm and (3.19) we derive that for every A-ideal a and every $\alpha \in K_S^*$ we have

$$\begin{aligned} &\nu(a) = \nu(A) \cdot Na ; \\ (3.21) \qquad &\nu(a^\perp) = \nu(A)^{-1} \cdot Na^{-1} ; \\ &\nu(\alpha a) = \nu(a) \cdot N(\alpha) . \end{aligned}$$

THEOREM (3.22). *The polar lattice* $A^\perp$ *and the determinant* $\nu(A)$ *of the ring* A *are given as follows:*

(a) *If* K *is a number field then* $A^\perp = \mathcal{D}(A)^{-1}$ *and* $\nu(A) = N(\mathcal{D}(A))^{\frac{1}{2}}$.

(b) *Suppose that* K *is a function field of genus* g *over* $\mathbb{F}_q$. *Let*

$t \in K$ *be such that* K *is a finite separable extension of* $\mathbb{F}_q(t)$. *Write* $dt = (\frac{dt}{dt_p})_{p \in S} \in K_S^*$. *Then* $A^\perp = dt \cdot \mathcal{D}_t(A)$, *where* $\mathcal{D}_t(A) = \{x \in K : \forall\, p \notin S : x \in (\frac{dt}{dt_p})^{-1}\tilde{\mathcal{O}}_p\}$ *and* $\nu(A) = q^{g-1}$.

PROOF. (a) Suppose that K is a number field. From (3.9)(b) and (3.5) we derive that

$$\mathcal{D}(A)^{-1} = \{x \in K : \forall\, p \notin S,\ \forall\, y \in \tilde{\mathcal{O}}_p : \langle x,y\rangle_p = 0\}.$$

Let P be the set of all primes of K. The annihilator of K in $\mathbb{A}_K = \mathbb{A}_P$, with respect to $\langle\ ,\ \rangle_P$, is K itself, cf. [Iy] ch.III §6.3 thm.6.2; §6.4 (10). Hence for any $x \in \mathcal{D}(A)^{-1}$ and $y \in A$ we have

$$\langle x,y\rangle_S = \sum_{p\in S} \langle x,y\rangle_p = -\sum_{p\notin S} \langle x,y\rangle_p = 0,$$

which shows that $\mathcal{D}(A)^{-1} \subset A^\perp$. Since both $A^\perp$ and $\mathcal{D}(A)^{-1}$ are lattices in K_S we have $\# A^\perp/\mathcal{D}(A)^{-1} < \infty$. This shows that $A^\perp \subset K$.

Take $x \in A^\perp$, $p \notin S$ and $y \in \tilde{\mathcal{O}}_p$. By the strong approximation theorem ([CF] ch.II §15) there exists $z \in A$ such that for all $q \notin S \cup \{p\}$ we have $\langle x,z\rangle_q = 0$ and $\langle x,y-z\rangle_p = 0$. Then

$$0 = \langle x,z\rangle_S = \sum_{q\in S} \langle x,z\rangle_q = -\sum_{q\notin S} \langle x,z\rangle_q = -\langle x,z\rangle_p = -\langle x,y\rangle_p,$$

which shows that $A^\perp \subset \mathcal{D}(A)^{-1}$, hence $A^\perp = \mathcal{D}(A)^{-1}$. From (3.21) we derive that $\nu(A) = N(A^\perp)^{-\frac{1}{2}} = N(\mathcal{D}(A))^{\frac{1}{2}}$.

(b) Suppose that K is a function field of genus g over $\mathbb{F}_q$. Let P be the set of all primes of K. The annihilator of K in $\mathbb{A}_K = \mathbb{A}_P$, with respect to $\langle\ ,\ \rangle_P$ is $(\frac{dt}{dt_p})_p \cdot K$, cf. [Iy] ch.III §6.3 thm.6.2; §6.4 (12).

From the definitions of $A^\perp$ and dt we derive that

$$A^\perp = dt \cdot \{x \in K_S : \sum_{p\in S} \langle x, y\,\frac{dt}{dt_p}\rangle_p = 0 \text{ for all } y \in A\}.$$

A computation as in part (a) gives

$$A^\perp = dt \cdot \{x \in K : \forall\, p \notin S,\ \forall\, y \in \tilde{\mathcal{O}}_p : \langle x, y\,\frac{dt}{dt_p}\rangle_p = 0\}.$$

Hence

$$A^{\perp} = dt \cdot \{x \in K : \forall\, p \notin S,\ \forall\, y \in \frac{dt}{dt_p}\tilde{\mathcal{O}}_p : \langle x,y\rangle_p = 0\} =$$

$$= dt \cdot \{x \in K : \forall\, p \notin S,\ x \in (\frac{dt}{dt_p})^{-1}\tilde{\mathcal{O}}_p\} = dt \cdot \mathcal{D}_t(A).$$

From (3.21) we derive that

$$\nu(A) = N(dt)^{-\frac{1}{2}}\, N(\mathcal{D}_t(A))^{-\frac{1}{2}} = \prod_{p\in S} \left|\frac{dt}{dt_p}\right|_p^{-\frac{1}{2}} \prod_{p\notin S} \left|\frac{dt}{dt_p}\right|_p^{-\frac{1}{2}} = q^{g-1},$$

cf. [Iy] ch.III §6.4 (13),(21); ch.II §8, p.174. □

§(3.7) Lattice constants

In this section we generalize some theorems from the geometry of numbers to our situation of lattices in K_S. First we state an analogue to the theorem of Blichfeldt ([C2] ch.III §2 thm.I, p.69).

LEMMA (3.23). *Let* Γ *be a lattice of* K_S, *let* U *be a measurable set in* K_S *and let* $n \in \mathbb{Z}_{\geq 0}$. *Suppose that* $\mu_S(U) > n\nu(\Gamma)$. *Then there exists* $x \in K_S$ *such that*

$$\#((x+\Gamma) \cap U) \geq n+1.$$

PROOF. Let $\varphi\colon K_S \to K_S/\Gamma$ be the quotient map. Define the function f on K_S/Γ by

$$f(\bar{x}) = \#(\varphi^{-1}(\bar{x}) \cap U) \quad \text{for all} \quad \bar{x} \in K_S/\Gamma.$$

Then $\int f\, d\bar{\mu}_S$ equals $\mu_S(U)$, where $\bar{\mu}_S$ is the unique Haar measure on K_S/Γ with the property that $\bar{\mu}_S(\varphi(B)) = \mu_S(B)$ for all measurable B for which $\varphi|B$ is injective, cf. section (3.5). Because $\mu_S(U) > n\nu(\Gamma) = \bar{\mu}_S(K_S/\Gamma)$ there exists $\bar{x} \in K_S/\Gamma$ such that $f(\bar{x}) > n$, i.e. $f(\bar{x}) \geq n+1$, which proves the lemma. □

For the rest of this section we only deal with the case that $\#S = 2$, and $S \supset S_\infty$. Suppose that $S = \{p,q\}$. We consider sets of the form

$$R(a,b) = \{x \in K_S : |x|_p \leq a,\ |x|_q \leq b\}. \tag{3.24}$$

LEMMA (3.25). *Let* $a,b \in \mathbb{R}_{>0}$ *be such that the quotient map* $\varphi\colon K_S \to K_S/\Gamma$ *is injective when restricted to* $R(a,b)$. *Then*

$$\liminf_{\min(A,B)\to\infty} \frac{\mu_S(R(A,B) \cap (\Gamma + R(a,b)))}{\mu_S(R(A,B))} \geq \frac{\mu_S(R(a,b))}{\nu(\Gamma)}$$

PROOF. Even if $K_p \neq \mathbb{C}$ we have $|x-y|_p \geq (\sqrt{|x|_p} - \sqrt{|y|_p})^2$ for all $x,y \in K_p$ and an analogous inequality holds for K_q. Hence for $A > a$ and $B > b$ we have $R(A,B) \cap (\Gamma + R(a,b)) \supset R(a,b) + (\Gamma \cap R((\sqrt{A}-\sqrt{a})^2,(\sqrt{B}-\sqrt{b})^2))$, thus

$$\text{(3.26)}\qquad \mu_S(R(A,B) \cap (\Gamma + R(a,b))) \geq \mu_S(R(a,b)) \cdot \#(\Gamma \cap R(\sqrt{A}-\sqrt{a})^2,(\sqrt{B}-\sqrt{b})^2)).$$

Because K_S/Γ is compact there exist $A_0, B_0 \in \mathbb{R}_{>0}$ such that $\varphi|R(A_0,B_0)$ is surjective. Suppose that $A > (\sqrt{A_0}+\sqrt{a})^2$ and $B > (\sqrt{B_0}+\sqrt{b})^2$, then we write $A' = (\sqrt{A}-\sqrt{A_0}-\sqrt{a})^2$ and $B' = (\sqrt{B}-\sqrt{B_0}-\sqrt{b})^2$. Applying (3.23) with $U = R(A',B')$ we find that there exists $x \in K_S$ such that

$$\#((x+\Gamma) \cap R(A',B')) \geq \frac{\mu_S(R(A',B'))}{\nu(\Gamma)}.$$

Subtracting some $x_0 \in R(A_0,B_0)$ that is congruent to $x \bmod \Gamma$ we obtain

$$\#(\Gamma \cap R((\sqrt{A}-\sqrt{a})^2,(\sqrt{B}-\sqrt{b})^2)) \geq \frac{\mu_S(R(A',B'))}{\nu(\Gamma)}.$$

Combining this with (3.26) we get

$$\frac{\mu_S(R(A,B) \cap (\Gamma + R(a,b)))}{\mu_S(R(A,B))} \geq \frac{\mu_S(R(a,b))}{\nu(\Gamma)} \cdot \frac{\mu_S(R(A',B'))}{\mu_S(R(A,B))}$$

This proves the lemma since

$$\lim_{\min(A,B)\to\infty} \frac{\mu_S(R(A',B'))}{\mu_S(R(A,B))} = 1. \qquad \square$$

Actually we have equality in (3.25) and we may replace 'lim inf' by 'lim'. However, we will not need this.

LEMMA (3.27). *Suppose that* $K_p = \mathbb{C}$. *If* $a,b \in \mathbb{R}_{>0}$ *are such that*

$$\mu_S(R(a,b)) > \frac{\pi}{2\sqrt{3}} \nu(\Gamma),$$

then there exists $x,y \in R(a,b)$ *with* $x - y \in \Gamma$.

PROOF. Suppose on the contrary that there do not exist such $x,y \in R(a,b)$. Then we may apply (3.25) for $R(a,b)$. For each $\beta \in K_q$ the set

$$U_\beta = \{\alpha \in \mathbb{C} : (\alpha,\beta) \in \Gamma + R(a,b)\}$$

is a disjoint union of discs of radius $\sqrt{a}$ in $\mathbb{C}$. By using [Le] ch.3 §22 prop.3 and thm.6 we find that there exists a function $f: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with $\lim_{A\to\infty} f(A) = 0$ such that

$$\frac{\mu_p(\{x \in U_\beta : |x|_p \leq A\})}{2\pi A} \leq \frac{\pi}{2\sqrt{3}} + f(A)$$

This shows that

$$\limsup_{\min(A,B)\to\infty} \frac{\mu_S(R(A,B) \cap (\Gamma + R(a,b)))}{\mu_S(R(A,B))} =$$

$$\limsup_{\min(A,B)\to\infty} \int_{|y|_q < B} \frac{\mu_p(\{x \in U_y : |x|_p \leq A\})}{2\pi A \cdot \mu_q(\{\beta \in K_q : |\beta|_q < B\})} d\mu_q \leq$$

$$\limsup_{\min(A,B)\to\infty} \left(\frac{\pi}{2\sqrt{3}} + f(A)\right) = \frac{\pi}{2\sqrt{3}}.$$

With (3.25) this shows that $\mu_S(R(a,b)) \leq \frac{\pi}{2\sqrt{3}} \nu(\Gamma)$. □

For each of the possible choices of S, with $S \supset S_\infty$, we define a constant C_S by

(3.28) (F) $C_S = 1$ if K is a function field;

(#1) $C_S = N(\mathcal{D}(K_q))^{\frac{1}{2}}$ if $K_p \simeq \mathbb{R}$ and K_q is non-archimedean;

($\#2^+$) $C_S = 1$ if $K_p \simeq K_q \simeq \mathbb{R}$;

($\#2^-$) $C_S = \frac{1}{\sqrt{3}} N(\mathcal{D}(K_q))^{\frac{1}{2}}$ if $K_p \simeq \mathbb{C}$ and K_q is non-archimedean;

(#3) $\quad C_S = \frac{1}{\sqrt{3}}$ if $K_p \simeq \mathbb{R}$ and $K_q \simeq \mathbb{C}$;

(#4) $\quad C_S = \frac{2}{\pi\sqrt{3}}$ if $K_p \simeq K_q \simeq \mathbb{C}$.

<u>PROPOSITION (3.29)</u>. *Let* Γ *be a lattice in* K_S. *If* $a \in |K_p^*|_p$ *and* $b \in |K_q^*|_q$ *are such that* $ab > C_S \nu(\Gamma)$ *then there exists* $\alpha \in \Gamma$, $\alpha \neq 0$ *with* $|\alpha|_p \leq a$ *and* $|\alpha|_q \leq b$. *If* p *or* q *is archimedean it suffices to assume that* $ab \geq C_S\ \nu(\Gamma)$.

<u>PROOF</u>. First suppose that $ab > C_S\ \nu(\Gamma)$. Define $a_0, b_0 \in \mathbb{R}_{>0}$ by

$a_0 = \frac{1}{2}a$ if $K_p \simeq \mathbb{R}$; $b_0 = \frac{1}{2}b$ if $K_q \simeq \mathbb{R}$;

$a_0 = \frac{1}{4}a$ if $K_p \simeq \mathbb{C}$; $b_0 = \frac{1}{4}b$ if $K_q \simeq \mathbb{C}$;

$a_0 = a$ if K_p is non-archimedean;

$b_0 = b$ if K_q is non-archimedean.

Then for each pair $x, y \in R(a_0, b_0)$ we have $x - y \in R(a,b)$. Using (3.12) we get

(F) $\quad \mu_S(R(a_0,b_0)) = ab$ if K is a function field;

(#1) $\quad \mu_S(R(a_0,b_0)) = N(\mathcal{D}(K_q))^{-\frac{1}{2}}ab$ if $K_p \simeq \mathbb{R}$ and K_q is non-archimedean;

(#2$^+$) $\quad \mu_S(R(a_0,b_0)) = ab$ if $K_p \simeq K_q \simeq \mathbb{R}$;

(#2$^-$) $\quad \mu_S(R(a_0,b_0)) = \frac{1}{2}\pi N(\mathcal{D}(K_q))^{-\frac{1}{2}}ab$ if $K_p \simeq \mathbb{C}$ and K_q is non-archimedean;

(#3) $\quad \mu_S(R(a_0,b_0)) = \frac{1}{2}\pi ab$ if $K_p \simeq \mathbb{R}$ and $K_q \simeq \mathbb{C}$;

(#4) $\quad \mu_S(R(a_0,b_0)) = \frac{1}{4}\pi^2 ab$ if $K_p \simeq K_q \simeq \mathbb{C}$.

From (3.23), with $n = 1$, and (3.27) we derive that there exist $x, y \in R(a_0, b_0)$ such that $x \neq y$ and $x - y \in \Gamma$. Then $x - y \in \Gamma \cap R(a,b)$, which proves the first assertion.

If K_p is archimedean it suffices that $ab \geq C_S\ \nu(\Gamma)$. To prove this we apply the previous result to $a + \varepsilon$, for $\varepsilon > 0$, and let ε tend to 0, taking into account that Γ is discrete. □

CHAPTER 4 EUCLIDEAN IDEAL CLASSES FOR $\#S = 1$

In this chapter we give the remainder of the proofs of (0.18) and (1.9). These theorems deal with the cases for which $\#S = 1$. In section (4.1) we deal with the case (F). Also we compute the class group of subrings A_S of $\mathbb{F}_q(t)$ for arbitrary non-empty sets S of primes. In section (4.2) we treat case (#2) of (1.9). The proofs of (1.9) (#1), (#2) were already given, see sections (0.1) and (0.2).

§(4.1) Function fields

Let K be a function field in one variable over $\mathbb{F}_q$. Let S be a non-empty set of primes of K. We do not always assume that $\#S = 1$. We show that $A = A_S$ has a Euclidean ideal class if the genus $g(K)$ equals 0. After this we prove that under the assumption that A has a Euclidean ideal class, with $\#S = 1$, we have $g(K) = 0$. Finally we compute the class group of A_S if $g(K) = 0$.

First we give two characterizations of the genus.

LEMMA (4.1). *Let* K *be a function field over* $\mathbb{F}_q$ *and let* S *be a non-empty set of primes of* K. *Then*

$$g(K) = \dim_{\mathbb{F}_q}(K_S/(\prod_{p\in S}\tilde{\mathcal{O}}_p + A_S)).$$

PROOF. From (3.22)(b), (3.9)(c) and (3.6) we derive that the annihilator of $\prod_{p\in S}\tilde{\mathcal{O}}_p + A_S$ in K_S, with respect to $\langle\ ,\ \rangle_S$ is equal to

$$\prod_{p\in S}\tilde{\mathcal{O}}_p \cap dt\cdot\mathcal{D}_t(A) = dt\cdot\mathcal{D}_t.$$

Because dt is a unit in K_S we have

$$\dim_{\mathbb{F}_q}(K_S/(\prod_{p\in S}\tilde{\mathcal{O}}_p + A_S)) = \dim_{\mathbb{F}_q}(\mathcal{D}_t) = g(K). \quad \square$$

COROLLARY (4.2). *Let* P *be the set of all primes of* K. *For each set* S *of primes of* K *for which both* S *and* P − S *are non-empty we have*

$$g(K) = \dim_{\mathbb{F}_q}(K/(A_S + A_{P-S})).$$

PROOF. The composite map

$$K \longrightarrow K_S \longrightarrow K_S/(\prod_{p\in S} \tilde{\mathcal{O}}_p + A_S)$$

has kernel $A_S + A_{P-S}$. The image of K is dense, and because $K_S/(\prod_{p\in S} \tilde{\mathcal{O}}_p + A_S)$ is finite the map is surjective. □

LEMMA (4.3). *Each function field* K *over* $\mathbb{F}_q$ *which has genus equal to* 0 *is isomorphic to* $\mathbb{F}_q(t)$.

PROOF. See [AT] ch.5 thm.5; [Wel] ap.V lemma 1; [De] §39. □

THEOREM (4.4). *Let* K *be a function field of genus* 0 *over* $\mathbb{F}_q$. *Let* S *be a non-empty set of primes of* K. *Then* A_S *has a Euclidean ideal class.*

PROOF. From lemma (4.3) we know that $K = \mathbb{F}_q(t)$ for some $t \in K$. Using (2.8) we may suppose that S consists of only one prime p. Replacing t by t^{-1}, if necessary, we may assume that $p \neq \infty$. The description of A_S in (0.6)(b) shows that there exists an irreducible $f \in \mathbb{F}_q[t]$, such that

$$A_S = \{g \cdot f^{-n} \in \mathbb{F}_q(t) : g \in \mathbb{F}_q[t];\ n \in \mathbb{Z}_{\geq 0};\ \deg(g) \leq \deg(f^n)\}.$$

The norm function with respect to S is given by $N(\frac{g}{h} f^{-n}) = q^{nd}$, with $d = \deg(p) = \deg(f)$, if $g,h \in \mathbb{F}_q[t]$ and $f \nmid gh$. We show that the prime ideal

$$q = \infty = \{g \cdot f^{-n} \in A_S :\ \deg(g) < \deg(f^n)\}$$

is Euclidean. Let $\frac{u}{v} f^{-n}$ be an element of K, with $u,v \in \mathbb{F}_q[t]$ and $f \nmid v$. Because all residue classes mod f^n in $\mathbb{F}_q[t]$ have representatives of degree less than $\deg(f^n)$, there exists $g \in \mathbb{F}_q[t]$ with $\deg(g) < \deg(f^n)$ and $u \equiv gv \bmod f^n$. Then $gf^{-n} \in q$ and $N(\frac{u}{v} f^{-n} - g \cdot f^{-n}) \leq 1 < q = Nq$. □

Another proof can be given as follows. Denote by P the set of all primes of K. We may suppose that $P \neq S$, since otherwise the theorem is trivial. Applying (4.2), with $g(K) = 0$, we find that $K = A_S + A_{P-S}$. Let the norm with respect to A_S be denoted by N and the norm with respect to A_{P-S} by N'. Then for each $x \in K^*$ we have $N(x) = N'(x)^{-1}$ by (1.3). From (4.3) we see that at least one of the rings A_S or A_{P-S} has a prime ideal of norm q, e.g. ∞.

First suppose that A_S has a prime ideal p of norm q. Then $A_S = \mathbb{F}_q + p$, hence $K = A_{P-S} + \mathbb{F}_q + p = A_{P-S} + p$. Because for each $x \in A_{P-S}$ we have $N(x) \leq 1 < q = Np$ we find that p is Euclidean.

Now suppose that A_{P-S} has a prime ideal p of norm q. Then $A_{P-S} = \mathbb{F}_q + p$, hence $K = \mathbb{F}_q + p + A_S = p + A_S$. Because for each $x \in p$ we have $N'(x) \geq N'(p) = q$, i.e. $N(x) \leq q^{-1} < 1$, we find that A_S is a Euclidean ring. □

<u>THEOREM (4.5)</u>. *Let* K *be a function field over* $\mathbb{F}_q$. *Suppose that* $\#S = 1$ *and that* $A = A_S$ *has a Euclidean ideal class. Then the genus of* K *equals* 0.

<u>PROOF</u>. Let p be the prime in S and let $a \neq A$ be an integral ideal of minimal norm. Then a is Euclidean by (2.3). Hence $A = a + A^* = a + \mathbb{F}_q$ and the norm of a equals q. This shows that the set of elements of K of norm $< Na$ is equal to $\mathcal{O}_p$. Since a is Euclidean this implies that $K = \mathcal{O}_p + a = \mathcal{O}_p + A$. Because $\mathcal{O}_p = A_{P-S}$ the theorem follows from (4.2). □

<u>THEOREM (4.6)</u>. *Let* S *be a non-empty set of primes of* $K = \mathbb{F}_q(t)$ *and let* $h = \gcd(\deg(p) : p \in S)$. *There exists an isomorphism*

$$\delta: \quad Cl(A_S) \longrightarrow \mathbb{Z}/h\mathbb{Z},$$

given by $\delta([q]) = \deg(q) \bmod h$, *for prime ideals* q *of* A_S. *Moreover* $\delta^{-1}(1 \bmod h)$ *is a Euclidean ideal class.*

<u>PROOF</u>. By demanding $\deg(a \cdot b) = \deg(a) + \deg(b)$ we may extend the degree function to all A_S-ideals and we have $N(a) = q^{\deg(a)}$. From the product formula (1.3) we derive that $\deg(xA_S) \equiv 0 \bmod h$ for all $x \in K^*$. Hence δ is a well defined homomorphism and $\delta([a]) = \deg(a) \bmod h$ for any A_S-ideal a.

If $\infty \in S$ we have $h = 1$ and $A_S \supset \mathbb{F}_q[t]$, hence $h(A_S) = 1$, thus δ is an isomorphism and all A_S - ideals are Euclidean.

If $\infty \notin S$ then ∞ may be regarded as an integral A_S - ideal of norm q. Hence $\delta([\infty]) \equiv 1 \bmod h$ and δ is surjective. From the description of (0.6)(b) we find that $\deg(\prod_{p\in S} f_p^{n(p)}) = -\sum_{p\in S} n(p)\deg(p)$, where $f_p \in \mathbb{F}_q[t]$ is a generator of the $\mathbb{F}_q[t]$ - ideal p. For a suitable choice of the $n(p)$ we find that A_S contains elements of norm q^h. Using the bound of (2.10) we find that $h(A_S) \le h$ and δ is an isomorphism. The last assertion follows from (4.4) and (2.3). □

REMARK (4.8). For (4.4) and (4.5) we do not really need that the field of constants of K is finite. Analogous theorems can be given for function fields with infinite constant fields: if S is a set of one prime of K then A_S has a Euclidean ideal class if and only if K has genus 0 and K has a prime of degree 1, cf. [S] prop.19.

This completes the proof of the (F) parts of (0.18) and (1.9). Also the 'if' - part of (0.19)(F) and (1.10)(F) and the assertions about the class numbers are proven by (4.4) and (4.6).

§(4.2) Number fields

In this section we finish the proof of (1.9)(#2). In section (1.2) we have already seen that the rings of integers of $\mathbb{Q}(\sqrt{-15})$ and $\mathbb{Q}(\sqrt{-20})$ have a Euclidean ideal class.

Suppose that the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{\Delta})$ has a non-principal Euclidean ideal class. We have to show that $\Delta \in \{-15,-20\}$. From (2.12) we know that $h(K) = 2$.

Let $\mathfrak{a}$ be a non-principal ideal of $\mathcal{O} = \mathcal{O}(K)$, corresponding to the reduced quadratic form (a,b,c). Because $\mathfrak{a}$ is non-principal we know that $\mathfrak{a}$ is Euclidean and we have $a \neq 1$. By (3.4) we have $ac(a-|b|+c) < |\Delta| = 4ac-b^2$. Because $a-|b|+c \ge c$ we have $ac^2 < 4ac$, i.e. $c \le 3$. Since $a \le c$ we have $a \le 3$ as well. If $a = 3$ then $c = 3$ and $|b| \le 3$, but then $9(6-|b|) \ge 36-b^2$, a contradiction; hence $a = 2$. If $b = 0$ we get $2c(2+c) < 8c$, i.e. $c < 2$, which is impossible. If $|b| = 1$ we find $c = 2$ and $\Delta = -15$. Finally if $|b| = 2$ we find $c = 3$, since $\gcd(a,b,c) = 1$, and $\Delta = -20$.

This finishes the proof of (1.9)(#2) and the determination of the rings with a Euclidean ideal class in the case that $\#S = 1$.

CHAPTER 5 APPLICATION OF THE GEOMETRY OF NUMBERS

Let K be a global field and let $S \supset S_\infty$ be a non-empty set of primes of K. In the first section we translate the Euclidean condition for an A_S - ideal in terms of the geometry of numbers. In the following sections we assume that $\#S = 2$ and we use the tools of chapter 3 to get bounds on the discriminant or genus in the case that A_S has a Euclidean ideal class. Finally in the last section we determine the rings in case $(\#2^+)$ with a Euclidean ideal class.

§(5.1) Translation of the Euclidean condition into the geometry of numbers

As in chapter 3 we regard K as a dense subset of $K_S = \prod_{p\in S} K_p$. For $t \in \mathbb{R}_{>0}$ we define a subset V_t of K_S by

$$(5.1) \qquad V_t = \{x \in K_S : \prod_{p\in S} |x|_p < t\}.$$

From the definition of the norm (1.5) we derive that an A_S - ideal $\mathfrak{a}$ is Euclidean if and only if $K \subset \mathfrak{a} + V_{N\mathfrak{a}}$.

For two different cases with $\#S = 2$ a picture of V_t is given in figures 5 and 6. In figure 5 we are in the case $(\#2^+)$, where $K = \mathbb{Q}(\sqrt{13})$ and $t = \frac{1}{3}$. The elements of $A_S = \mathcal{O}(K) = \mathbb{Z}[\frac{1}{2}(1+\sqrt{13})]$ are represented by dots and V_t is the open region bounded by hyperbolas. Figure 6 depicts the case $(\#1)$, where $K = \mathbb{Q}$, $S = \{\infty, 2\}$ and $t = 1$. The ring $A_S = \mathbb{Z}[\frac{1}{2}]$ is represented by dots. The shaded regions are background and are not part of the picture. In this case we have embedded $\mathbb{Q}_2$ topologically into $\mathbb{R}_{\geq 0}$ by sending $\sum_{k=n}^{\infty} a_k 2^k$ to $\sum_{k=n}^{\infty} a_k (\frac{9}{20})^k$, with $a_k \in \{0,1\}$. The regions V_t and $\frac{11}{2} + V_t$ are given by their boundaries.

In general it is not a trivial problem to decide whether a dense subset of K_S, viz. K, is contained in the union of the sets $\alpha + V_t$ for $\alpha \in \mathfrak{a}$. We will illustrate this for the case that $K = \mathbb{Q}(\sqrt{13})$, $S = S_\infty = \{p, q\}$, $\mathfrak{a} = \mathcal{O}$ and $t = \frac{1}{3}$. A partial covering of a neighbourhood of 0 is depicted in figure 7. Here only the sets $\alpha + V_t$ for $\alpha \in \mathcal{O}$, with

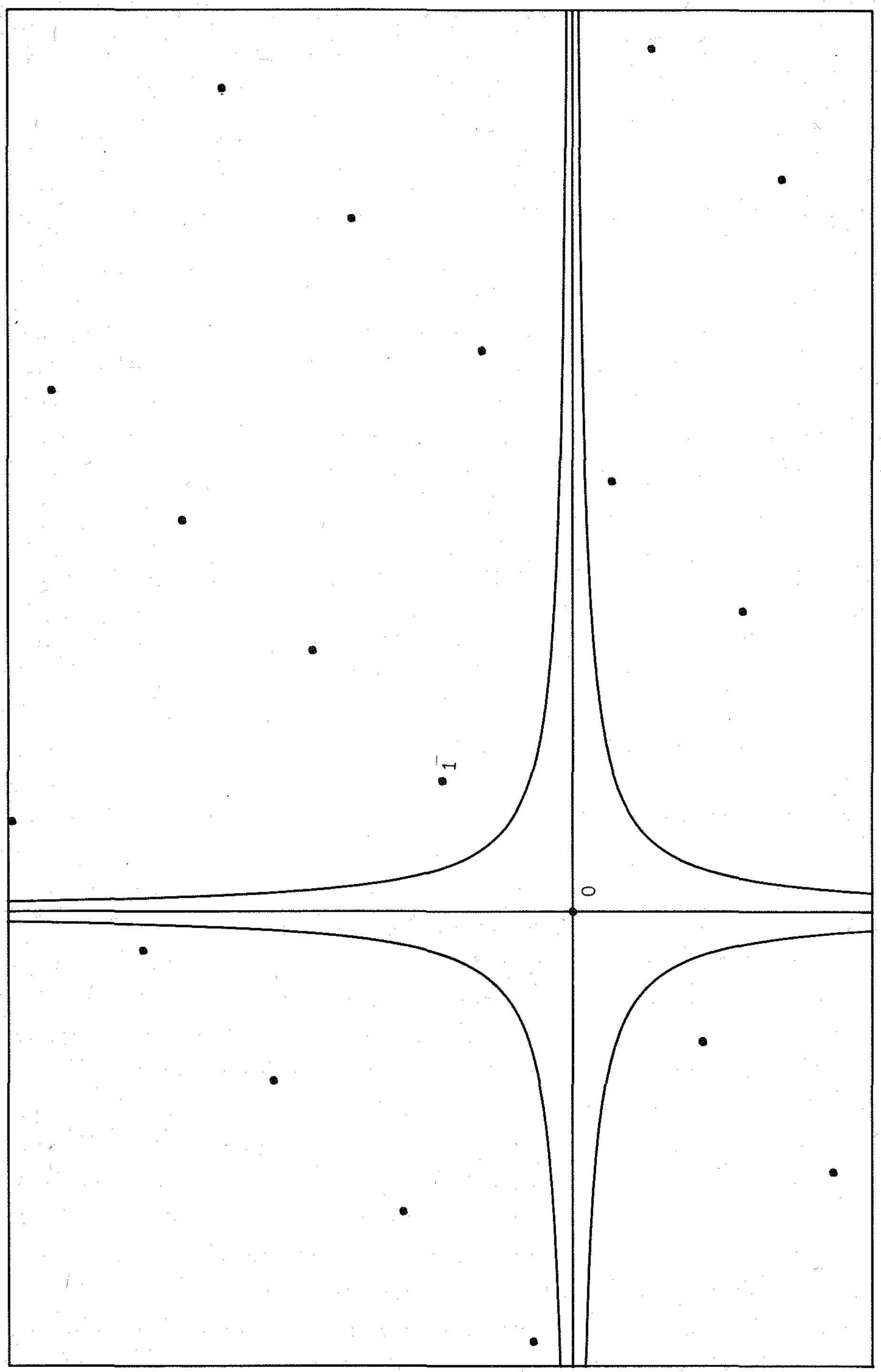


fig. 5

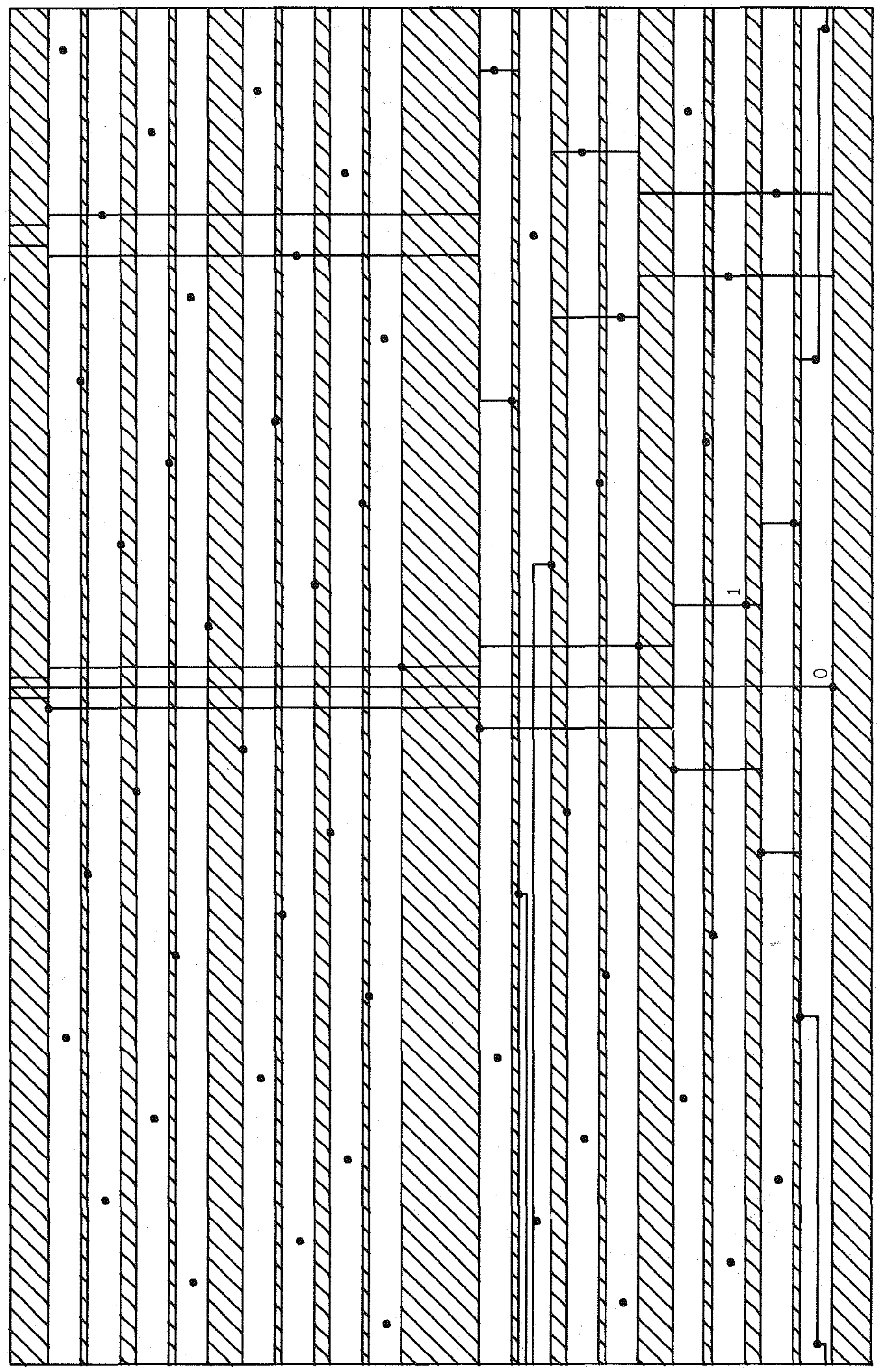


fig. 6

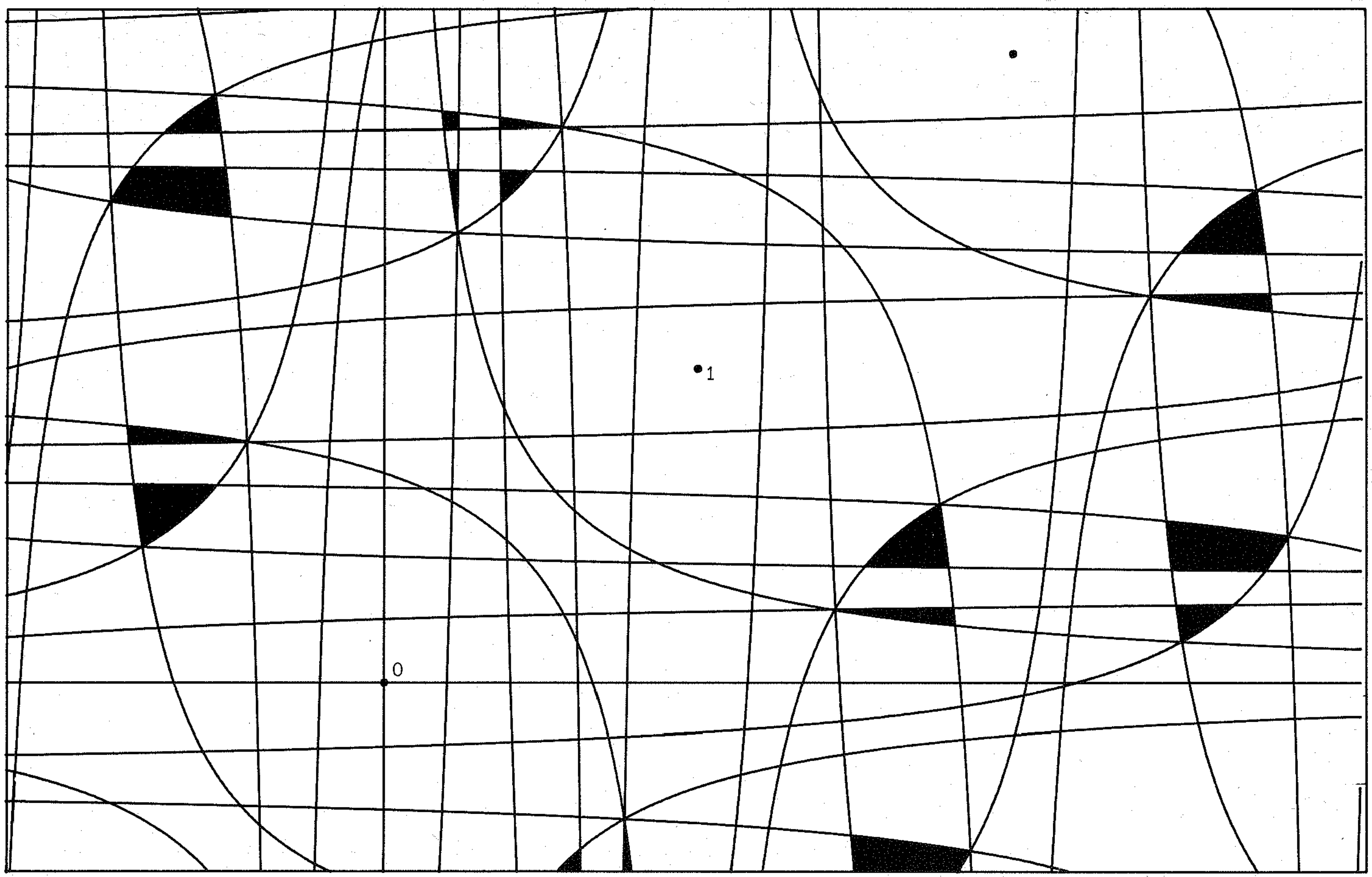


fig. 7

$-3.6 < \alpha_p < 5.5$ and $-3 < \alpha_q < 5$ are drawn. The black regions are not yet covered. One can prove that for any finite union U of sets of the form $\alpha + V_t$ for $\alpha \in \mathcal{O}$ there are regions in this neighbourhood of 0 that are contained in $K_S - U$, cf. [BSD1] §9. This shows that there are also elements of K, in this region, not contained in U. But in principle it remains still possible that $K \subset \mathcal{O} + V_t$. In fact this is not the case, cf. [BSD1] thm 7. Because $K_S/\mathcal{O}$ is compact we surely do *not* have that $K_S = \mathcal{O} + V_t$.

If $K_S = \mathfrak{a} + V_t$ we certainly have that $K \subset \mathfrak{a} + V_t$. It is not known whether the converse holds. However we might conjecture that the converse does hold indeed, analogously to a conjecture of Barnes and Swinnerton-Dyer [BSD2] p.313. In all situations where we found that $K_S \neq \mathfrak{a} + V_t$ we were able to prove that $K \not\subset \mathfrak{a} + V_t$, cf. (6.7) and section (9.1).

In the case that $\#S = 2$ we are able to prove a slightly weaker property: If $K_S \neq \mathfrak{a} + V_t$ then $K \not\subset \mathfrak{a} + V_{t'}$ for all $t' < t$. The proof of this will be given in the next section. This solves the problem if we can prove that $K_S \neq \mathfrak{a} + V_t$ for some $t > N\mathfrak{a}$, because $\mathfrak{a}$ is not Euclidean in this case.

§(5.2) The theorem of Barnes and Swinnerton-Dyer

In this section we prove a proposition, which in the case $(\#2^+)$ is due to Barnes and Swinnerton-Dyer, cf. [BSD2] thm. M. It is an important tool in disproving the existence of a Euclidean ideal class, when $\#S = 2$.

PROPOSITION (5.2). *Let* K *be a global field, let* $S \supset S_\infty$ *be a set of 2 primes of* K *and let* $\mathfrak{a}$ *be an* A_S*-ideal. If* $t \in \mathbb{R}_{>0}$ *is such that* $K \subset \mathfrak{a} + V_t$, *then for any* $t' > t$ *we have* $K_S = \mathfrak{a} + V_{t'}$.

PROOF. Suppose that $S = \{p,q\}$. Let τ be a fundamental unit of A_S with $|\tau|_p > 1$ and thus $|\tau|_q = |\tau|_p^{-1} < 1$. Because $|\tau|_p \neq 1$ and $|\tau|_q \neq 1$, there exists $c \in \mathbb{R}_{>0}$ for which

$$(5.3) \qquad |\tau^m - 1|_p > c \quad \text{and} \quad |\tau^m - 1|_q > c \quad \text{for any } m \in \mathbb{Z},\ m \neq 0.$$

Let B be the set

$$B = \{x \in V_t : |x|_p = 0 \text{ and } |x|_q \le 1, \text{ or } |x|_q = 0 \text{ and } |x|_p \le 1, \text{ or } 1 \le \frac{|x|_p}{|x|_q} \le \frac{|\tau|_p}{|\tau|_q}\},$$

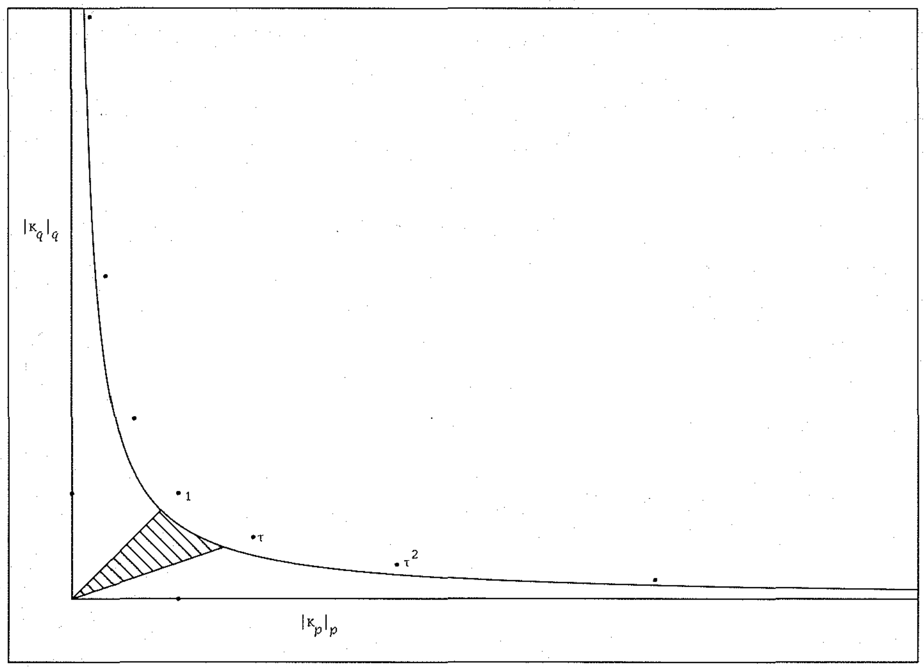


fig. 8

see fig. 8. We have $V_t = \bigcup_{n \in \mathbb{Z}} \tau^n B$. Because B is bounded its closure $\overline{B}$ in K_S is compact. Choose $t' \in \mathbb{R}$ with $t' > t$, then $\overline{B} \subset V_{t'}$. By the compactness of $\overline{B}$ there exists $\delta \in \mathbb{R}_{>0}$, such that for all $z \in K_S$ we have

$$(5.4) \qquad |z|_p < \delta, \quad |z|_q < \delta \quad \Rightarrow \quad z + \overline{B} \subset V_{t'}.$$

Choose $x \in K_S$. We show that $x \in \mathfrak{a} + V_{t'}$. Consider the sequence $(\tau^n x \bmod \mathfrak{a})_{n \in \mathbb{Z}}$ in $K_S/\mathfrak{a}$. Because $K_S/\mathfrak{a}$ is compact there exist $m,n \in \mathbb{Z}$ with $m > n$ and $\tau^m x - \tau^n x \equiv z \bmod \mathfrak{a}$ for some $z \in K_S$ with $|z|_p < \delta \cdot c$ and $|z|_q < \delta \cdot c$. Because $\tau^n x \in \mathfrak{a} + V_{t'}$ implies $x \in \mathfrak{a} + V_{t'}$ we may assume that $n = 0$. Let $\gamma \in \mathfrak{a}$ be the element such that $\tau^m x = x + \gamma + z$. We show that x is very close to the element $y \in K$ with $\tau^m y = y + \gamma$, i.e. to $y = \gamma(\tau^m - 1)^{-1}$. In fact by (5.3) we have for $0 \le k \le m$ that

$$|\tau^k x - \tau^k y|_p = |\tau^k (x-y)|_p \le |\tau^m (x-y)|_p = |z(1-\tau^{-m})^{-1}|_p < \frac{\delta c}{c} = \delta$$

and

$$|\tau^k x - \tau^k y|_q = |\tau^k (x-y)|_q \le |x-y|_q = |z(\tau^m - 1)^{-1}|_q < \frac{\delta c}{c} = \delta.$$

Because $y \in K \subset \mathfrak{a} + V_t = \bigcup_{r \in \mathbb{Z}} \tau^r B$, there exist $k \in \mathbb{Z}$ and $\beta \in B$ with $\tau^k y \equiv \beta \bmod \mathfrak{a}$. We may assume that $0 \le k \le m$ since $\tau^m y \equiv y \bmod \mathfrak{a}$. Because both $|\tau^k x - \tau^k y|_p$ and $|\tau^k x - \tau^k y|_q$ are less than δ we have by (5.4) that $\tau^k x - \tau^k y + \beta \in V_{t'}$. Since $\tau^k y - \beta \in \mathfrak{a}$ we have $\tau^k x \in \mathfrak{a} + V_{t'}$. Because τ^k is a unit also $x \in \mathfrak{a} + V_{t'}$. □

COROLLARY (5.5). *Suppose that* $\#S = 2$. *For an* A_S*-ideal* $\mathfrak{a}$ *we define*

$$t(\mathfrak{a}) = \inf\{t \in \mathbb{R}_{>0} : K_S = \mathfrak{a} + V_t\}.$$

Then

(a) *if* $t(\mathfrak{a}) < N\mathfrak{a}$, *then* $[\mathfrak{a}]$ *is a Euclidean ideal class;*

(b) *if* $t(\mathfrak{a}) > N\mathfrak{a}$ *then* $[\mathfrak{a}]$ *is* not *a Euclidean ideal class.*

PROOF. Part (a) follows directly from the definition of Euclidean ideal class. Part (b) follows from (5.2), taking $t = N\mathfrak{a}$. □

REMARK (5.6). If K is a function field over a finite field we may take $t' = t$ in (5.2): from the discreteness of the valuations in S we derive that $V_t = V_{t-\varepsilon}$ for ε small enough. Then we can use (5.2) with $t - \varepsilon$ instead of t.

§(5.3) The construction of Cassels

In this section and the next we suppose that S consists of two primes p and q. Let $\mathfrak{a}$ be an ideal of $A = A_S$. In this section we construct an element $\bar{x} \in K_S/\mathfrak{a}$ such that for every $x \in K_S$ with $x \in \bar{x}$ we have $x \notin V_t$ for some t only depending on K, S and $N\mathfrak{a}$. We want t to be as large as possible because by (5.5) we know that $\mathfrak{a}$ is not Euclidean if $t > N\mathfrak{a}$. This means that we want x to be far from $\mathfrak{a}$ with respect to the 'distance function' N. We will achieve this by demanding that $\langle \bar{x}, y \rangle_S$

(cf. section (3.5)) is near $\frac{1}{2}$ for many $y \in \mathfrak{a}^{\perp}$, which seems a reasonable choice since $\langle \mathfrak{a},\mathfrak{a}^{\perp}\rangle_S = 0$. Using this idea we arrive at the construction that Cassels used in the cases (#2^+), (#3) and (#4), cf. [C1].

LEMMA (5.7). (cf. [C1], lemmas 4, 12, 16). *Define* $Q = Nq$ *if* q *is non-archimedean and* $Q = 1$ *otherwise. Let* $k > 1$ *be in* $|K_p|_p$ *and let* $\mathfrak{a}$ *be an* A-*ideal. Finally, let constant* C_S *be as defined in (3.28). Then there exists a sequence* $(\alpha_n)_{n\in\mathbb{Z}}$ *in* $\mathfrak{a}^{\perp}$ *such that*

(a) $\quad |\alpha_n|_p \le k^{-1}|\alpha_{n-1}|_p$ for all $n \in \mathbb{Z}$;

(b) $\quad |\alpha_n|_q|\alpha_{n-1}|_p \le C_S Qk\nu(\mathfrak{a}^{\perp})$ for all $n \in \mathbb{Z}$;

(c) $\quad \lim_{n\to\infty} |\alpha_n|_p = \lim_{n\to-\infty} |\alpha_n|_q = 0$;

(d) $\quad \lim_{n\to-\infty} |\alpha_n|_p = \lim_{n\to\infty} |\alpha_n|_q = \infty$.

PROOF. Take any $\alpha_0' \neq 0$ in $\mathfrak{a}^{\perp}$. There exists a sequence $(\alpha_n')_{n>0}$ in $\mathfrak{a}^{\perp}-\{0\}$ such that $|\alpha_n'|_p \le k^{-1}|\alpha_{n-1}'|_p$ and $|\alpha_n'|_q|\alpha_{n-1}'|_p \le C_S Qk\nu(\mathfrak{a}^{\perp})$ for $n > 0$. This follows by induction on n from (3.29) with $a = k^{-1}|\alpha_{n-1}'|_p$ and $b = \sup\{b' \in |K_q|_q : ab' \le C_S Q\nu(\mathfrak{a}^{\perp})\}$. Let τ be a fundamental unit of A with $|\tau|_q < 1 < |\tau|_p$. Put $t = C_S Q\nu(\mathfrak{a}^{\perp})$ and define as in (5.2):

$$B = \{x \in V_t : |x|_p = 0 \text{ and } |x|_q \le 1, \text{ or } |x|_q = 0 \text{ and } |x|_p \le 1, \text{ or } 1 \le \frac{|x|_p}{|x|_q} \le \frac{|\tau|_p}{|\tau|_q}\}.$$

Then $\alpha_n' \in \bigcup_{m\in\mathbb{Z}} \tau^m B$ for $n \in \mathbb{Z}_{>0}$, hence there exists a unit $\eta_n \in A^*$ such that $\alpha_n'\eta_n \in \overline{B} \cap \mathfrak{a}^{\perp}$. The latter set is finite, because $\overline{B}$ is bounded and $\mathfrak{a}^{\perp}$ is discrete. Hence there exist $m,n \in \mathbb{Z}_{>0}$ with $m > n$ for which $\alpha_n'\eta_n = \alpha_m'\eta_m$. For $n \le i \le m$ we define $\alpha_i = \alpha_i'$, for $i > m$ we define inductively $\alpha_i = \alpha_{i-m+n}\eta_m^{-1}\eta_n$ and for $i < n$ we define inductively $\alpha_i = \alpha_{i+m-n}\eta_m\eta_n^{-1}$. From the construction of the α_i' we derive that $|\alpha_m'|_p < |\alpha_n'|_p$, hence $|\eta_m|_p > |\eta_n|_p$. This shows that the sequence $(\alpha_n)_{n\in\mathbb{Z}}$ satisfies (a), (b), (c) and (d). □

For an element $\bar{a} \in \mathbb{R}/\mathbb{Z}$ we define:

(5.8) $$\|\bar{a}\| = \min\{|a| : a \in \bar{a}\}.$$

In the next proposition we construct an element $\bar{x} \in K_S/\mathcal{a}$ such that $\|\langle\bar{x},\alpha_n\rangle_S\|$ is large for all $n \in \mathbb{Z}$. Afterwards we show that $N(x) = |x|_p|x|_q$ is large for all $x \in \bar{x}$.

For each $k \in |K_p|_p$ with $k > 1$ we define $f(k)$ by

(5.9)

(a) $f(k) = \frac{1}{p}$ if K is of characteristic $p > 0$;

(b) $f(k) = \frac{k'-1}{2k'}$ with $k' = \min\{p^n : |p^n|_p \le k^{-1}\}$ if K_p is a finite extension of $\mathbb{Q}_p$;

(c) $f(k) = \frac{k-2}{2(k-1)}$ if $K_p = \mathbb{R}$;

(d) $f(k) = \frac{\sqrt{k}-2}{2(\sqrt{k}-1)}$ if $K_p = \mathbb{C}$.

<u>PROPOSITION (5.10)</u>. *Suppose that* $k \in |K_p|_p$, *with* $k > 1$. *Let* $(\alpha_n)_{n\in\mathbb{Z}}$ *be a sequence in* $\mathcal{a}^\perp$ *such that* (5.7) (a), (b), (c) *and* (d) *hold. Then there exists* $\bar{x} \in K_S/\mathcal{a}$ *such that*

$$\|\langle\bar{x},\alpha_n\rangle_S\| \ge f(k) \quad \text{for all} \quad n \in \mathbb{Z}.$$

<u>PROOF</u>. Using the compactness of $K_S/\mathcal{a}$ we only have to construct for each pair $m,\ell \in \mathbb{Z}$ with $m < \ell$, an element $\bar{x}_{m,\ell} \in K_S/\mathcal{a}$ such that $\|\langle\bar{x}_{m,\ell},\alpha_n\rangle_S\| \ge f(k)$ for all n with $m \le n \le \ell$. After renumbering we may suppose that $\ell = 0$ and $m < 0$. Let β_n denote the p-coordinate of α_n. It suffices to find $x_m \in K_p$ such that

(5.11) $$\|\langle x_m,\beta_n\rangle_p\| \ge f(k), \quad \text{for} \quad m \le n \le 0,$$

because then we may take $\bar{x}_{m,\ell} = (x_m,0) \bmod \mathcal{a}$.

(a) Suppose that K is of characteristic $p > 0$. Then $K_p = \mathbb{F}_q((t_p))$ for some power q of p. Here t_p is a prime element of $\tilde{O}_p$. Let

Tr: $\mathbb{F}_q \to \mathbb{F}_p$ be the trace map. Choose $\xi \in \mathbb{F}_q$ such that $\mathrm{Tr}(\xi) \neq 0$. As in (3.9)(c) let $\mathrm{res}_p\colon K_p \to \mathbb{F}_q$ be the map that sends every element of K_p to its coefficient at t_p^{-1}.

By induction on $m \in \mathbb{Z}_{\leq 0}$ we construct a sequence $(x_m)_{m \leq 0}$ in K_p such that

$$\mathrm{res}_p(x_m\beta_n) = \xi \quad \text{if} \quad m \leq n \leq 0.$$

Then (5.11) is satisfied. For $m = 0$ we take $x_0 = \xi(\beta_0 t_p)^{-1}$. Now we suppose that $m < 0$. Then we define

$$x_m = (\xi - \mathrm{res}_p(x_{m+1}\beta_m))(\beta_m t_p)^{-1} + x_{m+1}.$$

For $n \in \mathbb{Z}$ we have

$$\mathrm{res}_p(x_m\beta_n) = (\xi - \mathrm{res}_p(x_{m+1}\beta_m))\mathrm{res}_p(\beta_n\beta_m^{-1}t_p^{-1}) + \mathrm{res}_p(x_{m+1}\beta_n).$$

If $n = m$ we get $\mathrm{res}_p(x_m\beta_n) = \xi$. If $m < n \leq 0$ then $|\beta_n\beta_m^{-1}|_p < 1$ by (5.7)(a), hence $\mathrm{res}_p(\beta_n\beta_m^{-1}t_p^{-1}) = 0$ and $\mathrm{res}_p(x_m\beta_n) = \mathrm{res}_p(x_{m+1}\beta_n) = \xi$ by induction.

(b) Suppose that K_p is a finite extension of $\mathbb{Q}_p$. Define k' as in (5.9)(b). Let $\kappa \in K_p$ be an element with $|\kappa|_p = k$.

The function $\lambda \circ \mathrm{Tr}\colon K_p \to \mathbb{R}/\mathbb{Z}$ is continuous and non-zero. Hence there exists a minimal integer $i \in \mathbb{Z}$ such that $\lambda \circ \mathrm{Tr}(p^i) = 0$. For $t \in \mathbb{Z}_{\geq 0}$ we have $\lambda \circ \mathrm{Tr}(\kappa p^i) \subset \mathbb{Z} \cdot p^{-t}/\mathbb{Z}$ if and only if $p^t\kappa p^i \subset p^i$ which happens if and only if $p^t \geq k'$. This shows that $\lambda \circ \mathrm{Tr}(\kappa p^i) = \mathbb{Z} \cdot k'^{-1}/\mathbb{Z}$. With induction on $m \in \mathbb{Z}_{\leq 0}$ we construct a sequence $(x_m)_{m \leq 0}$ in K_p such that

$$\text{(5.12)} \qquad \left\|\lambda \circ \mathrm{Tr}(x_m\beta_n) - \tfrac{1}{2}\right\| \leq \frac{1}{2k'} \quad \text{if} \quad m \leq n < 0.$$

Then (5.11) is satisfied. If $m = 0$ we choose $x_0 \in K_p$ such that $x_0\beta_0 \in \kappa p^i$ and

$$\lambda \circ \mathrm{Tr}(x_0\beta_0) = \frac{k' - 1}{2k'} \quad \text{if} \quad p \text{ is odd ;}$$

$$\lambda \circ \mathrm{Tr}(x_0\beta_0) = \frac{1}{2} \quad \text{if} \quad p = 2.$$

Then clearly (5.12) holds. Now suppose that $m < 0$. Then we choose $y_m \in K_p$ such that $y_m\beta_m \in \kappa p^i$ and

$$||\lambda \circ \mathrm{Tr}(y_m\beta_m) + \lambda \circ \mathrm{Tr}(x_{m+1}\beta_m) - \tfrac{1}{2}|| \leq \frac{1}{2k'},$$

which is possible because $\lambda \circ \mathrm{Tr}(\kappa p^i) = \mathbb{Z} \cdot k'^{-1}/\mathbb{Z}$. We take $x_m = x_{m+1} + y_m$. Then for $n \in \mathbb{Z}$ we have

$$\lambda \circ \mathrm{Tr}(x_m\beta_n) = \lambda \circ \mathrm{Tr}(y_m\beta_n) + \lambda \circ \mathrm{Tr}(x_{m+1}\beta_n).$$

If $n = m$ we have $||\lambda \circ \mathrm{Tr}(x_m\beta_n) - \frac{1}{2}|| \leq \frac{1}{2k'}$ by construction. If $m < n \leq 0$ we have $|\beta_n|_p \leq |\kappa^{-1}\beta_m|_p$ by (5.7)(a), so $y_m\beta_n \in p^i$ and $\lambda \circ \mathrm{Tr}(y_m\beta_n) = 0$. By induction this shows that (5.12) holds.

(c) Suppose that $K_p = \mathbb{R}$. There exists $x_0 \in K_p$ such that $x_0\beta_0 \equiv$ $\equiv \frac{1}{2} \bmod \mathbb{Z}$. With induction on $m \in \mathbb{Z}_{\leq 0}$ we choose $x_m \in K_p = \mathbb{R}$ such that $x_m\beta_m \equiv \frac{1}{2} \bmod \mathbb{Z}$ and $|x_m\beta_m - x_{m+1}\beta_m|_p \leq \frac{1}{2}$. Then for $m \leq n \leq 0$ we have

$$\begin{aligned}||(x_m\beta_n - \tfrac{1}{2}) \bmod \mathbb{Z}|| &= ||(x_m - x_n)\beta_n \bmod \mathbb{Z}|| \leq \\ &\leq |x_m - x_n|_p|\beta_n|_p \leq \sum_{j=m}^{n-1} |x_j - x_{j+1}|_p|\beta_n|_p \leq \frac{1}{2}\sum_{j=m}^{n-1} |\beta_n\beta_j^{-1}|_p \leq \\ &\leq \frac{1}{2}\sum_{j=m}^{n-1} k^{j-n} < \frac{1}{2(k-1)},\end{aligned}$$

hence (5.11) is satisfied.

(d) Suppose that $K_p = \mathbb{C}$. There exists $x_0 \in K_p$ such that $x_0\beta_0 \equiv$ $\equiv \frac{1}{4} \bmod (\frac{1}{2}\mathbb{Z} + i\mathbb{R})$. With induction on $m \in \mathbb{Z}_{\leq 0}$ we choose $x_m \in K_p = \mathbb{C}$ such that $x_m\beta_m \equiv \frac{1}{4} \bmod (\frac{1}{2}\mathbb{Z} + i\mathbb{R})$ and $|x_m\beta_m - x_{m+1}\beta_m|_p \leq \frac{1}{16}$. (Recall that $|\cdot|_p$ is the square of the usual absolute value on $\mathbb{C}$.) Notice that this is possible since the lines $\frac{1}{4} \bmod (\frac{1}{2}\mathbb{Z} + i\mathbb{R})$ are spaced $\frac{1}{2}$ apart. Let $\mathrm{Tr}\colon \mathbb{C} \to \mathbb{R}$ be the trace function. For $m \leq n \leq 0$ we have

$$\begin{aligned}||(\mathrm{Tr}(x_m\beta_n) - \tfrac{1}{2}) \bmod \mathbb{Z}|| &= ||\mathrm{Tr}((x_m - x_n)\beta_n) \bmod \mathbb{Z}|| \leq \\ &\leq 2|x_m - x_n|_p^{\frac{1}{2}}|\beta_n|_p^{\frac{1}{2}} \leq \frac{1}{2}\sum_{j=m}^{n-1} |\beta_n\beta_j^{-1}|_p^{\frac{1}{2}} \leq \frac{1}{2}\sum_{j=m}^{n-1} k^{\frac{1}{2}(j-n)} < \frac{1}{2(\sqrt{k}-1)},\end{aligned}$$

hence (5.11) holds. □

The construction of $\bar{x}$ in the last proposition shows that $\bar{x}$ is a limit of $(\bar{x}_m)_{m \leq 0}$, where $\bar{x}_m$ is of the form $(x_m,0)+a$. The element $\bar{x}$ itself is not of the form $(x,0)+a$, as we will see below. In fact we will prove that for any $x \in \bar{x}$ we have $N(x) \neq 0$, whereas $N((x_m,0)) = 0$.

LEMMA (5.13). *Let* $(\alpha_n)_{n \in \mathbb{Z}}$ *be a sequence in* $a^{\perp}$ *such that* (5.7) (a), (b), (c) *and* (d) *hold and let* $\bar{x} \in K_S/a$ *be such that* $\|\langle\bar{x},\alpha_n\rangle_S\| \geq f(k)$ *for all* $n \in \mathbb{Z}$. *Then for all* $x \in \bar{x}$ *we have* $N(x) \neq 0$.

PROOF. Suppose on the contrary that $N(x) = 0$ for some $x \in \bar{x}$. Then $x_p = 0$ or $x_q = 0$. If $x_p = 0$ we have $\lim_{n\to-\infty} \langle x,\alpha_n\rangle_S = \lim_{n\to-\infty} \langle x,\alpha_n\rangle_q = 0$ by (5.7)(c), a contradiction to our assumption on $\bar{x}$. In a similar way we derive a contradiction by supposing that $x_q = 0$. □

Now we will improve upon (5.13) in the sense that we will give a positive lower bound on $N(x)$ for $x \in \bar{x}$ where $\bar{x}$ is as constructed in (5.10). First we prove two lemmas.

LEMMA (5.14). *Let* u, v, a *and* b *be positive real numbers such that* $u \leq a$, $v \leq a$ *and* $uv \leq b$. *then*

$$u+v \leq a+\frac{b}{a}.$$

PROOF. We have $0 \leq (a-u)(a-v) = a^2-(u+v)a+uv \leq a^2-(u+v)a+b$, so $u+v \leq a+\frac{b}{a}$. □

LEMMA (5.15). *Let* u, v, a *and* b *be positive real numbers with* $b > 1$.. *Suppose that*

$$u \leq ab^2, \quad v \leq a\left(\frac{b^2+b}{2}\right) \quad \textit{and} \quad uv^2 \leq a^3\left(\frac{b^2+b}{2}\right)^2.$$

Then

$$u+2v \leq a(b^2+b+1).$$

PROOF. By monotonicity we see that for fixed a and b the maximum of $u+2v$ is attained at one of the points with $u = ab^2$, $v = a(\frac{b+1}{2})$ or $v = a(\frac{b^2+b}{2})$, $u = a$. In both points we have $u+2v = a(b^2+b+1)$. □

PROPOSITION (5.16). *Let* k *be an element of* $|K_p|_p$ *with* $k > 1$. *Let* $(\alpha_n)_{n \in \mathbb{Z}}$ *be a sequence in* $a^{\perp}$ *such that* (5.7) (a), (b), (c) *and* (d) *hold and let* $\bar{x} \in K_S/a$ *be such that* $\|\langle\bar{x},\alpha_n\rangle_S\| \geq f(k)$ *for all* $n \in \mathbb{Z}$. *Then for all* $x \in \bar{x}$ *we have*

$$N(x) \geq g(K,p,k)Na$$

for the following values of $g(K,p,k)$:

(F) $$g(K,p,k) = \frac{Np}{k} q^{g-1}$$

if K *is a function field of genus* g, *defined over* $\mathbb{F}_q$.

($\#2^+$) $$g(K,p,k) = \frac{k(k-2)^2}{4(k^2-1)^2}\sqrt{\Delta}$$

if $K = \mathbb{Q}(\sqrt{\Delta})$ *where* $\Delta > 0$ *is the discriminant of* K.

($\#2^-$) $$g(K,p,k) = \frac{\sqrt{3}}{16}\frac{Np}{k}\left(\frac{k'-1}{k'}\right)\sqrt{|\Delta|}$$

if $K = \mathbb{Q}(\sqrt{\Delta})$, *where*

$\Delta < 0$ *is the discriminant of* K;

p *is a non-archimedean prime of* K;

$k' = k$ *if* p *lies over a splitting prime in* $K/\mathbb{Q}$;

$k' = p^n$ *if* p *lies over an inert or a ramifying prime* p *in* $K/\mathbb{Q}$ *with* $k = p^{2n}$ or $k = p^{2n-1}$.

($\#3$) $$g(K,p,k) = \frac{\sqrt{3}}{32}\frac{k(k-2)^3}{(k^{1/2}+1)(k^{3/2}-1)^3}\sqrt{|\Delta(K)|}$$

if $[K:\mathbb{Q}] = 3$ *and* $K_p = \mathbb{R}$, $K_q = \mathbb{C}$.

($\#4$) $$g(K,p,k) = \frac{\pi\sqrt{3}}{512}\frac{k(k^{\frac{1}{2}}-2)^4}{(k-1)^4}\sqrt{\Delta(K)}$$

if $[K:\mathbb{Q}] = 4$ *and* $K_p = K_q = \mathbb{C}$.

PROOF. From (5.13) we know that $|x|_p \neq 0$ and $|x|_q \neq 0$. This will be used throughout the proof.

(F) Suppose that K is a function field of genus g, defined over $\mathbb{F}_q$.

By (5.7)(c), (d) there exists $n \in \mathbb{Z}$ such that

$$|\alpha_{n-1}x|_q \leq 1 < |\alpha_n x|_q.$$

Then $|\alpha_n x|_q \geq Nq$. Also $<\alpha_{n-1},x>_q = 0$ by (3.9)(c). So (5.10) implies that $<\alpha_{n-1},x>_p \neq 0$. In particular $|\alpha_{n-1}x|_p > 1$, so $|\alpha_{n-1}x|_p \geq Np$. We then find that

$$\begin{aligned} NpNq &\leq |\alpha_{n-1}x|_p |\alpha_n x|_q \\ &\leq C_S Nqk\nu(a^\perp)N(x) \qquad \text{by (5.7)(b)} \\ &= Nqkq^{1-g}(Na)^{-1}N(x). \end{aligned}$$

The last equality follows from (3.28), (3.21) and (3.22)(b). Hence

$$N(x) \geq \frac{Np}{k} q^{g-1} Na.$$

(#2$^+$) Suppose that $K = \mathbb{Q}(\sqrt{\Delta})$ with discriminant $\Delta > 0$. By (5.7)(c), (d) there exists $n \in \mathbb{Z}$ such that

$$|\alpha_{n-1}x|_q \leq (N(x)k\nu(a^\perp))^{\frac{1}{2}} < |\alpha_n x|_q.$$

Combining the second inequality with (5.7)(b) and (3.28) gives

$$|\alpha_{n-1}x|_p < (N(x)k\nu(a^\perp))^{\frac{1}{2}}.$$

Multiplication of (5.7)(a) by (5.7)(b) gives

$$|\alpha_{n-1}x|_p |\alpha_{n-1}x|_q \leq N(x)\nu(a^\perp).$$

Hence we may use (5.14) with $u = |\alpha_{n-1}x|_p$, $v = |\alpha_{n-1}x|_q$, $a = (N(x)k\nu(a^\perp))^{\frac{1}{2}}$ and $b = N(x)\nu(a^\perp)$ to obtain

$$|\alpha_{n-1}x|_p + |\alpha_{n-1}x|_q \leq (\nu(a^\perp)N(x))^{\frac{1}{2}}(k^{\frac{1}{2}} + k^{-\frac{1}{2}}),$$

so

$$\left(\frac{k-2}{2(k-1)}\right)^2 \le \|\langle\alpha_{n-1},x\rangle_S\|^2 \qquad \text{by (5.10)}$$

$$\le (|\alpha_{n-1}x|_p + |\alpha_{n-1}x|_q)^2$$

$$\le \nu(a^\perp)N(x)(k^{\frac{1}{2}} + k^{-\frac{1}{2}})^2 =$$

$$= (Na)^{-1}(\sqrt{\Delta})^{-1}N(x)(k^{\frac{1}{2}} + k^{-\frac{1}{2}})^2 \qquad \text{by (3.21) and (3.22)(a)}$$

and therefore

$$N(x) \ge \frac{k(k-2)^2}{4(k^2-1)^2}\sqrt{\Delta}\,Na\,.$$

($\#2^-$) Suppose that $K = \mathbb{Q}(\sqrt{\Delta})$ with discriminant $\Delta < 0$ and that K_p is non-archimedean. Then $K_q = \mathbb{C}$. By (5.7)(c), (d) there exists $n \in \mathbb{Z}$ such that

$$|\alpha_n x|_p < N(\mathcal{D}(K_p))Np \le |\alpha_{n-1}x|_p$$

From the definition of the local different and (3.9)(b) we get $\langle\alpha_n,x\rangle_p = 0$. From the second inequality we get

$$|\alpha_n x|_q \le C_S Qk\nu(a^\perp)N(\mathcal{D}(K_p))^{-1}Np^{-1}N(x) \qquad \text{by (5.7)(b)}$$

$$= \frac{1}{\sqrt{3}}\,k\nu(a^\perp)N(\mathcal{D}(K_p))^{-\frac{1}{2}}Np^{-1}N(x) \qquad \text{by (3.28)}$$

$$= \frac{1}{\sqrt{3}}\,k(Na)^{-1}N(\mathcal{D}(A))^{-\frac{1}{2}}N(\mathcal{D}(K_p))^{-\frac{1}{2}}Np^{-1}N(x) \qquad \text{by (3.21) and (3.22)(a)}$$

$$= \frac{1}{\sqrt{3}}\,k(Na)^{-1}\sqrt{|\Delta|}\;Np^{-1}N(x)$$

The last equality by (3.5) and the definition of the discriminant. Thus

$$\left(\frac{k'-1}{2k'}\right)^2 \le \|\langle\alpha_n,x\rangle_S\|^2 \qquad \text{by (5.10)}$$

$$= \|\langle\alpha_n,x\rangle_q\|^2 \le 4|\alpha_n x|_q \qquad \text{by (3.9)(b)}$$

$$\le \frac{4}{\sqrt{3}}\,k(Na)^{-1}\sqrt{|\Delta|}\;Np^{-1}\;N(x)\,.$$

This shows that

$$N(x) \geq \frac{\sqrt{3}}{16}\frac{N\mathfrak{p}}{k}\left(\frac{k'-1}{k'}\right)^2 \sqrt{|\Delta|}\ N\mathfrak{a}\,.$$

If p is the rational prime in $\mathfrak{p}$ we have $k' = \min\{p^n : |p^n|_{\mathfrak{p}} \leq k^{-1}\}$. If p is splitting in $K/\mathbb{Q}$ we have $|p^n|_{\mathfrak{p}} = p^{-n}$, which shows that $k' = k$. If p is inert or ramifying in $K/\mathbb{Q}$ we have $|p^n|_{\mathfrak{p}} = p^{-2n}$, which shows that $k' = p^n$ if $k = p^{2n}$ or $k = p^{2n-1}$.

(#3) Suppose that $[K:\mathbb{Q}] = 3$, with $K_{\mathfrak{p}} = \mathbb{R}$ and $K_{\mathfrak{q}} = \mathbb{C}$. By (5.7) there exists $n \in \mathbb{Z}$ such that

$$|\alpha_{n-1}x|_{\mathfrak{q}} \leq \left(\tfrac{1}{4}C_S^2\,\nu(\mathfrak{a}^{\perp})^2 N(x)^2 k(1+k^{\frac{1}{2}})^2\right)^{1/3} < |\alpha_n x|_{\mathfrak{q}}$$

Combining the second inequality with (5.7)(b) gives

$$|\alpha_{n-1}x|_{\mathfrak{p}} < \left(4C_S\nu(\mathfrak{a}^{\perp})N(x)\frac{k^2}{(1+k^{\frac{1}{2}})^2}\right)^{1/3}.$$

Multiplication of (5.7)(a) by (5.7)(b) gives

$$|\alpha_{n-1}x|_{\mathfrak{p}}|\alpha_{n-1}x|_{\mathfrak{q}} \leq C_S\nu(\mathfrak{a}^{\perp})N(x)\,.$$

Hence we may use (5.15) with $u = |\alpha_{n-1}x|_{\mathfrak{p}}$, $v = |\alpha_{n-1}x|_{\mathfrak{q}}^{\frac{1}{2}}$, $a = \left(\frac{4C_S\nu(\mathfrak{a}^{\perp})N(x)}{k(1+k^{\frac{1}{2}})^2}\right)^{1/3}$ and $b = k^{\frac{1}{2}}$ to obtain

$$|\alpha_{n-1}x|_{\mathfrak{p}} + 2|\alpha_{n-1}x|_{\mathfrak{q}}^{\frac{1}{2}} \leq \left(\frac{4C_S\nu(\mathfrak{a}^{\perp})N(x)}{k(1+k^{\frac{1}{2}})^2}\right)^{1/3}(k+k^{\frac{1}{2}}+1),$$

so

$$\begin{aligned}\left(\frac{k-2}{2(k-1)}\right)^3 &\leq \|\langle\alpha_{n-1},x\rangle_S\|^3 \qquad\qquad \text{by (5.10)}\\ &\leq \left(|\alpha_{n-1}x|_{\mathfrak{p}} + 2|\alpha_{n-1}x|_{\mathfrak{q}}^{\frac{1}{2}}\right)^3\\ &\leq 4C_S\nu(\mathfrak{a}^{\perp})N(x)\frac{(k+k^{\frac{1}{2}}+1)^3}{k(1+k^{\frac{1}{2}})^2}\\ &= \frac{4}{\sqrt{3}}(N\mathfrak{a})^{-1}\sqrt{|\Delta(K)|}^{\,-1}\,N(x)\,\frac{(k+k^{\frac{1}{2}}+1)^3}{k(1+k^{\frac{1}{2}})^2}\,,\end{aligned}$$

the last equality by (3.28), (3.21) and (3.22)(a). This shows that

$$N(x) \geq \frac{\sqrt{3}}{32} \frac{k(k-2)^3}{(k^{1/2}+1)(k^{3/2}-1)^3} \sqrt{|\Delta(K)|}\; N\mathfrak{a}\,.$$

(#4) Suppose that $[K:\mathbb{Q}] = 4$ and $K_p = K_q = \mathbb{C}$. By (5.7)(c), (d) there exists $n \in \mathbb{Z}$ such that

$$|\alpha_{n-1}x|_q \leq (C_S\nu(\mathfrak{a}^\perp)N(x)k)^{\frac{1}{2}} < |\alpha_n x|_q\,.$$

Combining the second inequality with (5.7)(b) gives

$$|\alpha_{n-1}x|_p \leq (C_S\nu(\mathfrak{a}^\perp)N(x)k)^{\frac{1}{2}}\,.$$

Multiplication of (5.7)(a) by (5.7)(b) gives

$$|\alpha_{n-1}x|_p|\alpha_{n-1}x|_q \leq C_S\nu(\mathfrak{a}^\perp)N(x)\,.$$

Hence we may use (5.14) with $u = |\alpha_{n-1}x|_p^{\frac{1}{2}}$, $v = |\alpha_{n-1}x|_q^{\frac{1}{2}}$, $b = (C_S\nu(\mathfrak{a}^\perp)N(x))^{\frac{1}{2}}$ and $a = k^{\frac{1}{4}}b^{\frac{1}{2}}$ to get

$$|\alpha_{n-1}x|_p^{\frac{1}{2}} + |\alpha_{n-1}x|_q^{\frac{1}{2}} \leq (C_S\nu(\mathfrak{a}^\perp)N(x))^{\frac{1}{4}}(k^{\frac{1}{4}} + k^{-\frac{1}{4}}),$$

thus

$$\begin{aligned}
\left(\frac{k^{\frac{1}{2}}-2}{2(k^{\frac{1}{2}}-1)}\right)^4 &\leq \|\langle\alpha_{n-1},x\rangle_S\|^4 && \text{by (5.10)}\\
&\leq 16(|\alpha_{n-1}x|_p^{\frac{1}{2}} + |\alpha_{n-1}x|_q^{\frac{1}{2}})^4\\
&\leq 16C_S\nu(\mathfrak{a}^\perp)N(x)(k^{\frac{1}{4}} + k^{-\frac{1}{4}})^4\\
&= \frac{32}{\pi\sqrt{3}}(N\mathfrak{a})^{-1}\sqrt{\Delta(K)}^{-1}N(x)(k^{\frac{1}{4}} + k^{-\frac{1}{4}})^4,
\end{aligned}$$

the last equality by (3.28), (3.21) and (3.22)(a). Therefore

$$N(x) \geq \frac{\pi\sqrt{3}}{512}\frac{k(k^{\frac{1}{2}}-2)^4}{(k-1)^4}\sqrt{\Delta(K)}\; N\mathfrak{a}\,. \quad \square$$

REMARK (5.17). The parts $(\#2^+)$, $(\#3)$ and $(\#4)$ of (5.16) were already proven by Cassels [C1], although he made an error in the estimate for case $(\#4)$ ([C1] lemmas 16,19). This mistake led to a better bound on the discriminant for quartic fields with a Euclidean ring of integers than we will derive in (5.19).

REMARK (5.18). There is an asymmetry in the cases $(\#2^-)$ and $(\#3)$. We can also obtain a value of $g(K,p,k)$ where $K_p = \mathbb{C}$ for those cases. However the results derived in this way are worse than those found in (5.16). This is possibly due to the fact that $f(k)$ may not be best possible in the case that $K_p = \mathbb{C}$. However, we failed to sharpen it.

§(5.4) Bounds on the discriminant and the genus

In this section we use (5.16) to obtain bounds on the discriminant or the genus in the case that A_S has a Euclidean ideal class.

THEOREM (5.19). *Let* K *be a global field and let* $S \supset S_\infty$ *be a set of two primes of* K. *If* $A = A_S$ *has a Euclidean ideal class we are in one of the following cases*

(F) K *is a function field of genus* 0 *over a finite field;*

$(\#1)$ $K = \mathbb{Q}$;

$(\#2^+)$ $K = \mathbb{Q}(\sqrt{\Delta})$ *with discriminant* $0 < \Delta \le 2577$;

$(\#2^-)$ $K = \mathbb{Q}(\sqrt{\Delta})$ *with discriminant* $0 > \Delta \ge -1364$, *moreover if* $S = \{p,\infty\}$ *and* p *is the rational prime in* p *we have*

$$|\Delta| \le \frac{256}{3}\left(\frac{\mathrm{p}}{\mathrm{p}-1}\right)^4;$$

$(\#3)$ $[K:\mathbb{Q}] = 3$ *and* $0 > \Delta(K) \ge -170520$;

$(\#4)$ $[K:\mathbb{Q}] = 4$ *and* $0 < \Delta(K) \le 230202117$.

PROOF. If $\#S = 2$ we are in one of the cases (F), $(\#1)$, $(\#2^+)$, $(\#2^-)$, $(\#3)$ or $(\#4)$, cf. (0.17). We show that when $K \ne \mathbb{Q}$, i.e. when we are not in case $(\#1)$, the ring A must satisfy the given restrictions. In all cases we use (5.10) to get for all $k \in |K_p|_p$ with $k > 1$ a residue class $\bar{x}$ of $K_S/\mathfrak{a}$, such that every element $x \in \bar{x}$ has norm $N(x) > g(K,p,k)$ for some $g(K,p,k)$ determined in (5.16). If $\mathfrak{a}$ is Euclidean we use (5.5) to find that $g(K,p,k) \le 1$. In case (F) we even have $g(K,p,k) < 1$ by (5.6).

(F) Suppose that K is a function field of genus g, defined over $\mathbb{F}_q$, then $g(K,p,k) = \frac{Np}{k} q^{g-1}$. Because $g(K,p,k) < 1$ we have $g(K,p,k) \le q^{-1}$. We choose $k = Np$ to get $q^{g-1} \le q^{-1}$, i.e. $g = 0$.

($\#2^+$) Suppose that $K = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta > 0$, then

$$g(K,p,k) = \frac{k(k-2)^2}{4(k^2-1)^2} \sqrt{\Delta} .$$

Hence $g(K,p,k) \le 1$ if and only if

$$\Delta \le \frac{16(k^2-1)^4}{k^2(k-2)^4} .$$

The right-hand side has a minimum near $k = 5.52$. Substituting $k = 5.52$ gives $\Delta \le 2579.97$. Because $\Delta \equiv 0,1 \bmod 4$ we have $\Delta \le 2577$.

($\#2^-$) Suppose that $K = \mathbb{Q}(\sqrt{\Delta})$, with $\Delta < 0$, and $S = \{p,\infty\}$, with p non-archimedean. Let p be the rational prime in p. We have

$$g(K,p,k) = \frac{\sqrt{3}}{16} \frac{Np}{k} \left(\frac{k'-1}{k'}\right)^2 \sqrt{|\Delta|} .$$

Hence $g(K,p,k) \le 1$ if and only if

$$|\Delta| \le \frac{256}{3} \left(\frac{k}{Np}\right)^2 \left(\frac{k'}{k'-1}\right)^4 .$$

We choose $k = Np$, then $k' = p$, and we get

$$|\Delta| \le \frac{256}{3} \left(\frac{p}{p-1}\right)^4 \le \frac{256}{3} \cdot 16 = 1365.33\ldots ,$$

because $\frac{p}{p-1} \le 2$. Since $\Delta \equiv 0,1 \bmod 4$ and $\Delta < 0$ we even have $|\Delta| \le 1364$.

($\#3$) Suppose that $[K:\mathbb{Q}] = 3$, then

$$g(K,p,k) = \frac{\sqrt{3}}{32} \frac{k(k-2)^3}{(k^{1/2}+1)(k^{3/2}-1)^3} \sqrt{|\Delta(K)|}$$

Hence $g(K,p,k) \le 1$ if and only if

$$|\Delta(K)| \le \frac{1024}{3} \frac{(k^{1/2}+1)^2(k^{3/2}-1)^6}{k^2(k-2)^6} .$$

The right-hand side has a minimum near $k = 7.46$. Substituting $k = 7.46$

gives $|\Delta(K)| \le 170522.95$. Since $\Delta \equiv 0,1 \bmod 4$ and $\Delta(K) < 0$ we even have $|\Delta(K)| \le 170520$.

(#4) Suppose that $[K:\mathbb{Q}] = 4$, then

$$g(K,p,k) = \frac{\pi\sqrt{3}}{512}\,\frac{k(k^{\frac{1}{2}}-2)^4}{(k-1)^4}\,\sqrt{\Delta(K)}.$$

Hence $g(K,p,k) \le 1$ if and only if

$$\Delta(K) \le \frac{262144}{3\pi^2}\,\frac{(k-1)^8}{k^2(k^{\frac{1}{2}}-2)^8}$$

The right-hand side has a minimum near $k = (5.5223)^2$. Substituting $k = (5.5223)^2$ gives $\Delta(K) \le 230202118.0\ldots$. Because $\Delta(K) \equiv 0,1 \bmod 4$ we even have $\Delta(K) \le 230202117$. □

The latter theorem proves the cases (F), (#3), (#4) of (0.19) and (1.10), except for the assertions about the class numbers. In case (F) the value of the class number follows from (4.6). For the cases (#3) and (#4) the bounds on the class numbers will be derived in section (10.1).

§(5.5) Real quadratic rings of integers with a Euclidean ideal class

In this section we finish the proofs for the case $(\#2^+)$. Theorem (0.19) $(\#2^+)$ is already known, cf. section (0.6), so we only have to deal with (1.10). From (2.12) we know that we only have to consider rings with class number equal to 2. Instead of the bound on the discriminant of (5.19) $(\#2^+)$ we use a result of Ennola [E]. He got a result like (5.16) $(\#2^+)$ for a certain series $(\alpha_n)_{n\in\mathbb{Z}}$ in $\mathfrak{a}^{\perp}$ where $g(K,p,k)$ is replaced by $\frac{1}{16+6\sqrt{6}}\sqrt{\Delta}$. Hence $\mathcal{O}(K)$ has a Euclidean ideal class only if the discriminant of K satisfies

(5.20) $$\Delta < (16+6\sqrt{6})^2 = 942.30\ldots\ .$$

This is the bound that we use in this section. If we use the bound of (5.19) $(\#2^+)$ the method would also work but then we have to do a larger amount of work.

First we prove the 'if' part.

<u>THEOREM (5.21)</u>. *The rings of integers of* $\mathbb{Q}(\sqrt{\Delta})$, *with* $\Delta \in \{40,60,85\}$ *have a non-principal Euclidean ideal class.*

<u>PROOF</u>. In all cases we have $h(K) = 2$, cf. [I].

First suppose that $\Delta = 40$, then $\mathcal{O} = \mathbb{Z}[\sqrt{10}]$. We prove that $\mathfrak{a} = \mathbb{Z}\cdot 3 + \mathbb{Z}(1+\sqrt{10})$ is Euclidean. The norm of $\mathfrak{a}$ is equal to 3. Let α be an element of K. Then there exist $x,y \in \mathbb{Q}$ such that $|y| \le \frac{1}{2}$, $|3x+y| \le \frac{3}{2}$ and $\alpha \equiv 3x + (1+\sqrt{10})y \bmod \mathfrak{a}$. For the norm we get

$$N(3x+(1+\sqrt{10})y) = |(3x+y)^2 - 10y^2| \le \max\{|3x+y|^2, 10y^2\} \le$$
$$\le \max\{\tfrac{9}{4}, \tfrac{5}{2}\} < 3 = N\mathfrak{a},$$

i.e. $\mathfrak{a}$ is Euclidean

Now suppose that $\Delta = 60$, then $\mathcal{O} = \mathbb{Z}[\sqrt{15}]$. The unit $\eta = 4+\sqrt{15}$ is a fundamental unit of $\mathcal{O}$. We prove that $\mathfrak{a} = \mathbb{Z}\cdot 3 + \mathbb{Z}\cdot\sqrt{15}$ is Euclidean. The norm of $\mathfrak{a}$ equals 3. Let α be an element of K. There exist $x,y \in \mathbb{Q}$ with $|x| \le \frac{1}{2}$ and $|y| \le \frac{1}{2}$ such that $\alpha \equiv \beta \bmod \mathfrak{a}$, where $\beta = 3x + y\sqrt{15}$. Since the norm of β does not depend on the sign of x and y we may suppose that $x \ge 0$ and $y \ge 0$. If $x \ge \frac{3}{10}$ we have $N(\beta) = |9x^2 - 15y^2| \le \max\{\frac{9}{4}, -\frac{81}{100}+\frac{15}{4}\} < 3 = N\mathfrak{a}$. If $y \le \frac{3}{7}$ we have $N(\beta) \le \max\{\frac{9}{4}, \frac{135}{49}\} < 3$. Now suppose that $x < \frac{3}{10}$ and $y > \frac{3}{7}$. Then we have $\eta\beta = u + v\sqrt{15}$, with $\frac{12}{7} \le v = 3x+4y \le \frac{29}{10}$. If $v \le \frac{17}{7}$ or $v \ge \frac{18}{7}$ we may shift $\eta\beta$ by an element of $\mathfrak{a}$ to $3x' + y'\sqrt{15}$ with $|y'| \le \frac{3}{7}$, thus $N(\eta^{-1}(3x'+y'\sqrt{15})) < 3$ and $\eta^{-1}(3x'+y'\sqrt{15}) \equiv \alpha \bmod \mathfrak{a}$. In the remaining case we have $\frac{17}{7} < 3x+4y < \frac{18}{7}$, thus $\frac{1}{7} < x < \frac{2}{7}$ and $\frac{225}{49} < 9(x-1)^2 < \frac{324}{49}$. Because $\frac{3}{7} < y \le \frac{1}{2}$ we have $\frac{15}{4} < 15(y-1)^2 \le \frac{240}{49}$. This gives $N(\beta - (3+\sqrt{15})) < \max\{-\frac{225}{49}+\frac{240}{49}, \frac{324}{49}-\frac{15}{4}\} < 3$ and we may conclude that $\mathfrak{a}$ is Euclidean.

Finally suppose that $\Delta = 85$, then $\mathcal{O} = \mathbb{Z}[\omega]$, with $\omega = \frac{1}{2}(1+\sqrt{85})$. The unit $\eta = 4+\omega$ is a fundamental unit of $\mathcal{O}$. We prove that $\mathfrak{a} = \mathbb{Z}\cdot 3 + \mathbb{Z}\cdot\omega$ is Euclidean. For each $x,y \in \mathbb{Q}$ we have

$$N(3x+(3+\omega)y) = |(3x+\tfrac{7}{2}y)^2 - \tfrac{85}{4}y^2| = |3(3x^2+7xy-3y^2)| =$$

$$= N(-3y+(3+\omega)x).$$

Let α be an element of K. Suppose there exists $\beta = 3x+(3+\omega)y \in \alpha + \mathfrak{a}$ such that $|x| \le \frac{3}{8}$ or $|y| \le \frac{3}{8}$. Then there exists such β with $|3y - \frac{7}{2}x| \le \frac{3}{2}$ in the former case and $|3x + \frac{7}{2}y| \le \frac{3}{2}$ in the latter. Then $N(\beta) < \max\{\frac{9}{4}, \frac{85}{4}(\frac{3}{8})^2\} < 3 = N\mathfrak{a}$ and we are done in this case. In the remaining case there exists $\beta = 3x+(3+\omega)y \in \alpha + \mathfrak{a}$ with $\frac{3}{8} < |x| \le \frac{1}{2}$ and $\frac{3}{8} < |y| \le \frac{1}{2}$. After applying the substitution $(x,y) \longmapsto (-y,x)$ several times if necessary we may suppose that $x \le 0$ and $y \ge 0$. Then $\eta\beta = 3(x+3y) + (3x+8y)(3+\omega)$ with $\frac{5}{8} \le x+3y \le \frac{9}{8}$, in particular $|x+3y-1| \le \frac{3}{8}$. Hence by the above computation there exists $\beta' \in \alpha + \mathfrak{a}$ with $N(\beta') < 3$. □

Now we will prove the 'only if' part. First we derive some arithmetical restrictions on the discriminant in the case that $\mathcal{O}$ has a non-principal Euclidean ideal class.

LEMMA (5.22). *Suppose that the ring of integers $\mathcal{O}$ of the real quadratic field $\mathbb{Q}(\sqrt{\Delta})$ has a non-principal Euclidean ideal class. Then*

(a) *$\mathcal{O}$ has a non-principal integral ideal of norm 3;*

(b) *If $6|\Delta$ then $\mathcal{O}$ has a non-principal integral ideal of norm 5;*

(c) *$\mathcal{O}$ has a non-principal integral ideal of norm 2, 5 or 7.*

PROOF. For (a) we use (2.1) with $\mathfrak{a} = 2\mathcal{O}$. This shows the existence of a non-principal integral ideal $\mathfrak{b}$ of odd norm < 4, thus $N\mathfrak{b} = 3$. For (b) observe that the integral ideal $\mathfrak{a}$ of norm 6 must be principal, since the ideals of norms 2 and 3 are not principal by (2.3) and part (a). Again using (2.1) we obtain a non-principal integral ideal of norm 5. For part (c) we use (2.1) with $\mathfrak{a} = 3\mathcal{O}$. □

Consulting a list of ideals of real quadratic fields, e.g. [I], we find that only 29 rings satisfy

(5.20), $\Delta \notin \{40,60,85\}$, $h(\mathcal{O}) = 2$, (5.22)(a), (b), (c) and the integral ideal of least norm is non-principal.

For all but one of them we can use the next lemma to disprove the existence of a Euclidean ideal class.

We will use the norm function $\mathcal{N}$ as defined in (1.7). For an element $x + y\sqrt{\Delta}$ of K we have $\mathcal{N}(x + y\sqrt{\Delta}) = x^2 - \Delta y^2$ and $|\mathcal{N}(x + y\sqrt{\Delta})| = N(x + y\sqrt{\Delta})$.

LEMMA (5.23). *Let* $\mathfrak{a}$ *be an integral* $\mathcal{O}$*-ideal which is a product of distinct prime ideals of* $\mathcal{O}$ *dividing* Δ. *Let* $\mathfrak{b}$ *be an integral* $\mathcal{O}$*-ideal such that* $\mathfrak{ab}$ *is non-principal, and such that* $\gcd(N\mathfrak{a}, N\mathfrak{b}) = 1$. *Write* $a = N\mathfrak{a}$ *and* $b = N\mathfrak{b}$. *Suppose that there exist* $n \in \mathbb{Z}$ *such that* $0 < n < a$, *such that* $x^2 \equiv nb \bmod a$ *has a solution in* $\mathbb{Z}$ *and such that* nb *and* $(n-a)b$ *are not in the image of* $\mathcal{N}\colon \mathcal{O} \to \mathbb{Z}$. *Then* $\mathcal{O}$ *does not have a Euclidean ideal class.*

PROOF. Suppose on the contrary that $\mathcal{O}$ has a Euclidean ideal class. Then $\mathfrak{ab}$ must be Euclidean. Choose $x \in \mathbb{Z}$ such that $x^2 \equiv nb \bmod a$. Since $\gcd(a,b) = 1$ we may even suppose that $x \in b\mathbb{Z}$. Because $\mathfrak{ab}$ is Euclidean there exists $\alpha \in x + \mathfrak{ab}$ such that $N\alpha = |\mathcal{N}\alpha| < ab$. The conjugate of $\mathfrak{a}$ is equal to $\mathfrak{a}$, hence $\mathcal{N}\alpha \in x^2 + (\mathfrak{a} \cap \mathbb{Z}) = nb + a\mathbb{Z}$. Also $\alpha \in \mathfrak{b}$, which implies $b \mid \mathcal{N}\alpha$, so $\mathcal{N}\alpha \in nb + ab\mathbb{Z}$. But only $\mathcal{N}\alpha = nb$ and $\mathcal{N}\alpha = (n-a)b$ satisfy $|\mathcal{N}\alpha| < ab$ and $\mathcal{N}\alpha \equiv nb \bmod ab$, which gives a contradiction. □

In table 3 we give a list of the fields for which it is possible to use (5.23) to disprove the existence of a Euclidean ideal class. The proof that nb and $(n-a)b$ are not norms can be given in all cases by showing that they are not norms mod p^3, where p is the least prime number dividing Δ.

It remains to prove that the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\sqrt{265})$ does not have a Euclidean ideal class. A fundamental unit of $\mathcal{O}$ is equal to $\eta = 6072 + 373\sqrt{265}$, cf. [I]. The ideal $\mathfrak{a} = \mathbb{Z}\cdot 22 + \mathbb{Z}\frac{1}{2}(1 + \sqrt{265})$ is non-principal of norm 22. It suffices to show that $\mathfrak{a}$ is not Euclidean. For this we show that there is no $\alpha \in \mathcal{O}$, such that $\alpha \equiv 10 \bmod \mathfrak{a}$ and $N(\alpha) < 22$. Let $\alpha\mathcal{O}$ be a principal ideal of norm less than 22. For any generator β of $\alpha\mathcal{O}$ we have $\beta \equiv \pm\alpha \bmod \mathfrak{a}$, since $\eta \equiv 1 \bmod \mathfrak{a}$. An easy check shows that no principal ideal of norm less than 22 has a generator $\equiv \pm 10 \bmod \mathfrak{a}$, cf. Table 4.

This finishes the proof of case $(\#2^+)$ of (1.10).

TABLE 3. Real quadratic fields with no non-principal Euclidean ideal

Δ	a	b	n	Δ	a	b	n
105 = 3•5•7	5	2	3	609 = 3•7•29	7	3	6
165 = 3•5•11	11	7	2	616 = 8•7•11	22	3	15
205 = 5•41	41	3	11	636 = 4•3•53	53	1	11
220 = 4•5•11	5	3	2	645 = 3•5•43	43	5	37
232 = 8•29	58	3	17	685 = 5•137	137	1	7
280 = 8•5•7	14	3	5	705 = 3•5•47	47	1	14
285 = 3•5•19	19	5	1	744 = 8•3•31	62	1	19
345 = 3•5•23	23	1	8	745 = 5•149	149	2	44
357 = 3•7•17	17	3	5	760 = 8•5•19	38	1	5
385 = 5•7•11	7	6	5	805 = 5•7•23	23	1	8
424 = 8•53	106	3	41	808 = 8•101	202	3	41
460 = 4•5•23	23	1	2	861 = 3•7•41	41	7	11
465 = 3•5•31	31	3	6	865 = 5•173	173	1	43
565 = 5•113	113	1	30	885 = 3•5•59	59	5	9

TABLE 4. Principal ideals of norm < 22 in $\mathbb{Z}[\omega]$. with $\omega = \frac{1}{2}(1+\sqrt{265})$

N	generator	generators mod $\mathfrak{a}$	N	generator	generators mod $\mathfrak{a}$
1	1	±1	10	$7+\omega$	±7
4	2	±2	10	$8-\omega$	±8
4	$23+3\omega$	±1	11	$107+14\omega$	±3
4	$26-3\omega$	±4	11	$121-14\omega$	11
6	$8+\omega$	±8	15	$61+8\omega$	±5
6	$9-\omega$	±9	15	$69-8\omega$	±3
6	$84+11\omega$	±4	16	4	±4
6	$95-11\omega$	±7	16	$46+6\omega$	±2
9	3	±3	16	$52-6\omega$	±8
9	$15+2\omega$	±7	16	$1123+147\omega$	±1
9	$17-2\omega$	±5	16	$1270-147\omega$	±6

CHAPTER 6 IMPROVEMENT OF THE DISCRIMINANT BOUND IN THE IMAGINARY QUADRATIC CASE

Throughout the next four chapters we consider the imaginary quadratic case ($\#2^-$). We fix an imaginary quadratic field K and a set $S = \{\infty, p\}$ of primes of K. Here the archimedean prime of K is denoted by ∞ and p is a non-archimedean prime. Since $K_\infty = \mathbb{C}$ the ring K_S, as defined by (3.13), is equal to $K_p \times \mathbb{C}$.

We have to deal with two different norm functions. The first one is the norm function N with respect to the ring of integers $\mathcal{O}$, which is defined for $\mathcal{O}$-ideals and for elements of K. For an element α of K the norm $N(\alpha)$ is equal to its archimedean valuation $|\alpha|_\infty$. Usually we will write $|\alpha|_\infty$ instead of $N(\alpha)$. The other norm function is the norm N with respect to $A = A_S$. It is defined for A-ideals and elements of K. For an element α of K we have $N(\alpha) = |\alpha|_p |\alpha|_\infty$, cf. (0.14), (0.15) and (1.5).

To each $\mathcal{O}$-ideal b there corresponds an unique A-ideal $a = bA$. All A-ideals are of this form. Two $\mathcal{O}$-ideals b and c correspond to the same A-ideal if and only if $b = cp^n$ for some $n \in \mathbb{Z}$, cf. section (2.2).

§(6.1) A translation of the theorem of Barnes and Swinnerton-Dyer

Let b be an $\mathcal{O}$-ideal, and let $a = bA$ be the corresponding A-ideal. Define

$$(6.1) \qquad t(a) = \inf\{t \in \mathbb{R}_{>0} : K_S = a + V_t\},$$

cf. (5.1). From the theorem of Barnes and Swinnerton-Dyer ((5.2) and (5.5)) we know that in most cases, i.e. if $t(a) \neq Na$, the value of $t(a)$ determines whether a is Euclidean. In this section we show how we may use knowledge of the sequence of $\mathcal{O}$-ideals bp^n, for $n \in \mathbb{Z}$, to determine $t(a)$. In the next two sections we determine lower bounds on

$t(\mathfrak{a})$ in this way. If $\mathfrak{a}$ is Euclidean this will lead to an upper bound on the discriminant.

For each $n \in \mathbb{Z}$ the $\mathcal{O}$-ideal $\mathfrak{b}\mathfrak{p}^n$ is a lattice in $\mathbb{C}$, cf. (3.20). We have a natural surjection of compact groups $\mathbb{C}/\mathfrak{b}\mathfrak{p}^n \twoheadrightarrow \mathbb{C}/\mathfrak{b}\mathfrak{p}^{n-1}$.

<u>LEMMA (6.2)</u>. *Let* $\mathfrak{b}$ *be an* $\mathcal{O}$-*ideal and let* $\mathfrak{a} = \mathfrak{b}A$ *be the corresponding* A-*ideal. There is a natural isomorphism*

$$K_S/\mathfrak{a} \xrightarrow{\sim} \varprojlim_{n\in\mathbb{Z}} \mathbb{C}/\mathfrak{b}\mathfrak{p}^n.$$

<u>PROOF</u>. Let π_1 be the projection $K_S = K_\mathfrak{p} \times \mathbb{C} \to K_\mathfrak{p}$ and let π_2 be the projection $K_S \to \mathbb{C}$. When restricted to K these projections are injective and equal to the natural embeddings of K into $K_\mathfrak{p}$ and $\mathbb{C}$ respectively. The inverse of π_i, when restricted to $\pi_i(K)$ will be denoted by ι_i for $i = 1,2$.

The $\mathcal{O}$-ideals will be regarded as lattices in $\mathbb{C}$ and the A-ideals will be regarded as lattices in K_S, cf. section (3.6).

We may assume that $\mathrm{ord}_\mathfrak{p}(\mathfrak{b}) = 0$. The union of all $\iota_2(\mathfrak{b}\mathfrak{p}^n)$ is equal to $\mathfrak{a}$ and $\iota_1(\pi_1(\mathfrak{a}) \cap \tilde{\mathfrak{p}}^n) = \iota_2(\mathfrak{b}\mathfrak{p}^n)$. By the strong approximation theorem ([CF] ch.II §15) $\pi_1(\mathfrak{a})$ is a dense subset of $K_\mathfrak{p}$. Hence we have a natural isomorphism

$$K_\mathfrak{p}/\tilde{\mathfrak{p}}^n \simeq (\pi_1(\mathfrak{a}) + \tilde{\mathfrak{p}}^n)/\tilde{\mathfrak{p}}^n \simeq \mathfrak{a}/\iota_2(\mathfrak{b}\mathfrak{p}^n).$$

The embedding $\pi_2\colon \mathfrak{a} \to \mathbb{C}$ gives rise to an injection $\mathfrak{a}/\iota_2(\mathfrak{b}\mathfrak{p}^n) \to \mathbb{C}/\mathfrak{b}\mathfrak{p}^n$ and thus we have an injection

$$f : K_\mathfrak{p} \simeq \varprojlim_{n\in\mathbb{Z}} K_\mathfrak{p}/\tilde{\mathfrak{p}}^n \longrightarrow \varprojlim_{n\in\mathbb{Z}} \mathbb{C}/\mathfrak{b}\mathfrak{p}^n.$$

Let g be the natural map

$$g : \mathbb{C} \longrightarrow \varprojlim_{n\in\mathbb{Z}} \mathbb{C}/\mathfrak{b}\mathfrak{p}^n.$$

We combine these maps to get a map

$$h : K_S \longrightarrow \varprojlim_{n\in\mathbb{Z}} \mathbb{C}/\mathfrak{b}\mathfrak{p}^n,$$

where $h(x) = f(\pi_1(x)) - g(\pi_2(x))$. Because the images of f and g are dense in $\varprojlim_{n\in\mathbb{Z}} \mathbb{C}/bp^n$ we find that the image of h is dense in $\varprojlim_{n\in\mathbb{Z}} \mathbb{C}/bp^n$ as well. We show that the kernel of h is equal to a. First notice that for $\alpha \in a$ we have $f(\pi_1(\alpha)) = g(\pi_2(\alpha)) = (\pi_2(\alpha) \bmod bp^n)_{n\in\mathbb{Z}}$. This shows that a is contained in the kernel of h. Now suppose that $x \in K_S$ is such that $h(x) = 0$, i.e. $f(\pi_1(x)) = g(\pi_2(x))$. By the definition of f there exists a sequence $(x_n)_{n\in\mathbb{Z}}$ in a such that $\pi_1(x_n) \equiv \pi_1(x) \bmod \tilde{p}^n$ and $f(\pi_1(x)) = (\pi_2(x_n) \bmod bp^n)_{n\in\mathbb{Z}}$. By assumption this is equal to $(\pi_2(x) \bmod bp^n)_{n\in\mathbb{Z}}$, hence $\pi_2(x) \in \pi_2(a)$. Choose $x' \in a$ with $\pi_2(x') = \pi_2(x)$, then $f(\pi_1(x-x')) = h(x-x') = 0$. By injectivity of f this shows that $\pi_1(x) = \pi_1(x')$ and $x = x' \in a$. Because K_S/a is compact and the image of h is dense we find that h is surjective and thus $K_S/a \simeq \varprojlim_{n\in\mathbb{Z}} \mathbb{C}/bp^n$. □

For each $t \in \mathbb{R}_{>0}$ and each $\mathcal{O}$-ideal c we define a subset of $\mathbb{C}$:

(6.3) $$W_t(c) = \{x \in \mathbb{C} : \exists\, \beta \in c \text{ such that } |x-\beta|_\infty < tNc\},$$

i.e. $W_t(c)$ is the union of open discs in $\mathbb{C}$ with radii $\sqrt{tNc}$ and centres at c.

In most proofs we use (5.5) to decide whether a given A-ideal is Euclidean. The next proposition will be used to simplify this decision for the present case (#2⁻). For the definition of V_t see (5.1).

PROPOSITION (6.4). *Let* b *be an* $\mathcal{O}$*-ideal and let* $a = bA$ *be the corresponding* A*-ideal. For* $t \in \mathbb{R}_{>0}$ *we have* $K_S = a + V_{tNa}$ *if and only if there exists* $m \in \mathbb{Z}_{>0}$ such that $\mathbb{C} = \bigcup_{n=0}^{m} W_t(bp^n)$.

PROOF. Since both conditions only depend on the $\mathcal{O}$-ideal class of b we may assume that $\mathrm{ord}_p(b) = 0$. For $n \in \mathbb{Z}$ we define the open set

$$U_n = \tilde{p}^n \times W_t(bp^n) \subset K_p \times \mathbb{C} = K_S$$

then $a + \bigcup_{n\in\mathbb{Z}} U_n = a + V_{tNa}$.

First we prove the 'only if' part. Suppose that $K_S = a + V_{tNa} = a + \bigcup_{n\in\mathbb{Z}} U_n$. Then $K_S/a = \bigcup_{n\in\mathbb{Z}} (U_n \bmod a)$. Because K_S/a is compact there exist $\ell, m \in \mathbb{Z}$ such that $K_S/a = \bigcup_{n=\ell}^{m} (U_n \bmod a)$. After multiplying by a suitable unit of A we may suppose that $\ell \geq 0$ and $m \geq 0$. Then $K_S = a + \bigcup_{n=0}^{m} U_n$. In particular for each $x \in \mathbb{C}$ we have $(0,x) \in a + \bigcup_{n=0}^{m} U_n$.

Hence there exist $\alpha \in \mathfrak{a}$ and $n \in \mathbb{Z}$ with $0 \le n \le m$ such that $(\alpha, x+\alpha) \in U_n$, i.e. $\alpha \in bp^n$ and $x+\alpha \in W_t(bp^n)$. Thus $x \in W_t(bp^n)$, which proves the 'only if' part.

Now we prove the 'if' part. Suppose that $\mathbb{C} = \bigcup_{n=0}^{m} W_t(bp^n)$. Let (x,y) be an element of $K_p \times \mathbb{C} = K_S$. There exists a unit τ of A such that $|\tau x|_p \le Np^{-m}$. By assumption there exist $n \in \mathbb{Z}$, with $0 \le n \le m$, and $\alpha \in bp^n$ such that $|\tau y - \alpha|_\infty < tN(bp^n)$. Because both $|\tau x|_p \le Np^{-n}$ and $|\alpha|_p \le Np^{-n}$ we have $|\tau x - \alpha|_p \le Np^{-n}$. Hence

$$|(x,y) - \tau^{-1}\alpha|_p |(x,y) - \tau^{-1}\alpha|_\infty = |\tau x - \alpha|_p |\tau y - \alpha|_\infty <$$

$$< Np^{-n} tN(bp^n) = tN(b) = tN\mathfrak{a}, \text{ i.e. } (x,y) \in \mathfrak{a} + V_{tN\mathfrak{a}}. \quad \square$$

COROLLARY (6.5). $t(\mathfrak{a}) = \inf\{t \in \mathbb{R}_{>0} : \exists m \in \mathbb{Z}_{\ge 0}$ such that $\mathbb{C} = \bigcup_{n=0}^{m} W_t(bp^n)\}$. $\square$

COROLLARY (6.6).

(a) *Suppose that there exists* $\varepsilon \in \mathbb{R}_{>0}$ *such that for all* $m \in \mathbb{Z}_{\ge 0}$ *we have* $\mathbb{C} \ne \bigcup_{n=0}^{m} W_{1+\varepsilon}(bp^n)$. *Then* $\mathfrak{a}$ *is* not *Euclidean.*

(b) *Suppose that there exists* $m \in \mathbb{Z}_{\ge 0}$ *such that* $\mathbb{C} = \bigcup_{n=0}^{m} W_1(bp^n)$. *Then* $\mathfrak{a}$ *is Euclidean.*

PROOF. This is only a reformulation of (5.5). $\square$

In certain circumstances we may improve upon (6.6)(a). In these cases we may take $\varepsilon = 0$ and we only have to decide whether the condition is valid for a given value of m:

PROPOSITION (6.7). *Let* η *be a unit of* A, *such that* $|\eta|_p < 1$. *Let* $h \in \mathbb{Z}_{>0}$ *be such that* $\eta 0 = p^h$. *Suppose that there exists* $x \in \mathbb{C}$ *such that*

$$\eta x \equiv x \bmod bp^{h-1}$$

and such that

$$x \notin \bigcup_{n=0}^{h-1} W_1(bp^n).$$

Then $\mathfrak{a} = bA$ *is not Euclidean.*

PROOF. Clearly the condition only depends on the ideal class of b, so we may assume that $\mathrm{ord}_p(b) = 0$.

There exists $\alpha \in bp^{h-1}$ such that $x = \alpha(\eta-1)^{-1}$, hence $x \in K$. We will show that $N(x-\beta) \geq N\mathfrak{a}$ for all $\beta \in \mathfrak{a}$, hence $\mathfrak{a}$ is not Euclidean. Since $bp^{h-1} \subset \mathfrak{a}$ and since η is a unit of A we have

$$\eta^m\alpha \equiv \alpha \bmod \mathfrak{a} \quad \text{for all } m \in \mathbb{Z}.$$

From $|\eta-1|_p = 1$ we see that $|x|_p \leq Np^{-h+1}$. Because $x \notin bp^{h-1}$ this shows that $x \notin \mathfrak{a}$. Let β be an element of $\mathfrak{a}$. There exists $m,n \in \mathbb{Z}$ with $0 \leq n < h$ such that

$$|\eta^m(\beta-x)|_p = Np^{-n}.$$

Then $\gamma = \eta^m\beta + (1-\eta^m)x$ is an element of $\mathfrak{a}$ and

$$|\gamma|_p = |x + \eta^m(\beta-x)|_p \leq Np^{-n},$$

hence $\gamma \in bp^n$. Because $x \notin W_1(bp^n)$ we have

$$|\eta^m(\beta-x)|_\infty = |\gamma-x|_\infty \geq N(bp^n).$$

Combining these inequalities we find

$$N(\beta-x) = N(\eta^m(\beta-x)) = |\eta^m(\beta-x)|_p|\eta^m(\beta-x)|_\infty \geq$$

$$\geq Np^{-n}N(bp^n) = Nb = N\mathfrak{a}. \quad \square$$

Our main tools in the determination whether a given A-ideal is Euclidean are (6.6) and (6.7). The advantage over (5.5) is that we may work in $\mathbb{C}$ instead of in K_S.

§(6.2) An improvement of the theorem of Cassels

In the case $(\#2^-)$ the theorem of Cassels (5.16) may be sharpened with the help of the results of the previous section. Essentially we will use the same proof as in (5.10) and (5.16).

PROPOSITION (6.8). *Let* b *be an* $\mathcal{O}$*-ideal. Let* $\hat{a}$ *be the maximum of the integers* a *occurring as the first coefficient of a reduced quadratic form corresponding to an ideal of the form* bp^n, *for* $n \in \mathbb{Z}$, *cf. section (3.1). Let* p *be the rational prime with* $p|p$. *Take* $k = Np^m$ *fixed for some* $m \in \mathbb{Z}_{>0}$. *Let* k' *be the smallest* p*-power with* $k' \in p^m$. *If* $a = bA$ *is Euclidean then*

$$\hat{a} \geq |\Delta| \frac{Np}{k} \left(\frac{k'-1}{4k'}\right)^2.$$

REMARK (6.9). Because $3\hat{a}^2 < |\Delta|$ (see the proof of (6.14)) we find that $\sqrt{|\Delta|} < \frac{16}{\sqrt{3}} \frac{k}{Np} \left(\frac{4k'}{k'-1}\right)^2$ if a is Euclidean, a conclusion we may also derive from (5.16) ($\#2^-$). However, since $\hat{a}$ is integral, we may improve the bound in many cases.

PROOF OF (6.8). For each $n \in \mathbb{Z}$ the ideal bp^n corresponds to a reduced quadratic form (a_n, b_n, c_n) with $a_n \leq \hat{a}$. Let $\{\alpha_n, \beta_n\}$ be a basis of bp^n, such that

$$|\alpha_n|_\infty = a_n Nbp^n, \quad |\beta_n|_\infty = c_n Nbp^n \quad \text{and} \quad \beta_n = \frac{b_n + \sqrt{\Delta}}{2a_n} \alpha_n,$$

cf. section (3.1). We define a map $\varphi_n : \mathbb{C} \longrightarrow \mathbb{R}$ by

(6.10) $\qquad \varphi_n(x\alpha_n + y\beta_n) = y \quad$ for $x, y \in \mathbb{R}$,

so $\varphi_n(z) = \mathrm{Im}(\frac{z}{\alpha_n}) / \mathrm{Im}(\frac{\beta_n}{\alpha_n})$. Thus $\varphi(bp^n) = \mathbb{Z}$ and for every $r \in \mathbb{Z}$ we have

(6.11) $\qquad p\varphi_n(bp^r) \subset \varphi_n(bp^{r+1}) \subset \varphi_n(bp^r)$.

Choose $\varepsilon \in \mathbb{R}_{>0}$ with $\hat{a}(1+\varepsilon) < |\Delta| \frac{Np}{k} \left(\frac{k'-1}{4k'}\right)^2$. With induction on $n \in \mathbb{Z}_{\geq 0}$ we prove the existence of $y_n \in \mathbb{C}$ such that

(6.12)(a) $\qquad |y_n - \gamma|_\infty > (1+\varepsilon) Nbp^r \quad$ for all $r \in \mathbb{Z}$ with $0 \leq r \leq n$ and all $\gamma \in bp^r$

(b) $\qquad |y_n - \gamma|_\infty > (1+\varepsilon) \frac{k}{Np} Nbp^n \quad$ for all $\gamma \in bp^n$.

Since $y_n \notin \bigcup_{r=0}^{n} W_{1+\varepsilon}(bp^r)$ the proposition follows from (6.6)(a).

We distinguish 2 cases.

Case 1. (Including the initial step). Suppose that for all r with $0 \le r \le n$ we have $\varphi_n(bp^r) = \mathbb{Z}$, then we choose $y_n = \frac{1}{2}\beta_n$. For all r with $0 \le r \le n$ and for all $\gamma \in bp^r$ we have $\varphi_n(y_n-\gamma) \ge \frac{1}{2}$. Hence

$$|y_n-\gamma|_\infty \ge \left(\mathrm{Im}\left(\frac{y_n-\gamma}{\alpha_n}\right)\right)^2 \cdot |\alpha_n|_\infty = (\varphi_n(y_n-\gamma))^2 \cdot \left|\mathrm{Im}\,\frac{\beta_n}{\alpha_n}\right|^2 |\alpha_n|_\infty \ge$$

$$\ge \frac{1}{4}\left|\mathrm{Im}\,\frac{\beta_n}{\alpha_n}\right|^2 |\alpha_n|_\infty = \frac{1}{4}\cdot\frac{|\Delta|}{4a_n^2}\cdot a_n Nbp^n \ge \frac{|\Delta|}{16\hat{a}} Nbp^n >$$

$$> (1+\varepsilon)\frac{k}{Np}\left(\frac{k'}{k'-1}\right)^2 Nbp^n \ge (1+\varepsilon)\frac{k}{Np} Nbp^n.$$

Because $k \ge Np$ and $r \le n$ we obtain (6.12).

Case 2. Suppose that there exists $t \in \mathbb{Z}$ with $0 \le t < n$, such that $\varphi_n(bp^t) \ne \mathbb{Z}$. Choose t as large as possible, then $\varphi_n(bp^t) = \frac{1}{p}\mathbb{Z}$ and $\varphi_n(bp^{t+1}) = \mathbb{Z}$.

For $i \in \mathbb{Z}_{\ge 0}$ we have

$$\varphi_n(bp^{t+1-m}) \subset p^{-i}\mathbb{Z} \iff$$

$$\varphi_n(p^i bp^{t+1-m}) \subset \mathbb{Z} \iff$$

$$\varphi_n(bp^{t+1}(p^i p^{-m} + O)) \subset \mathbb{Z} \iff$$

$$p^i p^{-m} \subset O \iff$$

$$p^i \in p^m.$$

By the definition of k' we derive that $\varphi_n(bp^{t+1-m}) = \frac{1}{k'}\mathbb{Z}$.

If $t+1-m \ge 0$ then by the induction hypothesis there exists an element $y = y_{t+1-m} \in \mathbb{C}$, such that (6.12) is satisfied, with n replaced by $t+1-m$, which is $< n$. If $t+1-m < 0$ then by the induction hypothesis there exists an element $y = y_{t+1-m} \in \mathbb{C}$, such that (6.12) is satisfied, with n replaced by 0 and b replaced by bp^{t+1-m}. These properties will not be changed if we shift y by an element of bp^{t+1-m}. Since $\varphi_n(bp^{t+1-m}) = \frac{1}{k'}\mathbb{Z}$ we may therefore assume that $|\varphi_n(y) - \frac{1}{2}| \le \frac{1}{2k'}$, cf. fig. 9. We show that y satisfies (6.12).

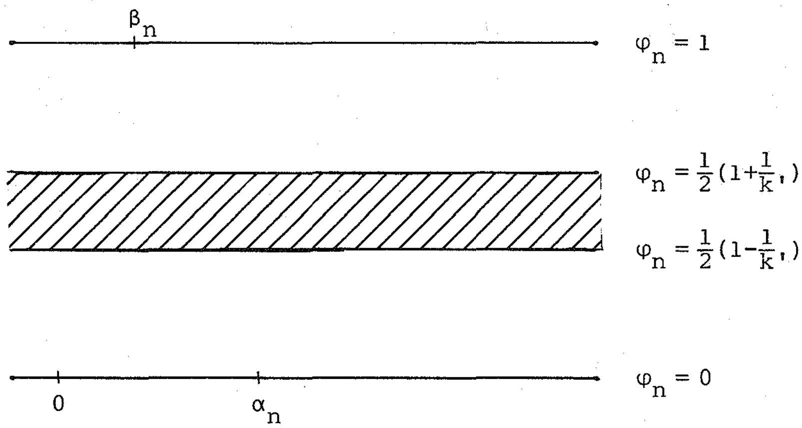


fig. 9

First, if $0 \le r < t+1-m$ and $\gamma \in bp^r$ we have $|y-\gamma|_\infty > (1+\varepsilon)Nbp^r$ by induction. If $t+1-m < r \le t$ and $\gamma \in bp^r$ then surely $\gamma \in bp^{t+1-m}$, and by induction we have

$$|y-\gamma|_\infty \;>\; (1+\varepsilon)\,\frac{k}{Np}\,Nbp^{t+1-m} \;=\; (1+\varepsilon)Nbp^t \;\ge\; (1+\varepsilon)Nbp^r.$$

Finally if $t < r \le n$ and $\gamma \in bp^r$, then $\varphi_n(\gamma) \in \mathbb{Z}$, hence $\varphi_n(y-\gamma) \ge$ $\ge \frac{k'-1}{2k'}$. This shows that

$$\begin{aligned} |y-\gamma|_\infty \;&\ge\; \left(\frac{k'-1}{2k'}\right)^2 \left|\operatorname{Im}\frac{\beta_n}{\alpha_n}\right|^2 |\alpha_n|_\infty \;= \\ &=\; \left(\frac{k'-1}{2k'}\right)^2 \cdot \frac{|\Delta|}{4a_n^2}\cdot a_n Nbp^n \;\ge \\ &\ge\; \left(\frac{k'-1}{2k'}\right)^2 \cdot \frac{|\Delta|}{4\hat{a}}\cdot Nbp^n \;> \\ &>\; (1+\varepsilon)\,\frac{k}{Np}\,Nbp^n \;\ge\; (1+\varepsilon)\,\frac{k}{Np}\,Nbp^r. \end{aligned}$$

Since $k \ge Np$ this proves (6.12). □

REMARK (6.13). In section (8.3) we show that in certain cases we do not need that $a < |\Delta|\frac{Np}{k}(\frac{k'-1}{4k'})^2$ for all reduced quadratic forms corresponding to ideals of the form bp^n. If there are few exceptions we may change the induction step.

THEOREM (6.14). *Let* p *be the rational prime in* p. *Suppose that* A *has a Euclidean ideal* a. *Let* b *be an* 0 *- ideal such that* a = bA *and let* $\hat{a}$ *be the maximum of the integers* a *occurring as the first coefficient of a reduced quadratic form corresponding to an ideal of the form* bp^n. *Then*

$$|\Delta| \leq 16(\frac{p}{p-1})^2\hat{a} ;$$

$$\hat{a} < \frac{16}{3}(\frac{p}{p-1})^2 ;$$

$$|\Delta| \leq 1344.$$

If moreover p *is equal to* 2 *and* $\Delta \equiv 1 \bmod 8$, *then*

$$|\Delta| \leq \frac{512}{9}\hat{a} ;$$

$$\hat{a} \leq 18 ;$$

$$|\Delta| \leq 1007.$$

PROOF. We take $m = 1$ in (6.8), then $k = Np$ and $k' = p$. Then we must have $\hat{a} \geq \frac{|\Delta|}{16}(\frac{p-1}{p})^2$. If $\Delta = -3$ the inequalities are certainly satisfied. If $\Delta \neq -3$ we have for each quadratic form (a,b,c) that $|\Delta| = 4ac - b^2 >$ $> 3a^2$, so certainly $|\Delta| > 3\hat{a}^2$. This gives

$$\hat{a} < \frac{16}{3}(\frac{p}{p-1})^2 .$$

Because $\frac{p}{p-1} \leq 2$ we have $\hat{a} < \frac{64}{3} = 21.333$ and $|\Delta| \leq 16\cdot\hat{a}\cdot(\frac{p}{p-1})^2 \leq$ $16\cdot 21\cdot 4 = 1344$.

If $p = 2$ and $\Delta \equiv 1 \bmod 8$ then p splits completely in $K/\mathbb{Q}$. We take $m = 2$ in (6.8), then $k = k' = 4$. Hence $\hat{a} \geq |\Delta|\cdot\frac{1}{2}\cdot(\frac{3}{16})^2$, i.e. $|\Delta| \leq \frac{512}{9}\hat{a}$. Again we use $|\Delta| > 3\hat{a}^2$ to get $\hat{a} < \frac{512}{27} = 18.963$, i.e. $\hat{a} \leq 18$ and $|\Delta| \leq \frac{512}{9}\cdot 18 = 1024$. For $\Delta = -1023$ and $\Delta = -1015$ there is no reduced quadratic form (a,b,c) with $a = 18$. For $\hat{a} \leq 17$ we get $|\Delta| \leq \frac{512}{9}\cdot 17 = 967.111$. This shows that $|\Delta| \leq 1007$. □

COROLLARY (6.15). *Let* $\tilde{a}$ *be the maximum of the integers* a *occurring as the first coefficient of a reduced quadratic form of discriminant* Δ. *Let* p *be the rational prime in* p. *If* A *has a Euclidean ideal class, then*

$$p \le (1 - 4\sqrt{\frac{\tilde{a}}{|\Delta|}})^{-1},$$

provided that the right-hand side is positive.

PROOF. We have $\hat{a} \le \tilde{a}$ hence also

$$|\Delta| \le 16(\frac{p}{p-1})^2\tilde{a},$$

i.e.

$$p \le (1 - 4\sqrt{\frac{\tilde{a}}{|\Delta|}})^{-1},$$

when the right-hand side is positive. □

In table 5 we list for certain given values of p the discriminant bounds that can be derived from (6.14). Notice that for $|\Delta| > 80$ only finitely many rings have a Euclidean ideal class.

TABLE 5.

p	$\tilde{a} \le$	$\lvert\Delta\rvert \le$
2	21	1344
3	11	396
5	8	200
7	7	152
11	6	116
$p \to \infty$	5	80

§(6.3) Bounds depending on the covering radii

In order to show that a given A-ideal a is not Euclidean it suffices, by (6.6), to find an $\varepsilon \in \mathbb{R}_{>0}$ and a sequence $(y_n)_{n\in\mathbb{Z}_{\ge 0}}$ in $\mathbb{C}$ such that $y_n \notin \bigcup_{r=0}^{n} W_{1+\varepsilon}(bp^r)$. Here b is an $\mathcal{O}$-ideal such that $bA = a$. In this section we show that such an ε and such a sequence exists if the covering radii of the ideals bp^r satisfy certain constraints, cf. (6.17). This will lead to upper bounds on $N\mathfrak{p}$ for rings with a Euclidean ideal class, in case $(\#2^-)$, whenever $\Delta \notin \{-3,-4,-7,-8,-11,-15,-20\}$. This shows that in the case $(\#2^-)$, apart from the known rings with a Euclidean ideal class, there are only finitely many others.

LEMMA (6.16). *Let* $\mathfrak{b}$ *be an* $\mathcal{O}$*-ideal, and let* ρ *be its covering radius, cf. (3.3). Then for each* $z \in \mathbb{C}$ *and each* $u \in \mathbb{R}$ *with* $0 \le u \le \rho$ *there exists* $v \in \mathbb{C}$ *such that*

(a) $|v - \alpha|_\infty \ge uN\mathfrak{b}$ for all $\alpha \in \mathfrak{b}$;

(b) $|v - z|_\infty \le uN\mathfrak{b}$.

PROOF. If $u = \rho$ we may take for v one of the points for which equality

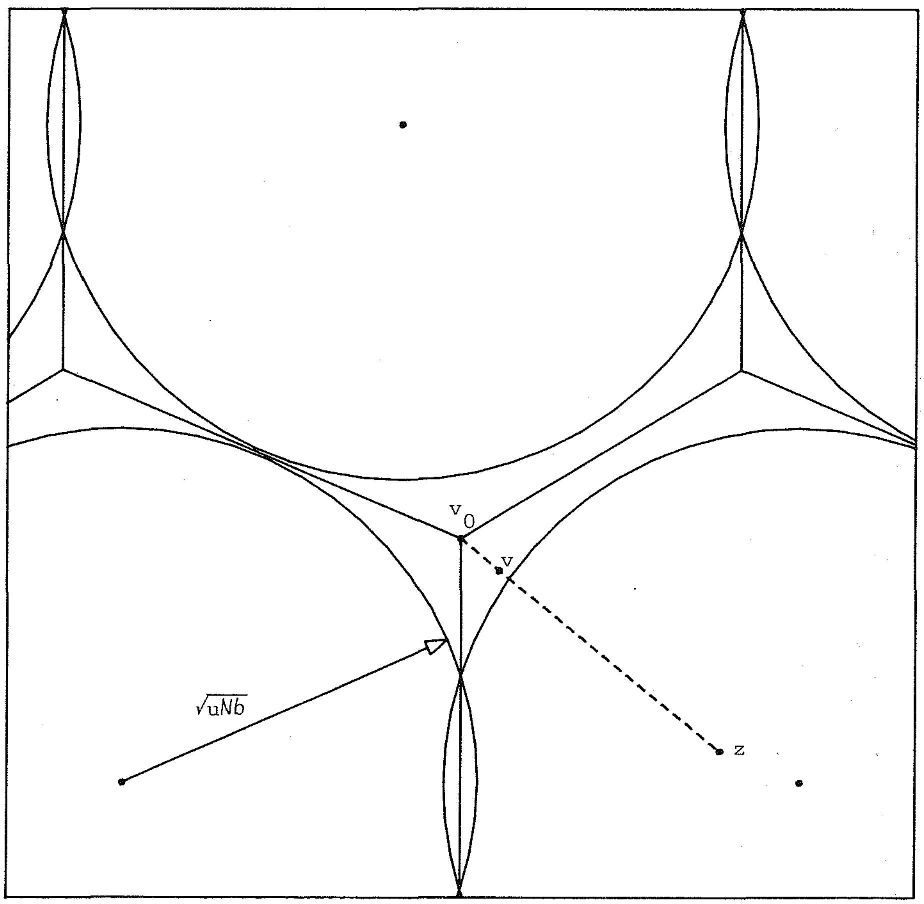


fig. 10

is obtained in (3.4). Then (a) is satisfied. By (3.4) we may shift v by an element of b such that also (b) is satisfied. Denote this point by v_0. If $u < \rho$ we take $v = \sqrt{\frac{u}{\rho}}(v_0 - z) + z$, cf. fig.10, then (a) and (b) are satisfied. □

Let b be an $\mathcal{O}$-ideal. We will denote by ρ_n the covering radius of bp^n, cf. (3.3). Since ρ_n is completely determined by the corresponding reduced quadratic form it only depends on the ideal class of bp^n. This shows that the sequence $(\rho_n)_{n\in\mathbb{Z}}$ is periodic mod h, where h is the order of $[p]$ in $\mathrm{Cl}(\mathcal{O})$.

PROPOSITION (6.17). *Suppose there exists* $\varepsilon \in \mathbb{R}_{>0}$ *and* $x_n \in \mathbb{R}_{>0}$ *for* $n \in \mathbb{Z}$, *such that for all* $n \in \mathbb{Z}$

(a) $$x_n \geq \min\{\sqrt{\rho_n},\ 1 + \varepsilon + \frac{2}{\sqrt{Np}} x_{n-1}\}$$

(b) $$\sqrt{\rho_n} \geq 1 + \varepsilon + \frac{1}{\sqrt{Np}} x_{n-1}.$$

Then $a = bA$ *is not Euclidean.*

PROOF. We will show that for $n \in \mathbb{Z}_{\geq 0}$ there exists $y_n \in \mathbb{C}$, such that for $0 \leq r \leq n$:

(6.18) $$|y_n - \alpha|_\infty \geq (1+\varepsilon)^2 Nbp^r \quad \text{for all} \quad \alpha \in bp^r.$$

By (6.6) this suffices to show that a is not Euclidean. For given $z \in \mathbb{C}$ we prove by induction on $n \in \mathbb{Z}_{\geq 0}$ that there exists such an element $y_n \in \mathbb{C}$ which satisfies in addition

(6.19) $$|y_n - z|_\infty \leq x_n^2 Nbp^n.$$

First let $n = 0$, and put $u = (1 + \varepsilon + x_{-1}/\sqrt{Np})^2$. Then $u \leq \rho_0$ by (b), so $u \leq x_0^2$ by (a). From (6.16) we find $y_0 \in \mathbb{C}$ such that

$$|y_0 - \alpha|_\infty \geq uNb \geq (1+\varepsilon)^2 Nb \quad \text{for all} \quad \alpha \in b\,;$$

$$|y_0 - z|_\infty \leq uNb \leq x_0^2 Nb\,,$$

as required.

Now suppose that $n > 0$. From the initial step with b replaced by bp^n we find $y \in \mathbb{C}$ such that

$$|y-\alpha|_\infty \geq (1+\varepsilon+\frac{1}{\sqrt{Np}}x_{n-1})^2 Nbp^n \quad \text{for all } \alpha \in bp^n;$$

$$|y-z|_\infty \leq (1+\varepsilon+\frac{1}{\sqrt{Np}}x_{n-1})^2 Nbp^n .$$

By the induction hypothesis, applied with y in the role of z, there exists y_{n-1} such that

$$|y_{n-1}-\alpha|_\infty \geq (1+\varepsilon)Nbp^r \quad \text{for all } r \text{ with } 0 \leq r \leq n-1 \text{ and all } \alpha \in bp^r;$$

$$|y_{n-1}-y|_\infty \leq x_{n-1}^2 Nbp^{n-1}.$$

We show that y_{n-1} also satisfies (6.18) for $r = n$. For $\alpha \in bp^n$ we have

$$|y_{n-1}-\alpha|_\infty \geq (|y-\alpha|_\infty^{\frac{1}{2}} - |y_{n-1}-y|_\infty^{\frac{1}{2}})^2 \geq$$

$$\geq ((1+\varepsilon+\frac{1}{\sqrt{Np}}x_{n-1})(Nbp^n)^{\frac{1}{2}} - x_{n-1}(Nbp^{n-1})^{\frac{1}{2}})^2 =$$

$$= (1+\varepsilon)^2 Nbp^n.$$

Next we check whether (6.19) holds. We have

$$|y_{n-1}-z|_\infty \leq (|y-z|_\infty^{\frac{1}{2}} + |y_{n-1}-y|_\infty^{\frac{1}{2}})^2 \leq$$

$$((1+\varepsilon+\frac{1}{\sqrt{Np}}x_{n-1})(Nbp^n)^{\frac{1}{2}} + x_{n-1}(Nbp^{n-1})^{\frac{1}{2}})^2 =$$

$$= (1+\varepsilon+\frac{2}{\sqrt{Np}}x_{n-1})^2 Nbp^n .$$

If $x_n \geq 1+\varepsilon+2x_{n-1}/\sqrt{Np}$ we find that (6.19) holds for y_{n-1}, and we may take $y_n = y_{n-1}$. Otherwise we have $x_n \geq \sqrt{\rho_n}$ by (a). Hence, by the properties of the covering radius (3.4), we may in that case shift y_{n-1} by an element of bp^n such that (6.19) holds. Such a shift does not affect (6.18). □

COROLLARY (6.20). *Let* ρ *be the minimum of the numbers* ρ_n, *for* $n \in \mathbb{Z}$. *If* $\rho > 1$ *and*

$$N\mathfrak{p} > \left(2 + \frac{1}{\sqrt{\rho} - 1}\right)^2,$$

then $\mathfrak{a}$ *is not Euclidean.*

PROOF. Choose $\varepsilon \in \mathbb{R}_{>0}$ such that $\sqrt{\rho} > 1 + \varepsilon$ and

$$N\mathfrak{p} > \left(2 + \frac{1+\varepsilon}{\sqrt{\rho} - 1 - \varepsilon}\right)^2.$$

For all $n \in \mathbb{Z}$ we define $x_n = \frac{\sqrt{N\mathfrak{p}}}{\sqrt{N\mathfrak{p}} - 2}(1+\varepsilon)$. Then

$$1 + \varepsilon + \frac{1}{\sqrt{N\mathfrak{p}}} x_{n-1} = (1+\varepsilon)\left(1 + \frac{1}{\sqrt{N\mathfrak{p}} - 2}\right) < \sqrt{\rho};$$

$$1 + \varepsilon + \frac{2}{\sqrt{N\mathfrak{p}}} x_{n-1} = x_n,$$

so the conditions of (6.17) are satisfied. □

COROLLARY (6.21). *Suppose that* A *has a Euclidean ideal class. Then*

$$N\mathfrak{p} \le 73 \quad \text{if } \Delta = -19;$$

$$N\mathfrak{p} \le 2351 \quad \text{if } \Delta = -23;$$

$$N\mathfrak{p} \le 109 \quad \text{if } \Delta = -24;$$

$$N\mathfrak{p} \le \left(2 + \frac{1}{r(\Delta) - 1}\right)^2 \quad \text{if } \Delta < -27,$$

with $r(\Delta) = \left(\frac{|\Delta|}{27}\right)^{\frac{1}{4}}$.

PROOF. Let ρ be the minimum of the ρ_n. By definition (3.3) there exist $a, b, c \in \mathbb{Z}_{\ge 0}$ with $b \le a \le c$, $|\Delta| = 4ac - b^2$ and $\rho = \frac{ac(a-b+c)}{|\Delta|}$.

If $\Delta = -19$, then $\rho = \frac{25}{19}$, so

$$N\mathfrak{p} \le \left(2 + \left(\sqrt{\tfrac{25}{19}} - 1\right)^{-1}\right)^2 = 77.424 \quad .$$

If $\Delta = -23$, then $\rho = \frac{24}{23}$, so

$$N\mathfrak{p} \le \left(2 + \left(\sqrt{\tfrac{24}{23}} - 1\right)^{-1}\right)^2 = 2351.734 \quad .$$

If $\Delta = -24$, then $\rho \geq \frac{5}{4}$, so

$$Np \leq (2 + (\sqrt{\tfrac{5}{4}} - 1)^{-1})^2 = 109.666 \quad .$$

Now suppose that $\Delta < -27$. As a function of b the value of $\rho|\Delta|^{-\frac{1}{2}} = ac(a-b+c)(4ac-b^2)^{-3/2}$ is decreasing, so $\rho|\Delta|^{-\frac{1}{2}} \geq ac^2(4ac-a^2)^{-3/2}$. As a function of c the value of $ac^2(4ac-a^2)^{-3/2}$ is increasing, so $\rho|\Delta|^{-\frac{1}{2}} \geq a^3(3a^2)^{-3/2} = 27^{-\frac{1}{2}}$, i.e. $\sqrt{\rho} \geq r(\Delta)$. Hence

$$Np \leq (2 + \frac{1}{r(\Delta) - 1})^2. \quad \square$$

PROPOSITION (6.22). *Let the* ρ_n *be as defined before (6.17). Suppose that* $\rho_0 = \min\{\rho_n : n \in \mathbb{Z}\}$ *and that* $\rho_0 > 1$. *Let* h *be the order of* p *in* $\mathrm{Cl}(\mathcal{O})$. *Define*

$$x_0 = \sqrt{\rho_0}\,;$$

$$x_n = \min\{\sqrt{\rho_n},\ 1 + \frac{2}{\sqrt{Np}}\, x_{n-1}\} \quad \text{for } 0 < n \leq h.$$

If $1 + x_{n-1}/\sqrt{Np} < \sqrt{\rho_n}$ *for* $0 < n \leq h$ *then* a *is not Euclidean.*

PROOF. By (6.20) we may suppose that $Np \leq (2 + \frac{1}{\sqrt{\rho_0} - 1})^2$. For $\varepsilon \in \mathbb{R}_{\geq 0}$ we define

$$x_0(\varepsilon) = \sqrt{\rho_0}\,;$$

$$x_n(\varepsilon) = \min\{\sqrt{\rho_n},\ 1 + \varepsilon + \frac{2}{\sqrt{Np}}\, x_{n-1}(\varepsilon)\} \quad \text{for } 0 < n \leq h.$$

Because the $x_n(\varepsilon)$ are continuous in ε there exists $\varepsilon > 0$ such that

$$1 + \varepsilon + \frac{x_{n-1}(\varepsilon)}{\sqrt{Np}} < \sqrt{\rho_n} \quad \text{for } 0 < n \leq h.$$

With induction on n, for $0 \leq n \leq h$ we show that $x_n(\varepsilon) \geq \sqrt{\rho_0}$. If $n = 0$ this is obvious. Now suppose that $n > 0$. If $x_n(\varepsilon) = \sqrt{\rho_n}$ we are done. Otherwise we have by induction

$$
\begin{aligned}
x_n(\varepsilon) &= 1 + \varepsilon + \frac{2}{\sqrt{Np}}\, x_{n-1}(\varepsilon) \;\geq\; 1 + \varepsilon + \frac{2}{\sqrt{Np}} \sqrt{\rho_0} \;\geq \\
&\geq \varepsilon + \frac{2\rho_0 - 1}{2\sqrt{\rho_0} - 1} \qquad\qquad \text{since } \sqrt{Np} \leq 2 + \frac{1}{\sqrt{\rho_0} - 1} \\
&> \sqrt{\rho_0}\,.
\end{aligned}
$$

In particular this shows that $x_h(\varepsilon) = \sqrt{\rho_0} = x_0(\varepsilon)$. If for all $n \in \mathbb{Z}$ we inductively define $x_n(\varepsilon) = x_{n+h}(\varepsilon)$ we see that the $x_n(\varepsilon)$ satisfy the requirements of (6.17). □

The results of the last two sections show that for $\Delta \notin \{-3,-4,-7,-8,-11,-15,-20\}$ there are only finitely many rings with a Euclidean ideal class.

CHAPTER 7 ARITHMETICAL RESTRICTIONS ON A EUCLIDEAN IDEAL CLASS

As in chapter 6 we will only consider the imaginary quadratic case ($\#2^-$) in this chapter. We will use the notation explained at the beginning of chapter 6.

Let $\mathfrak{a}$ be an A-ideal. In section (7.1) we derive several necessary conditions for $\mathfrak{a}$ to be Euclidean, by using (1.8) for $\alpha \in \mathfrak{a}\mathfrak{c}^{-1}$, where $\mathfrak{c}$ is an integral ideal of small norm. In section (7.2) we check whether these conditions are satisfied in the case that $\mathfrak{p}$ is Galois-invariant, i.e. lies over an inert or ramifying prime in $K/\mathbb{Q}$. We will find that in this case at most ten rings have a Euclidean ideal class. In chapter 9 we will see that all these ten rings do in fact have a Euclidean ideal class. This finishes the determination in this case.

In section (7.3) we list all rings, in case ($\#2^-$), for which we do at this stage not yet know whether or not they have a Euclidean ideal class. In section (7.4) we apply the methods of section (7.1) to several rings in this list. In contrast to section (7.2) these are rings for which $\mathfrak{p}$ lies over a prime that splits in $K/\mathbb{Q}$.

§(7.1) Elements with small denominators

Let $\mathfrak{a}$ be an A-ideal and let $\mathfrak{c}$ be an integral A-ideal. We may check the Euclidean condition (1.8) for elements of $\mathfrak{a}\mathfrak{c}^{-1}$ in order to determine whether $\mathfrak{a}$ is Euclidean.

The unit group A^* acts on $\mathfrak{a}\mathfrak{c}^{-1}/\mathfrak{a}$ by multiplication. Whether or not a residue class of $\mathfrak{a}\mathfrak{c}^{-1}$ mod $\mathfrak{a}$ contains an element of norm less than $N\mathfrak{a}$ only depends on the A^*-orbit of this residue class. If the number of A^*-orbits is large we may hope that there are residue classes that do not contain elements of norm less than $N\mathfrak{a}$.

PROPOSITION (7.1). *Let* $\mathfrak{c}$ *be an integral* A*-ideal. Denote by* k *the order of the subgroup* (A^* mod $\mathfrak{c}$) *in* $(A/\mathfrak{c})^*$. *Suppose that* $\mathfrak{a}$ *is a Euclidean* A*-ideal. Then the number of integral* A*-ideals* $\mathfrak{d}$ *in the ideal class* $[\mathfrak{a}^{-1}\mathfrak{c}]$ *with* $N\mathfrak{d} < N\mathfrak{c}$ is at least $\frac{N\mathfrak{c}-1}{k}$.

PROOF. Each orbit of A^* in $(\mathfrak{a}\mathfrak{c}^{-1}/\mathfrak{a}) - \{0\}$ contains at most k elements. Since $\#((\mathfrak{a}\mathfrak{c}^{-1}/\mathfrak{a}) - \{0\}) = N\mathfrak{c} - 1$ the number m of A^*-orbits is at least $\frac{N\mathfrak{c}-1}{k}$. Let $\alpha_1,\ldots,\alpha_m \in \mathfrak{a}\mathfrak{c}^{-1}$ be such that the $\alpha_i + \mathfrak{a}$ form a system of representatives of A^*-orbits in $(\mathfrak{a}\mathfrak{c}^{-1}/\mathfrak{a}) - \{0\}$. Because $\mathfrak{a}$ is Euclidean we may suppose that $N(\alpha_i) < N\mathfrak{a}$. By construction the residue classes $\alpha_i + \mathfrak{a}$ lie in different A^*-orbits, hence all ideals $\alpha_i A$ are different. This shows that the integral ideals $\mathfrak{d}_i = \alpha_i \mathfrak{a}^{-1}\mathfrak{c}$ are all different and all satisfy $N\mathfrak{d}_i < N\mathfrak{c}$. Also we have $\mathfrak{d}_i \in [\mathfrak{a}^{-1}\mathfrak{c}]$. □

Proposition (7.1) is only useful if k is small. In fact, we only rarely apply (7.1) with k exceeding 2. In addition, we only consider ideals $\mathfrak{c}$ of small norm, not only to avoid too lengthy computations, but also for the following reason. For a given ring A the value of $\frac{N\mathfrak{c}-1}{k}$ is bounded above by $a\frac{N\mathfrak{c}}{\log N\mathfrak{c}}$ for some constant a not depending on $\mathfrak{c}$, whereas the number of integral A-ideals in a given ideal class of norm less than $N\mathfrak{c}$ is asymptotically equal to a linear function of $N\mathfrak{c}$, cf. [La2] ch.VI §3 thm.3. Hence for $\mathfrak{c}$ with a large norm (7.1) cannot be applied.

We will need two special cases of (7.1).

COROLLARY (7.2). *Suppose that* $p \nmid 2$ *and that for any* $\tau \in A^*$ *we have* $\tau \equiv 1 \bmod 2A$. *Also suppose that* A *has a Euclidean ideal class* $[\mathfrak{a}]$. *Then* A *has at least* 3 *distinct integral ideals of norm* < 4 *in* $[\mathfrak{a}]$.

PROOF. Take $\mathfrak{c} = 2A$ in (7.1). Then $N\mathfrak{c} = 4$ and $k = 1$. Notice that $[\mathfrak{a}] = [\mathfrak{a}^{-1}]$ since $h(A)\,|\,2$. □

COROLLARY (7.3). *Suppose that* $p \nmid 3$ *and that for each* $\tau \in A^*$ *we have* $\tau \equiv \pm 1 \bmod 3A$. *Also suppose that* A *has a Euclidean ideal class* $[\mathfrak{a}]$. *Then* A *has at least* 4 *distinct integral ideals of norm* < 9 *in* $[\mathfrak{a}]$.

PROOF. Take $\mathfrak{c} = 3A$ in (7.1). Then $N\mathfrak{c} = 9$ and $k = 2$. □

If $h(A) = 2$ we have additional information.

LEMMA (7.4). *Suppose that* $h(A) = 2$ *and that* A *has a Euclidean ideal class.*

(a) *If* $p \nmid 2$ *then* A *has a non-principal integral ideal of norm* 3.

(b) *If* $6 \mid \Delta$ *and* $p \nmid 6$ *then* A *has a non-principal integral ideal of norm* 5.

(c) *If* $p \nmid 3$ *then* A *has a non-principal integral ideal of norm* 2, 5 *or* 7.

PROOF. Analogous to the proof of (5.22). □

§(7.2) Primes that are Galois-invariant.

In this section we assume that the Galois group Gal(K/ℚ) acts on A. This means that for the generator σ of Gal(K/ℚ) we have $\sigma p = p$, i.e. p lies over a ramifying or an inert prime in K/ℚ. We will use the results of section (7.1) to show that if A has a Euclidean ideal class it must be one of the rings listed in theorem (7.6). In section (9.2) we show that all these 10 rings have in fact a Euclidean ideal class.

In the proof of (7.6) we need the following information about rings $\mathcal{O}$ with principal ideals of small norm.

TABLE 6. Elements of small norms in $\mathcal{O}$.

Notation: 'h = 2 × 2' means $Cl(\mathcal{O}) \simeq V_4$
'h = m' means $Cl(\mathcal{O}) \simeq \mathbb{Z}/m\mathbb{Z}$

n	Δ	h	n	Δ	h
2	-		21	-35	2
3	-			-68	4
4	-			-84	2×2
5	-19	1	25	-19	1
6	-24	2		-24	2
7	-19	1		-51	2
	-24	2		-84	2×2
9	-35	2		-91	2
10	-24	2	35	-19	1
	-39	4		-35	2
	-40	2		-40	2
14	-40	2		-91	2
	-52	2		-115	2
	-55	4		-136	4
	-56	4	49	-19	1
15	-24	2		-24	2
	-35	2		-40	2
	-51	2		-52	2
	-56	4		-115	2
				-132	2×2
				-187	2
				-195	2×2

LEMMA (7.5). *In table 6 one finds for each n in the first column all values of $\Delta < -20$ or $\Delta = -19$ for which there exists $\alpha \in \mathcal{O} - \mathbb{Z}$ of norm n, and for which $h(\mathcal{O})$ divides 4.*

PROOF. Such a discriminant Δ must satisfy $X^2 - \Delta Y^2 = 4n$ for certain $X,Y \in \mathbb{Z}$, with $Y \neq 0$. This gives the bound $|\Delta| \leq 4n$. Table 6 is obtained by checking whether this equation is satisfied for these Δ. We use an existing list of class numbers, e.g. [BS], to restrict to those Δ for which $h(\mathcal{O})|4$. □

THEOREM (7.6). *Let K be an imaginary quadratic number field and let p be a prime number that is inert or ramifying in $K/\mathbb{Q}$. Let S be equal to $\{\infty,\mathfrak{p}\}$ where $\mathfrak{p}$ is the prime of K lying over p. Suppose that $\Delta \notin \{-3,-4,-7,-8,-11,-15,-20\}$ and that $A = A_S$ has a Euclidean ideal class. Then we are in one of the following cases.*

h(A) = 1:		h(A) = 2:	
Δ	p	Δ	p
-19	2	-35	2
-24	2	-56	2
-35	5	-68	2
-35	7	-84	2
-40	2	-136	2

PROOF. Because the order of $[\mathfrak{p}]$ in $Cl(\mathcal{O})$ is at most 2 and h(A) divides 2 we have $h(\mathcal{O})|4$, cf. (2.7) and (2.12). Let η be a fundamental unit of A with $|\eta|_{\mathfrak{p}} < 1$.

We split the proof into 10 parts:

(a) $p \neq 2$ and $\eta \not\equiv 1 \bmod 2A$;
(b) $p \neq 2$, $\eta \equiv 1 \bmod 2A$ and $h(\mathcal{O}) = 1$;
(c) $p \neq 2$, $\eta \equiv 1 \bmod 2A$ and $h(\mathcal{O}) = 2$;
(d) $p \neq 2$, $\eta \equiv 1 \bmod 2A$ and $Cl(\mathcal{O}) \simeq \mathbb{Z}/4\mathbb{Z}$;
(e) $p \neq 2$, $\eta \equiv 1 \bmod 2A$ and $Cl(\mathcal{O}) \simeq V_4$;
(f) $p = 2$ and $\eta \not\equiv \pm 1 \bmod 3A$;
(g) $p = 2$, $\eta \equiv \pm 1 \bmod 3A$ and $h(\mathcal{O}) = 1$;
(h) $p = 2$, $\eta \equiv \pm 1 \bmod 3A$ and $h(\mathcal{O}) = 2$;
(i) $p = 2$, $\eta \equiv \pm 1 \bmod 3A$ and $Cl(\mathcal{O}) \simeq \mathbb{Z}/4\mathbb{Z}$;
(j) $p = 2$, $\eta \equiv \pm 1 \bmod 3A$ and $Cl(\mathcal{O}) \simeq V_4$.

Since each unit of A is of the form $\pm\eta^k$ for some $k \in \mathbb{Z}$ we may use (7.2) for parts (b), (c), (d) and (e) to find that A has at least 3 integral ideals of norm < 4 in the Euclidean ideal class. For parts (g), (h), (i) and (j) we use (7.3) to find that A has at least 4 integral ideals of norms < 9 in the Euclidean ideal class. Moreover, since $p = 2$, these ideals have odd norms.

(a) Suppose that $p \neq 2$ and $\eta \not\equiv 1 \bmod 2A$. Then p must be ramified in $K/\mathbb{Q}$ and $\mathfrak{p} = \eta\mathcal{O}$, since otherwise η is equal to $\pm p \equiv 1 \bmod 2A$. This shows that $h(A) = h(\mathcal{O})$ and $\eta^2 = \pm p$, i.e. $\eta = \sqrt{-p}$. This is only possible if $\Delta = -p$ or $\Delta = -4p$. However if $\Delta = -p$ then $p \equiv -1 \bmod 4A$ and thus $\eta = \sqrt{-p} \equiv 1 \bmod 2A$. So $\Delta = -4p$ and also 2 ramifies in $K/\mathbb{Q}$. Using table 6 we find that the $\mathcal{O}$-ideal of norm 2 cannot be principal hence $h(\mathcal{O}) = h(A) = 2$. From (7.4)(a) we deduce that A, and hence $\mathcal{O}$, has a non-principal ideal of norm 3. Multiplying by the non-principal ideal of norm 2 shows that $\mathcal{O}$ has a principal ideal of norm 6. Inspecting table 6 shows that $\Delta = -24$, but this is not of the form $-4p$, a contradiction.

(b) Suppose that $p \neq 2$, $\eta \equiv 1 \bmod 2A$ and $h(\mathcal{O}) = 1$. Intersecting the integral A-ideals of norm < 4 with $\mathcal{O}$ shows that $\mathcal{O}$ has at least 3 integral ideals of norm < 4 as well. From table 6 we see that this is impossible.

(c) Suppose that $p \neq 2$, $\eta \equiv 1 \bmod 2A$ and $h(\mathcal{O}) = 2$. If $\mathfrak{p}$ is principal, then also $h(A) = 2$. Intersecting the 3 non-principal integral A-ideals of norm < 4 with $\mathcal{O}$ shows that $\mathcal{O}$ has 3 non-principal integral ideals of norm < 4 as well. By multiplying or squaring them we find an element of $\mathcal{O}$ of norm 6 and an element of $\mathcal{O} - \mathbb{Z}$ of norm 4 or 9. A look at table 6 shows that this is not possible.

If $\mathfrak{p}$ is not principal then p must be ramified in $K/\mathbb{Q}$ and $h(A) = 1$. We intersect the A-ideals of norm < 4 with $\mathcal{O}$ to obtain at least 3 integral $\mathcal{O}$-ideals of norm < 4. We find by inspecting table 6 that at most one of them can be principal, and then it is equal to $\mathcal{O}$. Hence two of them must be non-principal. By multiplying or squaring them we find an element of $\mathcal{O} - \mathbb{Z}$ with norm 4, 6 or 9. From table 6 we find that $\Delta = -24$ or $\Delta = -35$. However if $\Delta = -24$ then $p = 3$ and A does not have 3 integral ideals of norm < 4. So $\underline{\Delta = -35 \text{ and } p = 5 \text{ or } p = 7}$.

(d) Suppose that $p \neq 2$, $\eta \equiv 1 \bmod 2A$ and $Cl(\mathcal{O}) \simeq \mathbb{Z}/4\mathbb{Z}$. Then $h(A) = \frac{1}{2}h(\mathcal{O}) = 2$ and $\mathfrak{p}$ is non-principal, hence p is ramified in $K/\mathbb{Q}$.

Then $\mathcal{O}$ must have at least 3 integral ideals of norms < 4 in ideal classes of order 4. Because the conjugate of an ideal is in the inverse ideal class we see that both ideal classes of order 4 contain integral ideals of norms 2 and 3. By an appropriate multiplication we find that $\mathcal{O}$ has an element of norm 6. A look at table 6 shows that this is not possible.

(e) Suppose that $p \neq 2$, $\eta \equiv 1 \bmod 2A$ and $Cl(\mathcal{O}) \simeq V_4$. Again we have $h(A) = \frac{1}{2}h(\mathcal{O}) = 2$ and $\mathfrak{p}$ is non-principal, hence p is ramified in $K/\mathbb{Q}$. Then $\mathcal{O}$ has at least 3 integral non-principal ideals of norm < 4. By squaring we find that there exist elements of $\mathcal{O}$, not in $\mathbb{Z}$, with norm 4 or 9. By inspecting table 6 we find that this is impossible.

(f) Suppose that $p = 2$ and $\eta \not\equiv \pm 1 \bmod 3A$. Then η is an element of $\mathcal{O}$ of norm 2, which is not possible.

(g) Suppose that $p = 2$, $\eta \equiv \pm 1 \bmod 3A$ and $h(\mathcal{O}) = 1$. Then $\mathcal{O}$ has 4 integral ideals of odd norms < 9. By inspecting table 6 we find that $\underline{\Delta = -19}$.

(h) Suppose that $p = 2$, $\eta \equiv \pm 1 \bmod 3A$ and $h(\mathcal{O}) = 2$. If $\mathfrak{p}$ is principal then $h(A) = 2$ and 2 is inert in $K/\mathbb{Q}$, since $\mathcal{O}$ does not contain elements of norm 2. There are at least 4 non-principal integral $\mathcal{O}$-ideals of odd norms < 9. By multiplying and squaring we find 3 elements of $\mathcal{O} - \mathbb{Z}$ whose norms form one of the sets $\{9,15,25\}$, $\{9,21,49\}$, $\{25,35,49\}$, $\{15,21,35\}$. A look at table 6 shows that $\underline{\Delta = -35}$.

If $\mathfrak{p}$ is non-principal then $h(A) = 1$ and 2 ramifies in $K/\mathbb{Q}$. There are at least 4 integral $\mathcal{O}$-ideals of odd norms < 9. This occurs when $\underline{\Delta = -24}$. If $\Delta \neq -24$ at least 3 of these ideals must be non-principal. By multiplication we find that $\mathcal{O}$ has an element of norm 15, 21 or 35. A look at table 6 shows that $\underline{\Delta = -40}$.

(i) Suppose that $p = 2$, $\eta \equiv \pm 1 \bmod 3A$ and $Cl(\mathcal{O}) \simeq \mathbb{Z}/4\mathbb{Z}$. Then $h(A) = \frac{1}{2}h(\mathcal{O}) = 2$ and $\mathfrak{p}$ is non-principal, hence 2 ramifies in $K/\mathbb{Q}$. The ideal classes of order 4 of $\mathcal{O}$ must contain at least 4 integral ideals of odd norms < 9. Because the conjugate of an ideal is in the inverse ideal class we find that each ideal class of order 4 contains two integral ideals of norms 3, 5 or 7. By multiplication we obtain an element of $\mathcal{O}$ of norm 15, 21 or 35. From table 6 we derive that $\underline{\Delta = -56, -68 \text{ or } -136}$.

(j) Finally suppose that $p = 2$, $\eta \equiv \pm 1 \bmod 3A$ and $Cl(\mathcal{O}) \simeq V_4$. Then $h(A) = \frac{1}{2}h(\mathcal{O}) = 2$ and $\mathfrak{p}$ is non-principal, hence 2 ramifies in $K/\mathbb{Q}$. There are 4 integral $\mathcal{O}$-ideals of odd norms < 9 in the two ideal classes of $Cl(\mathcal{O}) - \langle[\mathfrak{p}]\rangle$. If there are two pairs of two ideals of the same norm we find by squaring two elements of $\mathcal{O} - \mathbb{Z}$ with different norms in $\{9,25,49\}$. Consulting table 6 shows that this is not possible. Hence $\mathcal{O}$ has ideals of norms 3, 5 and 7 and there is an ideal class that contains ideals with two of these norms. Multiplying them shows that $\mathcal{O}$ has an element of norm 15, 21 or 35. We use table 6 to get $\underline{\Delta = -84}$. □

§(7.3) List of unsettled cases

In chapter 6 we found that there are only finitely many rings for which we have not yet decided whether they have a Euclidean ideal class. (As remarked at the beginning of this chapter, we are still assuming that we are in case $(\#2^-)$.) All these rings have $|\Delta| \leq 1007$. This follows from the fact that we found in (6.14) that $|\Delta| > 1007$ may only occur if $\mathfrak{p}|2$ and 2 is inert in $K/\mathbb{Q}$. However, we found in the last section that $|\Delta| \leq 35$ for such $\mathfrak{p}$.

In the preceding sections we derived several restrictions that rings with a Euclidean ideal class must satisfy. Table 7 lists all rings for which the existence of a Euclidean ideal class remains unsettled, when these restrictions are taken into account. In section (7.4) and in chapters 8 and 9 we will deal with the rings occurring in table 7.

Table 7 is organized as follows. The first column 'Δ' lists the discriminants Δ with $\Delta = -19$ or $-23 \geq \Delta \geq -1007$. The second column 'H' gives the class number of $\mathcal{O}$. The third column '$\tilde{a}$' gives the largest a for which there is a reduced quadratic form (a,b,c) of discriminant Δ. In the fourth column we find the value $\rho \cdot |\Delta|$, which is a positive integer, where ρ is the least value of a covering radius of an $\mathcal{O}$-ideal. In the fifth column 'p≤' we find the integral part of $(1 - 4\sqrt{\tilde{a}/|\Delta|})^{-1}$, which is an upper bound on p by (6.15). In the sixth column 'N𝔭≤' we find the integral part of $(2 + 1/(\sqrt{\rho} - 1))^2$. In (6.20) we found that this is an upperbound on $N\mathfrak{p}$. In the seventh column 'primes' we list all rational primes p contained in a prime $\mathfrak{p}$ of K, such that p and $N\mathfrak{p}$ satisfy these bounds and the additional conditions given below. If there are no primes left in this column we have omitted the whole row containing Δ. In the last column '#' we find the number of rings in this list with discriminant $\geq \Delta$. In particular we see that the table contains 274 rings.

The additional conditions for a prime p to occur in the seventh column of table 7 are as follows. If p is not splitting we must be in one of the cases listed in (7.6). Also we must have $h(A) | 2$ by (2.12). If $N\mathfrak{p} = 2$ we must have $|\Delta| \leq \frac{512}{9} \hat{a}$, by (6.14). If $h(A) = 2$ the condition of (7.4) must be satisfied. In this case also the upperbounds on p and $N\mathfrak{p}$ may be improved. This is because the values of $\hat{a}$ and ρ occurring in (6.14) and (6.20) may be different from the values of $\tilde{a}$ and ρ listed in table 7. If p does not satisfy these new bounds, but it does satisfy the conditions given above, then p is not included in table 7, but it is listed in table 9. In fact it did not occur that (6.20) was used in this way. Possibly this is due to the fact that for most Δ the bound of (6.14) is better. Finally (6.22) must be satisfied (we include $h(A) = 1$ again). The primes $\mathfrak{p}$ for which A has no Euclidean ideal class by (6.22) but that satisfy the earlier conditions are listed in table 10; they are not included in table 7.

For $\Delta = -23$ there are 116 primes that satisfy the conditions. They are listed separately in table 8.

TABLE 7. Rings that may have a Euclidean ideal class.

Δ	H	$\tilde{a}$	$\rho\cdot\|\Delta\|$	p≤	Np≤	primes	#
-19	1	1	25	12	77	2, 5, 7, 11	4
-23	3	2	24	-	2351	see table 8	120
-24	2	2	30	-	109	2, 5, 7, 11, 29, 31, 53, 59, 73, 79, 83, 101	132
-31	3	2	40	-	87	2, 5, 7, 19, 41, 59, 71	139
-35	2	3	45	-	89	2, 3, 5, 7, 11, 13, 17, 29, 47, 71, 73, 83	151
-39	4	3	48	-	124	2, 5, 11, 41, 47, 59, 71, 83, 89	160
-40	2	2	70	9	25	2, 7	162
-47	5	3	72	-	83	2, 3, 7, 17	166
-51	2	3	75	33	44	5, 11, 13, 19, 23, 29	172
-55	4	4	80	-	46	2, 7, 13, 17, 43	177
-56	4	3	90	13	32	2, 3, 5, 13	181
-59	3	3	105	10	24	3, 5, 7	184
-68	4	3	126	6	22	2, 3	186
-71	7	4	120	19	28	2, 3, 5, 19	190
-79	5	4	160	10	19	2, 5	192
-83	3	3	189	4	15	3	193
-84	4	5	150	41	24	2, 11, 19	196
-87	6	4	168	7	20	2	197
-91	2	5	175	16	21	5	198
-95	8	5	180	12	21	2, 3	200
-103	5	4	224	4	16	2	201
-104	6	5	210	8	19	5, 7	203
-107	3	3	297	3	12	3	204
-111	8	5	240	6	17	2, 5	206
-116	6	5	270	5	15	3	207
-119	10	6	252	9	17	3, 5	209
-127	5	4	352	3	12	2	210
-131	5	5	315	4	14	3	211
-136	4	5	350	4	13	2	212
-143	10	6	336	5	15	2	213
-151	7	5	400	3	12	2	214

TABLE 7. Continued.

Δ	H	$\tilde{a}$	ρ·|Δ|	p≤	Np≤	primes	#
−152	6	6	378	4	13	3	215
−155	4	5	405	3	13	3	216
−159	10	6	420	4	12	2	217
−164	8	6	450	4	12	3	218
−167	11	6	432	4	13	2, 3	220
−179	5	5	585	3	10	3	221
−183	8	6	528	3	11	2	222
−191	13	6	540	3	12	2, 3	224
−199	9	7	560	4	12	2	225
−203	4	7	567	3	12	3	226
−212	6	6	702	3	10	3	227
−215	14	7	660	3	11	2, 3	229
−223	7	7	784	3	9	2	230
−227	5	7	693	3	11	3	231
−239	15	8	720	3	11	2	232
−247	6	8	832	3	10	2	233
−248	8	7	858	3	10	3	234
−251	7	7	945	3	9	3	235
−263	13	8	864	3	10	2, 3	237
−271	11	8	880	3	10	2	238
−287	14	8	1008	3	9	3	239
−295	8	8	1040	2	9	2	240
−303	10	8	1056	2	9	2	241
−311	19	9	1080	3	9	2, 3	243
−319	10	10	1100	3	10	2	244
−323	4	9	1377	3	8	3	245
−327	12	8	1232	2	9	2	246
−335	18	9	1248	2	9	2	247
−359	19	10	1320	3	9	2, 3	249
−367	9	8	1456	2	9	2	250
−383	17	9	1512	2	9	2	251
−407	16	11	1584	2	9	2	252
−415	10	10	1760	2	8	2	253
−439	15	10	1820	2	8	2	254

TABLE 7. Continued.

Δ	H	$\tilde{a}$	ρ·|Δ|	p≤	N𝑝≤	primes	#
-447	14	11	1848	2	8	2	255
-471	16	10	2080	2	8	2	256
-479	25	11	2100	2	8	2	257
-519	18	11	2400	2	8	2	258
-535	14	11	2464	2	8	2	259
-543	12	12	2496	2	8	2	260
-551	26	12	2520	2	8	2	261
-559	25	12	2548	2	8	2	262
-583	8	11	2816	2	8	2	263
-591	22	12	2856	2	8	2	264
-599	25	12	2880	2	8	2	265
-607	13	13	2912	2	8	2	266
-647	23	13	3264	2	7	2	267
-671	30	14	3360	2	7	2	268
-703	14	14	3724	2	7	2	269
-719	31	14	3780	2	7	2	270
-727	13	14	3808	2	7	2	271
-839	33	15	4788	2	7	2	272
-863	21	16	4896	2	7	2	273
-1007	30	18	6156	2	7	2	274

TABLE 8. Subrings $A_{\{\mathfrak{p},\infty\}}$ of $\mathbb{Q}(\sqrt{-23})$ that may have a Euclidean ideal class.

$N\mathfrak{p}$	$N\mathfrak{p}$	$N\mathfrak{p}$	$N\mathfrak{p}$
2	461	1087	1733
3	487	1093	1741
13	491	1129	1777
29	499	1153	1783
31	509	1223	1823
41	541	1237	1933
47	547	1277	1973
71	577	1283	1979
73	587	1289	1987
127	601	1291	2003
131	647	1297	2017
139	653	1301	2063
151	673	1327	2083
163	683	1361	2099
179	739	1373	2111
193	761	1381	2129
197	811	1409	2141
233	823	1427	2203
239	857	1429	2221
257	859	1439	2237
269	863	1499	2239
277	887	1511	2243
311	929	1531	2267
331	947	1543	2281
349	967	1549	2293
353	1013	1559	2341
397	1021	1567	
409	1039	1619	
439	1051	1637	
443	1061	1657	

TABLE 9. Primes that do not satisfy (6.14). For the rational prime p in $\mathfrak{p}$ we must have $p \le (1 - 4\sqrt{\frac{\hat{a}}{|\Delta|}})^{-1}$

Δ	p	$\hat{a}$	$(1 - 4\sqrt{\frac{\hat{a}}{|\Delta|}})^{-1}$
-39	61	2	10.618
-39	79	2	10.618
-84	5	3	4.097
-84	7	3	4.097
-87	7	3	3.888
-95	11	3	3.458
-116	5	3	2.803
-120	5	3	2.721

TABLE 10. The use of (6.22).

Δ	$N\mathfrak{p}$	H	n	$\rho_n \cdot |\Delta|$	x_n
-24	97	1	0	30	1.118
-24	103	1	0	30	1.118
-24	107	1	0	30	1.118
-35	79	1	0	45	1.134
-47	37	5	0	72	1.238
			1	84	1.337
			2	84	1.337
			3	72	1.238
			4	144	1.407
-84	23	2	0	150	1.336
			1	210	1.557

§(7.4) Splitting primes

If p lies over a splitting prime in $K/\mathbb{Q}$ it is in most cases not possible to use (7.1). Usually the primes over 2 and 3 generate already too many ideals of small norm. However for certain rings we can use (7.2), i.e. $\mathfrak{a} = 2A$. Table 11 lists those rings.

TABLE 11. Rings A occurring in table 7 with p splitting, $\eta \equiv 1 \bmod 2A$ and less than 3 integral ideals in the generating class of Cl(A) have norm < 4. If $\Delta \equiv 0 \bmod 4$ we write $\omega = \frac{1}{2}\sqrt{\Delta}$, otherwise $\omega\ \frac{1}{2}(1 + \sqrt{\Delta})$.

Δ	p	h(A)	η
-24	73	2	$7 + 2\omega$
-35	71	2	$5 + 2\omega$
-40	7	1	$3 + 2\omega$
-51	29	1	$1 + 8\omega$
-84	19	2	$5 + 4\omega$
-179	3	1	$7 + 2\omega$
-227	3	1	$3 + 2\omega$
-251	3	1	$43 + 2\omega$

For other rings we may use a refinement of (7.1). In fact it is the same method which has been used in section (5.5) to deal with $\Delta = 265$. Let $\mathfrak{a}$ be an integral ideal such that $\eta \bmod \mathfrak{a}$ has small multiplicative order, where η is a fundamental unit of A. In fact we only consider the case that this order is 1 or 2. By investigating all principal ideals of norm $< N\mathfrak{a}$ we find whether there exists a residue class mod $\mathfrak{a}$ not containing an element of norm $< N\mathfrak{a}$. If we find such a residue class we know that $\mathfrak{a}$ is not Euclidean. Although the method should work for every ring which has no Euclidean ideal class it is only feasible if $N\mathfrak{a}$ is small. In table 12 we list those rings, occurring in table 7 but not in table 11, for which the method works for some ideal $\mathfrak{a}$ with $N\mathfrak{a} < 80$. In all cases the order of $\eta \bmod \mathfrak{a}$ is equal to 1 or 2.

Tables 11 and 12 contain 34 rings. Hence for 240 rings we still do not know whether there is a Euclidean ideal class. These rings will be dealt with in the next two chapters.

TABLE 12. Integral ideals of small norm in the generating class of Cl(A) which are not Euclidean. The letter c denotes a residue class mod $\mathfrak{a}$ which does not contain an element of norm $< N\mathfrak{a}$. If Δ is even we write $\omega = \frac{1}{2}\sqrt{\Delta}$, otherwise $\omega = \frac{1}{2}(1+\sqrt{\Delta})$.

Δ	p	η	$\mathfrak{a}$	$N\mathfrak{a}$	c
−24	11	$5 + 4\omega$	$\langle 2\rangle$	4	$1+\omega$
	31	$5 + \omega$	$\langle 21,\eta+1\rangle$	21	10
	59	$5 + 24\omega$	$\langle 2\rangle$	4	$1+\omega$
	83	$67 + 20\omega$	$\langle 2\rangle$	4	$1+\omega$
−35	29	$4 + \omega$	$\langle 7,\eta-1\rangle$	7	3
−51	5	$3 + \omega$	$\langle 11,\eta+1\rangle$	11	4
	13	ω	$\langle 39,\eta^2-1\rangle$	39	7
	19	$2 + \omega$	$\langle 15,\eta^2-1\rangle$	75	$2+2\omega$
−56	3	$5 + 2\omega$	$\langle 2\rangle$	4	$1+\omega$
−59	7	$13 + 3\omega$	$\langle 7,\eta-1\rangle$	7	3
−83	3	$2 + \omega$	$\langle 11,\eta+1\rangle$	11	5
−84	11	$10 + \omega$	$\langle 6,\eta-1\rangle$	6	3
−91	5	$1 + \omega$	$\langle \eta-1\rangle$	23	7
−107	3	ω	$\langle \eta-1\rangle$	27	12
−152	3	$11 + 4\omega$	$\langle 2\rangle$	4	$1+\omega$
−155	3	$6 + \omega$	$\langle 23,\eta-1\rangle$	23	10
−203	3	$5 + \omega$	$\langle 31,\eta+1\rangle$	31	13
−212	3	$26 + \omega$	$\langle 17,\eta+1\rangle$	17	7
−223	2	$8 + \omega$	$\langle 16\rangle$	16	5
−247	2	$1 + \omega$	$\langle 17,\eta+1\rangle$	17	5
−248	3	$19 + 10\omega$	$\langle 2\rangle$	4	$1+\omega$
−295	2	$13 + \omega$	$\langle 23,\eta-1\rangle$	23	5
−323	3	ω	$\langle 9\rangle$	9	4
−367	2	$20 + \omega$	$\langle 8\rangle$	8	3
−415	2	$8 + 3\omega$	$\langle 3\rangle$	9	ω
−607	2	$24 + 7\omega$	$\langle 13,\eta-1\rangle$	13	6

CHAPTER 8 REFINEMENT OF THE METHODS

As in the last two chapters we restrict ourselves in this chapter to the case $(\#2^-)$. Also we restrict to the case that p lies over a splitting prime. This is not a severe restriction since in section (7.2) we considered the other primes. We continue to use the notation as given at the beginning of chapter 6.

When we consider the lists of unsettled cases in section (7.3) it is striking that they contain many more rings with $\Delta = -23$ than with any other discriminant. Also there are more rings for which the non-archimedean infinite prime has norm 2 than with any other given norm. For both cases we will refine Cassels' theorem (5.16). The first refinement also works for other cases where $h(\mathcal{O})$ is small, but the main gain is for $\Delta = -23$. It will be treated in sections (8.1) and (8.2). For the cases with $Np = 2$ we will refine the proof of (6.14) in section (8.3).

§(8.1) Jumping to points in a given ideal

In this section we take an integer $h \in \mathbb{Z}_{>0}$ fixed such that p^h is a principal $\mathcal{O}$-ideal. We will construct an $\alpha \in K$ such that $\eta\alpha \equiv \alpha \bmod bp^{h-1}$ for some generator η of p^h and for which $\alpha \notin \bigcup_{i=0}^{h-1} W_t(bp^i)$ for some large $t \in \mathbb{R}_{>0}$. (For the definition of $W_t(bp^i)$ see (6.3).) Using (6.7) we find that a is not Euclidean if $t \geq 1$. The construction of α is a refinement of the construction used in the proof of (6.17). A close look at this proof shows that we are constructing a series $(\alpha_n)_{n \in \mathbb{Z}_{\geq 0}}$ such that $\alpha_n \notin \bigcup_{i=0}^{n} W_t(bp^{-i})$ for some fixed $t \in \mathbb{R}_{>0}$. We get α_{n+1} by shifting α_n by some $v_n \in \mathbb{C}$ for which $|v_n|_\infty$ is not larger than $N(bp^{-n-1})$ times some constant depending on the covering radii of the ideals bp^i. Then α is taken to be the limit in $\mathbb{C}$ of the sequence $(\alpha_n)_{n \in \mathbb{Z}_{\geq 0}}$. The refinement consists of demanding that each α_n is in a certain $\mathcal{O}$-ideal. This allows us to use arithmetical data to obtain better upper-bounds on $|v_n|_\infty$. Also we will choose α_n in such a way as to get $\eta\alpha \equiv \alpha \bmod bp^{h-1}$. The bounds on $|v_n|_\infty$ give us values of t for which

$\alpha \notin \bigcup_{i=0}^{h-1} W_t(bp^i)$. This in turn gives us bounds on Np for rings with a Euclidean ideal class. These bounds may be better than the bounds of chapter 6.

Let b_i be O-ideals such that $[b_i] = [bp^i]$, for $0 \le i \le h$. With induction we define $b_{i+h} = b_i$ for $i \in \mathbb{Z}_{>0}$ and $b_i = b_{i+h}$ for $i \in \mathbb{Z}_{<0}$. Then for all $i \in \mathbb{Z}$ we have $[b_i] = [bp^i]$. Let c be an integral O-ideal. For each $i \in \mathbb{Z}$ we choose an element $\gamma_i \in b_i c^{-1}$, such that $\gamma_{i+h} = \gamma_i$ for all $i \in \mathbb{Z}$. In the applications we will take γ_i far away from b_i, but for the moment this is not needed.

LEMMA (8.1). *There exists a unit* η *of* A *with* $\eta O = p^h$, *and for each* $i \in \mathbb{Z}$ *there exist* $\delta_i \in K$ *and* $\beta_i \in b_i c^{-1}$, *such that for each* $i \in \mathbb{Z}$ *we have*

(a) $\quad bp^i = \delta_i b_i$;

(b) $\quad \eta\delta_i = \delta_{i+h}, \quad \beta_{i+h} = \beta_i$;

(c) $\quad \beta_i\delta_i \equiv \gamma_i\delta_i - \gamma_{i+1}\delta_{i+1} \bmod bp^i$;

(d) $\quad |\beta_i|_\infty = \min\{|\beta|_\infty \,:\, \beta\delta_i \equiv \gamma_i\delta_i \pm \gamma_{i+1}\delta_{i+1} \bmod bp^i\}$.

PROOF. We choose $\delta_0 \in K$ such that $b = \delta_0 b_0$. By induction on n for $0 < n \le h$ we construct $\delta_n \in K$ and $\beta_{n-1} \in b_{n-1}c^{-1}$, such that (a) holds for $i = n$ and such that (c) and (d) hold for $i = n-1$. First we choose $\delta'_n \in K$ such that $bp^n = \delta'_n b_n$. Then $\gamma_n\delta'_n \in bp^n c^{-1} \subset bp^{n-1}c^{-1}$ and by induction $\gamma_{n-1}\delta_{n-1} \in bp^{n-1}c^{-1}$, hence $\gamma_{n-1}\delta_{n-1} \pm \gamma_n\delta'_n \in bp^{n-1}c^{-1}$. Choose $\beta_{n-1} \in b_{n-1}c^{-1}$ such that

$$\beta_{n-1}\delta_{n-1} \equiv \gamma_{n-1}\delta_{n-1} \pm \gamma_n\delta'_n \bmod bp^{n-1} ;$$

$$|\beta_{n-1}|_\infty = \min\{|\beta|_\infty \,:\, \beta\delta_{n-1} \equiv \gamma_{n-1}\delta_{n-1} \pm \gamma_n\delta'_n \bmod bp^{n-1}\}.$$

If $\beta_{n-1}\delta_{n-1} \equiv \gamma_{n-1}\delta_{n-1} - \gamma_n\delta'_n \bmod bp^{n-1}$ we take $\delta_n = \delta'_n$, otherwise we take $\delta_n = -\delta'_n$. Then (a) holds for $i = n$ and (c) and (d) hold for $i = n-1$.

Define $\eta = \delta_0^{-1}\delta_h$, then $\eta O = p^h$ since $b_0 = b_h$. For $i \in \mathbb{Z}_{>0}$ we define $\delta_{i+h} = \eta\delta_i$ and $\beta_{i+h} = \beta_i$ and for $i \in \mathbb{Z}_{<0}$ we define $\delta_i = \eta^{-1}\delta_{i+h}$ and $\beta_i = \beta_{i+h}$. Then for all $i \in \mathbb{Z}$ the conditions (a), (b), (c) and (d) are satisfied. □

In the remainder of this section we will assume that there exist $r_i \in \mathbb{R}_{>0}$ for $i \in \mathbb{Z}$ such that

(8.2) $$|\beta - \gamma_i|_\infty \geq (1 + r_i)^2 Nb_i \quad \text{for all } \beta \in b_i.$$

Since $\gamma_{i+h} = \gamma_i$ we may suppose that $r_{i+h} = r_i$ for all $i \in \mathbb{Z}$. Let β_i, δ_i and η be as in (8.1). For each $i \in \mathbb{Z}$ we define the polynomial $f_i \in \mathbb{R}[X]$ by

(8.3) $$f_i = \sum_{j=0}^{h-1} |\beta_{i+j}|_\infty^{\frac{1}{2}} (Nb_{i+j})^{-\frac{1}{2}} X^j + r_i(1 - X^h).$$

PROPOSITION (8.4). *Let* $b_i, \gamma_i, \beta_i, \delta_i, r_i$ and η *be as given above, such that (8.1) and (8.2) are satisfied. Let for* $i \in \mathbb{Z}$ *the polynomials* f_i *be given by (8.3). Suppose that for all* $i \in \mathbb{Z}$, *with* $0 \leq i < h$, *we have* $f_i(Np^{\frac{1}{2}}) \leq 0$. *Then* $a = bA$ *is not Euclidean.*

PROOF. Choose $\alpha_h \in bp^h c^{-1}$ such that $\alpha_h \equiv \gamma_h \delta_h \bmod bp^h$. We define inductively

$$\alpha_i = \alpha_{i+1} + \beta_i \delta_i \quad \text{for } i \in \mathbb{Z}_{<h};$$

$$\alpha_i = \alpha_{i-1} - \beta_{i-1}\delta_{i-1} \quad \text{for } i \in \mathbb{Z}_{>h}.$$

From (8.1) we derive that

(8.5) $$\alpha_i \equiv \gamma_i \delta_i \bmod bp^i \quad \text{for all } i \in \mathbb{Z}_{\leq h};$$
$$\eta(\alpha_i - \alpha_{i+1}) = \alpha_{i+h} - \alpha_{i+h+1} \quad \text{for all } i \in \mathbb{Z}.$$

Hence $\alpha = \lim_{i \to -\infty} \alpha_i$ exists in $\mathbb{C}$. For all $n \in \mathbb{Z}$ we have

(8.6) $$\alpha = \alpha_n + \sum_{i=0}^{\infty} (\alpha_{n-i-1} - \alpha_{n-i}) = \alpha_n + \sum_{i=0}^{h-1} (\alpha_{n-i-1} - \alpha_{n-i}) \frac{\eta}{\eta - 1} =$$
$$= \alpha_n + \sum_{i=0}^{h-1} (\alpha_{n+i} - \alpha_{n+i+1})(\eta - 1)^{-1} = (\eta\alpha_n - \alpha_{n+h})(\eta - 1)^{-1}.$$

Combining this with (8.5) and (8.1)(b) gives $\eta\alpha - \alpha = \eta\alpha_0 - \alpha_h \equiv 0 \bmod bp^h$, hence

(8.7) $$\eta\alpha \equiv \alpha \bmod bp^h.$$

By (6.7) it suffices to show that $\alpha \notin \bigcup_{n=0}^{h-1} W_1(bp^n)$. Take $n \in \mathbb{Z}$ with $0 \le n < h$. Then from (8.5) and (8.6) we derive that

$$
\begin{aligned}
(8.8) \qquad \alpha &= \alpha_n + \sum_{i=0}^{h-1} (\alpha_{n+i} - \alpha_{n+i+1})(\eta - 1)^{-1} \\
&\equiv \gamma_n \delta_n + \sum_{i=0}^{h-1} \beta_{n+i}\delta_{n+i}(\eta - 1)^{-1} \bmod bp^n.
\end{aligned}
$$

Take $\beta \in bp^n$. Then from (8.8), (8.2), (8.1)(a) and (8.3) we get

$$
\begin{aligned}
|\beta - \alpha|_\infty &\ge (|\beta - \gamma_n\delta_n|_\infty^{\frac{1}{2}} - \sum_{i=0}^{h-1} |\beta_{n+i}\delta_{n+i}|_\infty^{\frac{1}{2}} |\eta - 1|_\infty^{-\frac{1}{2}})^2 \ge \\
&\ge ((1 + r_n)(Nb_n)^{\frac{1}{2}} |\delta_n|_\infty^{\frac{1}{2}} - \sum_{i=0}^{h-1} |\beta_{n+i}\delta_{n+i}|_\infty^{\frac{1}{2}} (|\eta|_\infty^{\frac{1}{2}} - 1)^{-1})^2 = \\
&= ((1 + r_n)(Nbp^n)^{\frac{1}{2}} - \sum_{i=0}^{h-1} |\beta_{n+i}|_\infty^{\frac{1}{2}} (Nbp^{n+i} b_{n+i}^{-1})^{\frac{1}{2}} (|\eta|_\infty^{\frac{1}{2}} - 1)^{-1})^2 = \\
&= (1 + r_n - \sum_{i=0}^{h-1} |\beta_{n+i}|_\infty^{\frac{1}{2}} (Nb_{n+i})^{-\frac{1}{2}} Np^{i/2} (Np^{h/2} - 1)^{-1})^2 Nbp^n = \\
&= (1 - f_n(Np^{\frac{1}{2}})(Np^{h/2} - 1)^{-1})^2 Nbp^n \ge Nbp^n,
\end{aligned}
$$

hence $\alpha \notin W_1(bp^n)$. □

<u>REMARK (8.9)</u>. In (8.4) the ideal c does not play an important role. Whenever the γ_i are in K, for $0 \le i < h$, there is always an integral $\mathcal{O}$-ideal c for which $\gamma_i \in b_i c^{-1}$. However in the main application (8.10) we choose Nc as small as possible, such that there exists γ_i for which (8.3) holds for certain $r_i > 0$. We do this for the following reason. For given sequences of b_i and γ_i we may choose β_i in a way that only depends on the so called *ray class* of p mod c, cf. [Iy] AP.2 §2.1. We will not prove this in general, but for a special case it will be proven implicitly in (8.10). Hence for rings with a Euclidean ideal class we get an upper bound on Np only depending on the ray class of p mod c. If Nc is small there is only a small number of ray classes mod c and thus the computations for getting the upper bounds remain limited.

§(8.2) Application to rings with small discriminants

In this section we use (8.4) to show that several of the rings listed in tables 7 and 8 do not have a Euclidean ideal class. We apply (8.4) only if the order of $[p]$ in $Cl(\mathcal{O})$ is small, since otherwise there are too many polynomials f_i to be calculated. We only consider the ideals c with $c = 2\mathcal{O}$ or $c | \sqrt{\Delta}\cdot\mathcal{O}$. The latter ideal is the ideal for which the r_i, cf. (8.2), are as large as possible, see the proof of (3.4).

For $\Delta = -23$ we get the largest gain. In table 8 we listed 116 rings with $\Delta = -23$ for which the existence of a Euclidean ideal class is still unsettled. We will use (8.4) to reduce this number to 51.

Assume $\Delta = -23$. We write $\omega = \frac{1}{2}(1+\sqrt{-23})$, then $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega$. We will apply (8.4) with $c = \mathcal{O}\cdot\sqrt{-23}$. Let $q = \mathbb{Z}\cdot 2 + \mathbb{Z}\cdot\omega$ and $r = \mathbb{Z}\cdot 2 + \mathbb{Z}\cdot(\omega - 1)$ be the two integral ideals of norm 2 of $\mathcal{O}$. Then $\mathcal{O}$, q and r are representatives of the ideal classes of $\mathcal{O}$. In particular we may choose $b_i \in \{c, qc, rc\}$. Figure 11 shows, for each $a \in \{\mathcal{O}, q, r\}$, the representatives of $a \bmod ac$ that lie in the fundamental hexagon belonging to ac. In the case that $a = \mathcal{O}$ each $\alpha \in a$ is $\equiv n \bmod ac$ for a unique $n \in \mathbb{Z}$ with $|n| \le 11$. In the case that $a = q$ or $a = r$ each $\alpha \in a$ is $\equiv n \bmod ac$ for a unique $n \in 2\mathbb{Z}$ with $|n| \le 22$. In figure 11 we find these numbers n. Also the circle $\{x \in \mathbb{C} : |x|_\infty = Nac\}$ is drawn. The minimal values of $|\beta|_\infty N(ac)^{-1}$ for β in a given residue class of $a \bmod ac$ are listed in table 13. From this table we derive that in order to satisfy (8.2) we must take $\gamma_i \equiv \pm 5, \pm 6, \pm 7 \bmod b_i$ if $b_i = c$ and $\gamma_i \equiv \pm 18 \bmod b_i$ if $b_i = qc$ or $b_i = rc$.

THEOREM (8.10). *Suppose that* $K = \mathbb{Q}(\sqrt{-23})$ *and that* $A = A_S$ *has a Euclidean ideal class, with* $S = \{p, \infty\}$.

(a) *If* $Np \equiv 1 \bmod 23$ *then* $Np \le 1427$;

(b) *If* $Np \equiv 2 \bmod 23$ *then* $Np \le 1129$;

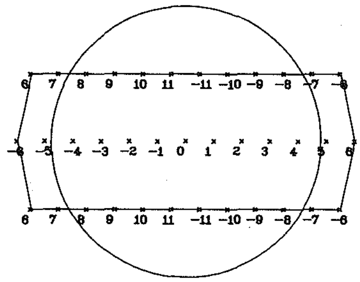
(c) *If* $Np \equiv 3 \bmod 23$ *then* $Np \le 1153$;

(d) *If* $Np \equiv 4 \bmod 23$ *then* $Np \le 487$;

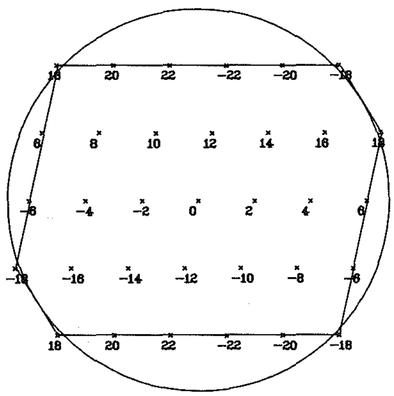
(e) *If* $Np \equiv 6 \bmod 23$ *then* $Np \le 1409$;

(f) *If* $Np \equiv 8 \bmod 23$ *then* $Np \le 491$;

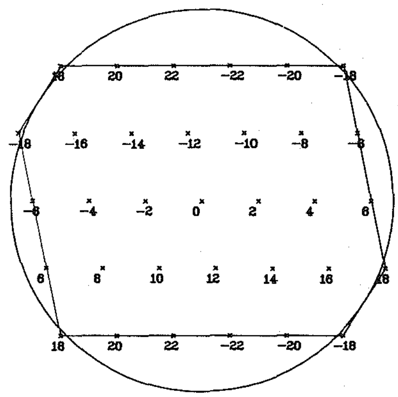
(g) *If* $Np \equiv 9 \bmod 23$ *then* $Np \le 331$;



0 mod c



q mod qc



r mod rc

fig. 11

<u>TABLE 13</u>. Minimal value of $23|\beta|_\infty N(ac)^{-1}$ for $\beta \in a$, cf. fig.11.

$a = 0$		$a = q$ or $a = r$	
β mod c	$\lvert\beta\rvert_\infty$	β mod ac	$\frac{1}{2}\lvert\beta\rvert_\infty$
0	0	0	0
±1	1	±2	2
±2	4	±4	8
±3	9	±6	18
±4	16	±8	9
±5	25	±10	4
±6	36	±12	3
±7	26	±14	6
±8	18	±16	13
±9	12	±18	24
±10	8	±20	16
±11	6	±22	12

(h) *If* $Np \equiv -11 \bmod 23$ *then* $Np \leq 587$;

(i) *If* $Np \equiv -10 \bmod 23$ *then* $Np \leq 151$;

(j) *If* $Np \equiv -7 \bmod 23$ *then* $Np \leq 131$;

(k) *If* $Np \equiv -5 \bmod 23$ *then* $Np \leq 179$.

PROOF. We use (8.4) with $c = \mathcal{O}\cdot\sqrt{-23}$. In all cases we take $h = h(\mathcal{O}) = 3$. Suppose that p is an $\mathcal{O}$-ideal such that $A = A_{\{p,\infty\}}$ has a Euclidean ideal class. Notice that $h(A) = 1$, hence A is a Euclidean ring. Let q and r be as above. Because the conjugate of p gives rise to an isomorphic ring we may assume that $[p] = [q]$. For $i \in \mathbb{Z}$ we take $b_i = c$ if $i \equiv 0 \bmod 3$; $b_i = qc$ if $i \equiv 1 \bmod 3$ and $b_i = rc$ if $i \equiv 2 \bmod 3$. Also we take $b = c$. Then for each $i \in \mathbb{Z}$ we have $[bp^i] = [b_i]$.

Let $\pi \in p$ be such that $p = \frac{\pi}{2}q$, then $\pi\mathcal{O} = pr$. Because $q^3 = \mathcal{O}\cdot(2-\omega)$ we have $p^3 = \mathcal{O}\cdot(\frac{2-\omega}{8}\pi^3)$. Because $2Np = |\pi|_\infty \equiv \pi^2 \bmod c$, we find that $\pm\pi \bmod c$ only depends on $Np \bmod 23$. In table 14 we find for each value of $Np \bmod 23$ a choice of $\gamma_i \in b_i c^{-1}$, for $i = 0, 1, 2$, such that (8.2) is satisfied for some $r_i > 0$. Suppose that we have δ_i, β_i and η such that (8.1)(a), (b), (c) and (d) are satisfied. Then there exist $\varepsilon_i \in \{\pm 1\}$ such that

(8.11)
$$\delta_{3i} = \varepsilon_{3i}\left(\frac{2-\omega}{8}\pi^3\right)^i ;$$

$$\delta_{3i+1} = \varepsilon_{3i+1}\,\frac{\pi}{2}\left(\frac{2-\omega}{8}\pi^3\right)^i ;$$

$$\delta_{3i+2} = \varepsilon_{3i+2}\,\pi^{-1}\left(\frac{2-\omega}{8}\pi^3\right)^{i+1}, \quad \text{for all } i \in \mathbb{Z} ;$$

$$\eta = \varepsilon_0\varepsilon_3\,\frac{2-\omega}{8}\pi^3 ;$$

$$\beta_0 \equiv (\gamma_0 - \varepsilon_0\varepsilon_1\gamma_1\,\tfrac{\pi}{2}) \bmod c ;$$

$$\beta_1 \equiv (\gamma_1 - \varepsilon_1\varepsilon_2\gamma_2\,\tfrac{(2-\omega)\pi}{4}) \bmod c ;$$

$$\beta_2 \equiv (\gamma_2 - \varepsilon_2\varepsilon_3\gamma_0\,\pi) \bmod c .$$

From table 13 we see that the minimal value of $|\beta|_\infty$ for β in a residue class of $a \bmod ac$ uniquely determines the residue class up to sign. Since

$\gamma_i \not\equiv 0 \bmod c$ and $\pi \not\equiv 0 \bmod c$, we find that the β_i and also the $\varepsilon_i\varepsilon_{i+1}$ are uniquely determined by (8.1)(c) and (8.1)(d). Hence the only freedom of choice in (8.11) consists of changing the sign of all δ_i and ε_i simultaneously. In particular we find that the β_i are the same for two primes p with the same norm mod 23. This justifies the fact that we treat those primes together.

The rest of the proof can be derived from table 14. For the various possibilities of Np mod 23 we find the value of $\pm\pi \bmod c$ in the second column. For $i = 0, 1, 2$ we find in the fourth column the value of the $\gamma_i \bmod b_i$ that we have chosen. They are chosen to give the best results. In the fifth column we find the value of $23(1+r_i^2)$, which is an integer that can be derived from table 13. In the sixth column we find the values m_i defined by $m_0 \equiv \varepsilon_0\varepsilon_1 \frac{\pi}{2} \bmod c$, $m_1 \equiv \varepsilon_1\varepsilon_2 \frac{(2-\omega)\pi}{4} \bmod c$ and $m_2 \equiv$ $\equiv \varepsilon_2\varepsilon_3\, \pi \bmod c$. They are used in the computation of the β_i. The residue classes of $\beta_i \bmod b_i$ are given in the seventh column. Using table 13 we derive from this the value of $23|\beta_i|_\infty Nb_i^{-1}$, which is listed in the eighth column. Finally in the last column we find the minimal value B_i such that $Np \geq B_i$ implies that $f_i(Np^{\frac{1}{2}}) \leq 0$. The largest of these values is underlined, because by (8.5) we know that for a ring with a Euclidean ideal class Np must be less than this bound. □

Notice that, since $r_i > 0$, there are only six possibilities of $\gamma_0 \bmod b_0$, viz. ±5, ±6, ±7. For $\gamma_1 \bmod b_1$ and $\gamma_2 \bmod b_2$ there are only the possibilities ±18. Changing the sign of the γ_i only results in changing the sign of the β_i and the δ_i. This will give the same bound on Np.

TABLE 14. Bounds on $N\mathfrak{p}$ for subrings in $\mathbb{Q}(\sqrt{-23})$, with $\#S = 2$, with a Euclidean ideal class.

$N\mathfrak{p}$ mod 23	π mod $\mathfrak{c}$	i	γ_i	$23(1+r_i)^2$	m_i	β_i	$23\lvert\beta_i\rvert_\infty N\mathfrak{b}_i^{-1}$	B_i
1	±5	0	5	25	−9	4	16	314.2
		1	18	24	22	0	0	1573.1
		2	18	24	18	16	13	44.2
2	±2	0	5	25	1	0	0	250.1
		1	18	24	−18	16	13	35.2
		2	18	24	−2	8	9	1223.6
3	±11	0	7	26	−17	0	0	65.4
		1	18	24	16	−16	13	26.4
		2	18	24	12	10	4	1223.1
4	±10	0	5	25	5	3	9	174.3
		1	18	24	2	8	9	894.8
		2	18	24	−10	14	6	904.8
6	±9	0	7	26	−7	−4	16	50.8
		1	18	24	−12	−14	6	1538.5
		2	18	24	−14	12	3	640.5
8	±4	0	7	26	2	−3	9	11.4
		1	18	24	10	14	6	847.7
		2	18	24	4	0	0	620.9
9	±8	0	5	25	−4	2	4	92.6
		1	18	24	20	10	4	410.8
		2	18	24	8	12	3	415.5
−11	±1	0	7	26	11	−2	4	40.1
		1	18	24	−14	−4	8	405.7
		2	18	24	−22	2	2	791.3
−10	±7	0	6	36	−8	0	0	6.9
		1	18	24	−6	2	2	26.6
		2	18	24	−16	14	6	191.6
−7	±3	0	5	25	10	1	1	110.5
		1	18	24	4	−2	2	132.1
		2	18	24	−20	10	4	209.1
−5	±6	0	7	26	−3	−1	1	77.2
		1	18	24	−8	12	3	140.0
		2	18	24	6	14	6	303.8

TABLE 15. The subring A_S of $\mathbb{Q}(\sqrt{-23})$, with $S = \{p,\infty\}$ has a Euclidean subring only if Np is in the list below.

Np mod 23	Np
1	47, 139, 277, 461, 967, 1013, 1289, 1381, 1427
2	2, 71, 163, 439, 577, 761, 1129
3	3, 233, 509, 601, 647, 739, 1061, 1153
4	73, 257, 349, 487
6	29, 397, 443, 673, 811, 857, 1087, 1409
8	31, 353, 491
9	193, 239, 331
-11	127, 311, 541, 587
-10	13, 151
-7	131
-5	41, 179

Table 15 lists those primes of $\mathbb{Q}(\sqrt{-23})$ for which the existence of a Euclidean ideal class remains unsettled by (8.10). This list contains 51 rings, which is 65 less than the list in table 8.

For discriminants other than -23 we may also use (8.4). For 18 rings we disproved the existence of a Euclidean ideal class in this way. They are listed in table 16. The values of $|\beta_i|_\infty Nb_i^{-1}$ and $(1+r_i)^2$ are rational numbers with denominator Nc. We only list their numerators. Instead of the δ_i the values of $\delta_{i+1}\delta_i^{-1}$ are listed. These latter values are what we need for the computation of the β_i, cf. (8.1)(c), (d). If h is the order of $[p]$ in $Cl(O)$ we may compute the fundamental unit η by $\eta = \prod_{i=0}^{h-1} \delta_{i+1}\delta_i^{-1}$. If we take $b = b_0$ and $\delta_0 = 1$ we find that $\delta_i = \prod_{j=0}^{i-1} \delta_{j+1}\delta_j^{-1}$. We have chosen the b_i in such a way that $\gamma_i \in O = \mathbb{Z}[\omega]$, where $\omega = \frac{1}{2}\sqrt{\Delta}$ if Δ is even and $\omega = \frac{1}{2}(1+\sqrt{\Delta})$ if Δ is odd.

After this section there are still 157 rings to be investigated.

TABLE 16. Rings with no Euclidean ideal class.

Δ	Np	h	Nc	i	b_i	$\delta_{i+1}\delta_i^{-1}$	γ_i	$(1+r_i)^2 Nc$	β_i	$\lvert\beta_i\rvert_\infty Nb_i^{-1}c$	$f_i(Np^{\frac{1}{2}})$
-24	79	1	4	0	$\mathbb{Z}\cdot 4+\mathbb{Z}\cdot 2\omega$	$5+3\omega$	$2+\omega$	5	2	2	-0.22
-24	101	2	24	0	$\mathbb{Z}\cdot 12+\mathbb{Z}\cdot 12\omega$	$\frac{14+\omega}{2}$	$6+5\omega$	31	5ω	25	-8.04
				1	$\mathbb{Z}\cdot 24+\mathbb{Z}\cdot 12\omega$	$14+\omega$	$12+6\omega$	30	$6+2\omega$	5	-1.09
-31	41	3	31	0	$\mathbb{Z}\cdot 31+\mathbb{Z}\cdot 31\omega$	$\frac{5-3\omega}{2}$	$8-16\omega$	64	$-3+6\omega$	9	-91.25
				1	$\mathbb{Z}\cdot 62+\mathbb{Z}\cdot 31\omega$	$\frac{-12-\omega}{2}$	$24+14\omega$	40	$-2+4\omega$	2	-9.95
				2	$\mathbb{Z}\cdot 62+\mathbb{Z}\cdot 31(1-\omega)$	$-5+3\omega$	$38-14\omega$	40	$4-8\omega$	8	-21.18
-31	59	3	31	0	$\mathbb{Z}\cdot 31+\mathbb{Z}\cdot 31\omega$	$\frac{11-\omega}{2}$	$7-14\omega$	49	$5-10\omega$	25	-68.87
				1	$\mathbb{Z}\cdot 62+\mathbb{Z}\cdot 31\omega$	$\frac{4+5\omega}{2}$	$24+14\omega$	40	$-22+13\omega$	25	-2.42
				2	$\mathbb{Z}\cdot 62+\mathbb{Z}\cdot 31(1-\omega)$	$11-\omega$	$38-14\omega$	40	$11+9\omega$	14	-0.91
-31	71	3	31	0	$\mathbb{Z}\cdot 31+\mathbb{Z}\cdot 31\omega$	$\frac{7+3\omega}{2}$	$8-16\omega$	64	$-1+2\omega$	1	-223.60
				1	$\mathbb{Z}\cdot 62+\mathbb{Z}\cdot 31\omega$	$\frac{12-5\omega}{2}$	$24+14\omega$	40	$14+3\omega$	5	-64.02
				2	$\mathbb{Z}\cdot 62+\mathbb{Z}\cdot 31(1-\omega)$	$-7-3\omega$	$38-14\omega$	40	$-18+5\omega$	7	-50.68
-35	13	2	4	0	$\mathbb{Z}\cdot 2+\mathbb{Z}\cdot 2\omega$	$\frac{5+\omega}{3}$	$1+\omega$	11	1	1	-7.40
				1	$\mathbb{Z}\cdot 6+\mathbb{Z}\cdot 2\omega$	$-3+2\omega$	$3+\omega$	7	0	0	-2.07

TABLE 16. Continued.

Δ	Np	h	Nc	i	b_i	$\delta_{i+1}\delta_i^{-1}$	γ_i	$(1+r_i)^2 Nc$	β_i	$\lvert\beta_i\rvert_\infty Nb_i^{-1}c$	$f_i(Np^{\frac{1}{2}})$
-35	17	2	4	0	$\mathbb{Z}\cdot 2+\mathbb{Z}\cdot 2\omega$	$\frac{7-\omega}{3}$	$1+\omega$	11	1	1	-10.03
				1	$\mathbb{Z}\cdot 6+Z\cdot 2\omega$	$3+2\omega$	$3+\omega$	7	0	0	-3.10
-35	47	2	4	0	$\mathbb{Z}\cdot 2+\mathbb{Z}\cdot 2\omega$	$\frac{11+\omega}{3}$	$1+\omega$	11	1	1	-29.78
				1	$\mathbb{Z}\cdot 6+\mathbb{Z}\cdot 2\omega$	$3-4\omega$	$3+\omega$	7	0	0	-11.42
-35	73	2	4	0	$\mathbb{Z}\cdot 2+\mathbb{Z}\cdot 2\omega$	$\frac{14+\omega}{3}$	$1+\omega$	11	ω	9	-38.50
				1	$\mathbb{Z}\cdot 6+\mathbb{Z}\cdot 2\omega$	$3-5\omega$	$3+\omega$	7	3	3	-9.57
-35	83	2	4	0	$\mathbb{Z}\cdot 2+\mathbb{Z}\cdot 2\omega$	$\frac{16-\omega}{3}$	$1+\omega$	11	ω	9	-44.59
				1	$\mathbb{Z}\cdot 6+\mathbb{Z}\cdot 2\omega$	$3+5\omega$	$3+\omega$	7	3	3	-11.94
-39	41	4	39	0	$\mathbb{Z}\cdot 39+\mathbb{Z}\cdot 39\omega$	$\frac{-9+\omega}{2}$	$13+13\omega$	52	$-3+6\omega$	9	-103.50
				1	$\mathbb{Z}\cdot 78+\mathbb{Z}\cdot 39\omega$	$\frac{4-5\omega}{3}$	$10-20\omega$	50	$4-8\omega$	8	-71.76
				2	$\mathbb{Z}\cdot 117+\mathbb{Z}\cdot 39(1+\omega)$	$\frac{4-5\omega}{2}$	$12-24\omega$	48	$9-18\omega$	27	-41.46
				3	$\mathbb{Z}\cdot 78+\mathbb{Z}\cdot 39(1-\omega)$	$-9+\omega$	$30+18\omega$	60	$4-8\omega$	8	-163.25

TABLE 16. Continued.

Δ	Np	h	Nc	i	b_i	$\delta_{i+1}\delta_i^{-1}$	γ_i	$(1+r_i)^2 Nc$	β_i	$\lvert\beta_i\rvert_\infty Nb_i^{-1}c$	$f_i(Np^{\frac{1}{2}})$
-39	47	4	39	0	$\mathbb{Z}\cdot 39 + \mathbb{Z}\cdot 39\omega$	$\frac{-1-3\omega}{2}$	$9 - 18\omega$	81	$2 - 4\omega$	4	-727.22
				1	$\mathbb{Z}\cdot 78 + \mathbb{Z}\cdot 39\omega$	$\frac{-16-\omega}{3}$	$10-20\omega$	50	$-2+4\omega$	2	-152.92
				2	$\mathbb{Z}\cdot 117 + \mathbb{Z}\cdot 39(1+\omega)$	$\frac{-16-\omega}{2}$	$12-24\omega$	48	$6-12\omega$	12	-148.32
				3	$\mathbb{Z}\cdot 78 + \mathbb{Z}\cdot 39(1-\omega)$	$-1-3\omega$	$30+18\omega$	60	$-6 + 12\omega$	18	-338.44
-39	59	4	39	0	$\mathbb{Z}\cdot 39 + \mathbb{Z}\cdot 39\omega$	$\frac{7 - 3\omega}{2}$	$10+19\omega$	100	0	0	-1762.21
				1	$\mathbb{Z}\cdot 78 + \mathbb{Z}\cdot 39\omega$	$\frac{-8-5\omega}{3}$	$32+14\omega$	44	$-4+8\omega$	8	-173.36
				2	$\mathbb{Z}\cdot 117 + \mathbb{Z}\cdot 39(1+\omega)$	$\frac{8 + 5\omega}{2}$	$12-24\omega$	48	$-21 + 3\omega$	4	-169.92
				3	$\mathbb{Z}\cdot 78 + \mathbb{Z}\cdot 39(1-\omega)$	$7 - 3\omega$	$10-20\omega$	50	$-6 + 12\omega$	18	-287.79
-39	71	4	39	0	$\mathbb{Z}\cdot 39 + \mathbb{Z}\cdot 39\omega$	$\frac{-11-\omega}{2}$	$7 - 14\omega$	49	$4 - 8\omega$	16	-61.04
				1	$\mathbb{Z}\cdot 78 + \mathbb{Z}\cdot 39\omega$	$\frac{-16 + 5\omega}{3}$	$30-21\omega$	60	$6-12\omega$	18	-763.17
				2	$\mathbb{Z}\cdot 117 + \mathbb{Z}\cdot 39(1+\omega)$	$\frac{16-5\omega}{2}$	$12-24\omega$	48	0	0	-91.83
				3	$\mathbb{Z}\cdot 78 + \mathbb{Z}\cdot 39(1-\omega)$	$-11-\omega$	$9 + 21\omega$	60	$-8 + 16\omega$	32	-1156.81

TABLE 16. Continued.

Δ	Np	h	Nc	i	b_i	$\delta_{i+1}\delta_i^{-1}$	γ_i	$(1+r_i)^2 Nc$	β_i	$\lvert\beta_i\rvert_\infty Nb_i^{-1}c$	$f_i(Np^{\frac{1}{2}})$
-39	83	4	39	0	$\mathbb{Z}\cdot 39+\mathbb{Z}\cdot 39\omega$	$\frac{13-\omega}{2}$	$7-14\omega$	49	$2-4\omega$	4	-783.87
				1	$\mathbb{Z}\cdot 78+\mathbb{Z}\ 39\omega$	$\frac{8-7\omega}{3}$	$32+14\omega$	44	$14+11\omega$	20	-180.73
				2	$\mathbb{Z}\cdot 117+\mathbb{Z}\cdot 39(1+\omega)$	$\frac{-8+7\omega}{2}$	$12-24\omega$	48	$15+9\omega$	10	-184.96
				3	$\mathbb{Z}\cdot 78+\mathbb{Z}\cdot 39(1-\omega)$	$-13+\omega$	$10-20\omega$	50	0	0	-465.78
-39	89	4	39	0	$\mathbb{Z}\cdot 39+\mathbb{Z}\cdot 39\omega$	$\frac{-11+3\omega}{2}$	$7-14\omega$	49	$3-6\omega$	9	-674.62
				1	$\mathbb{Z}\cdot 78+\mathbb{Z}\cdot 39\omega$	$\frac{4+7\omega}{3}$	$32+14\omega$	44	$2-4\omega$	2	-59.11
				2	$\mathbb{Z}\cdot 117+\mathbb{Z}\cdot 39(1+\omega)$	$\frac{-4-7\omega}{2}$	$12-24\omega$	48	$-9-21\omega$	40	-630.41
				3	$\mathbb{Z}\cdot 78+\mathbb{Z}\cdot 39(1-\omega)$	$11-3\omega$	$10-20\omega$	50	$2-4\omega$	2	-172.40
-51	23	2	17	0	$\mathbb{Z}\cdot 17+\mathbb{Z}\cdot 17\omega$	$\frac{8-\omega}{3}$	$4-8\omega$	48	0	0	-13.80
				1	$\mathbb{Z}\cdot 51+\mathbb{Z}\cdot 17(1+\omega)$	$-8+\omega$	$22+7\omega$	25	$1-2\omega$	1	-4.44
-55	43	4	11	0	$\mathbb{Z}\cdot 11+\mathbb{Z}\cdot 11\omega$	$\frac{-9+\omega}{2}$	$4+3\omega$	14	$5+\omega$	4	-11.29
				1	$\mathbb{Z}\cdot 22+\mathbb{Z}\cdot 11\omega$	$\frac{-2+5\omega}{4}$	$8-5\omega$	17	0	0	-245.03
				2	$\mathbb{Z}\cdot 44+\mathbb{Z}\cdot 11(1+\omega)$	$9-\omega$	$20+4\omega$	16	0	0	-349.61
				3	$\mathbb{Z}\cdot 22+\mathbb{Z}\cdot 11(1-\omega)$	$-9+\omega$	$3+5\omega$	17	$-7+3\omega$	7	-444.61

§(8.3) Primes of norm 2

In this section we assume that $Np = 2$ and $\Delta \equiv 1 \bmod 8$, i.e. 2 is splitting in $K/\mathbb{Q}$. If each reduced quadratic form (a,b,c) of discriminant Δ satisfies $a < \frac{9|\Delta|}{512}$ we see from (6.14) that A has no Euclidean ideal class. This result was derived by taking $k = k' = 4$ in (6.8). In this section we will improve upon (6.8) for the case that $Np = k = k' = 2$. This will lead to a better upper bound for $|\Delta|$ for rings with a Euclidean ideal class.

Let b be an $\mathcal{O}$-ideal and let $a = b\mathrm{A}$ be the corresponding A-ideal. For $n \in \mathbb{Z}$ let (a_n, b_n, c_n) be the reduced quadratic form corresponding to bp^n. If a_n, b_n and c_n, for all $n \in \mathbb{Z}$, satisfy certain restrictions, stated in (8.16) we may construct a sequence $(y_n)_{n \in \mathbb{Z}_{\geq 0}}$ in $\mathbb{C}$ such that for some $\varepsilon \in \mathbb{R}_{>0}$ and for all $n \in \mathbb{Z}_{\geq 0}$ we have

$$(8.12) \qquad |\gamma - y_n|_\infty > (1+\varepsilon)Nbp^r \quad \text{for all } r \in \mathbb{Z} \text{ with } 0 \leq r \leq n \text{ and all } \gamma \in bp^r.$$

This enables us to conclude that a is not Euclidean, by (6.6). We will only consider $\Delta \leq -23$. So for ε small enough the existence of y_0 is trivial. For the induction step we need some lemmas..

LEMMA (8.13). *Let* $m \in \mathbb{Z}_{>0}$ *and* $\varepsilon \in \mathbb{R}_{>0}$. *Suppose that for each* $n \in \mathbb{Z}$ *with* $0 \leq n < m$ *there exists* $y_n \in \mathbb{C}$ *such that (8.12) holds, and that* $a_m(1+\varepsilon) < \frac{|\Delta|}{64}$. *Then there exists* $y_m \in \mathbb{C}$ *such that (8.12) holds for* $n = m$.

PROOF. Essentially this will be the proof of (6.8). Choose $\alpha, \beta \in bp^m$ such that $|\alpha|_\infty = a_m Nbp^m$ and $\beta = (b_m + \sqrt{\Delta})\alpha/2a_m$. Let k be the least integer ≥ 0 such that $bp^k = \mathbb{Z}\alpha\cdot 2^{k-m} + \mathbb{Z}\beta$; then $k \leq m$. If $k = 0$ we take $y = y_0 = \frac{1}{2}\beta$. If $k > 0$, let first $y = y_{k-1} \in \mathbb{C}$ be such that (8.12) holds for $n = k-1$; next shift y by an element of bp^{k-1} in order to achieve that $\sqrt{|\Delta|}/8a_m \leq \mathrm{Im}\,\frac{y}{\alpha} \leq 3\sqrt{|\Delta|}/8a_m$, cf. fig. 12; this does not affect (8.12). We show that y satisfies (8.12) for $n = m$.

Take $r \in \mathbb{Z}$ with $0 \leq r \leq m$ and take $\gamma \in bp^r$. If $r < k$ we have (8.12) by assumption. If $k \leq r \leq m$ we have

$$|y-\gamma|_\infty \geq \frac{|\Delta|}{64a_m^2}|\alpha|_\infty = \frac{|\Delta|}{64a_m}Nbp^m > (1+\varepsilon)Nbp^m \geq (1+\varepsilon)Nbp^r. \qquad \square$$

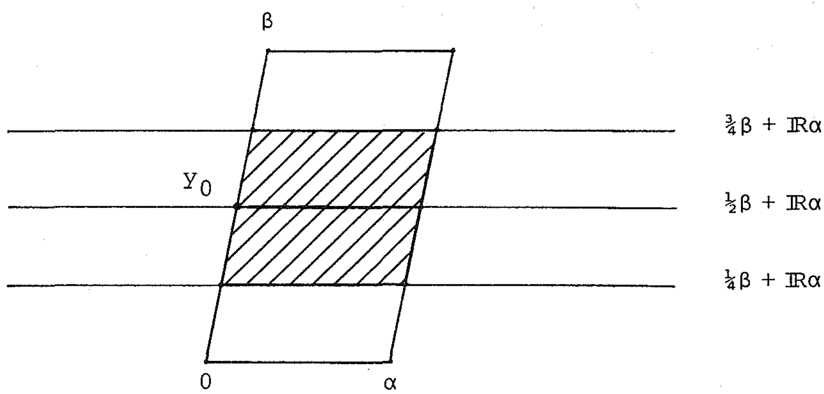


fig. 12

LEMMA (8.14). *Let* $m \in \mathbb{Z}_{>0}$ *and* $\varepsilon \in \mathbb{R}_{>0}$. *Suppose that for each* $n \in \mathbb{Z}$ *with* $0 \le n < m$ *there exists* $y_n \in \mathbb{C}$ *such that (8.12) holds. Let* $e, f \in \mathbb{Z}$ *be such that there is a basis* α, β *of* bp^m *with*

$$|\alpha|_\infty = eNbp^m ;$$

$$\beta = \frac{f + \sqrt{\Delta}}{2e}\alpha \quad ;$$

$$bp^{m-1} = \mathbb{Z}\cdot\tfrac{1}{2}\alpha + \mathbb{Z}\beta.$$

If $8 \le e < \frac{|\Delta|}{32(1+2\varepsilon)}$ *then there exists* $y_m \in \mathbb{C}$ *such that (8.12) holds for* $n = m$.

PROOF. Let k be the least integer ≥ 0 such that $bp^k = \mathbb{Z}\alpha\cdot 2^{k-m} + \mathbb{Z}\beta$; then $k < m$. If $k = 0$ we take $y = y_0 = (\frac{1}{2} + \frac{\sqrt{\Delta}}{4e})\alpha$. If $k > 0$ let first $y = y_{k-1}$ be such that (8.12) holds for $n = k - 1$; next shift y by an element of bp^{k-1} in order to achieve that

$$\frac{\sqrt{|\Delta|}}{8e} \le \left|\mathrm{Im}\,\frac{y}{\alpha}\right| \le \frac{\sqrt{|\Delta|}}{4e}.$$

Finally shift y by a suitable integral multiple of $\frac{\alpha}{2} \in bp^{k-1}$ in order to achieve that also

$$\frac{1}{4} \le \mathrm{Re}\,\frac{y}{\alpha} \le \frac{3}{4},$$

cf. fig. 13. We show that y satisfies (8.12) for $n = m$.

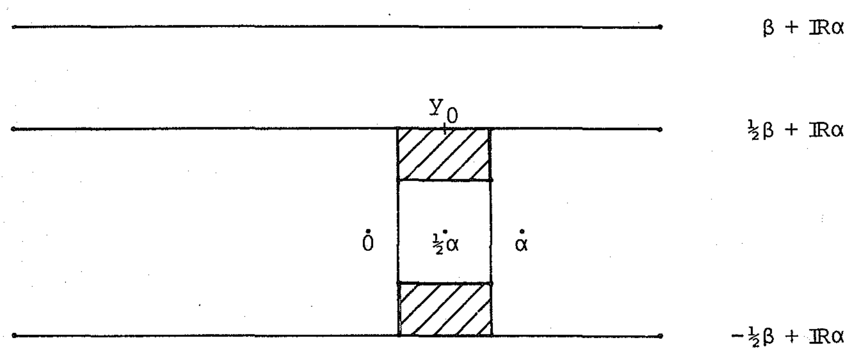


fig. 13

Take $r \in \mathbb{Z}$ with $0 \le r \le m$ and take $\gamma \in ap^r$. If $r < k$ we have (8.12) by assumption. If $k \le r < m$ we have

$$|y-\gamma|_\infty \ge \frac{|\Delta|}{64e^2}\,|\alpha|_\infty = \frac{|\Delta|}{64e}\,Nbp^m > \frac{1+2\varepsilon}{2}\,Nbp^m > (1+\varepsilon)Nbp^r.$$

Let finally $r = m$. Then

$$|y-\gamma|_\infty \ge \min\left\{\frac{|\Delta|}{16e^2}\,|\alpha|_\infty,\ \left(\frac{|\Delta|}{64e^2}+\frac{1}{16}\right)|\alpha|_\infty\right\}.$$

Now

$$\frac{|\Delta|}{16e^2}\,|\alpha|_\infty = \frac{|\Delta|}{16e}\,Nbp^m > 2(1+2\varepsilon)Nbp^m > (1+\varepsilon)Nbp^m,$$

and

$$\left(\frac{|\Delta|}{64e^2} + \frac{1}{16}\right)|\alpha|_\infty = \left(\frac{|\Delta|}{64e} + \frac{e}{16}\right)Nbp^m >$$

$$> \left(\frac{1+2\varepsilon}{2} + \frac{1}{2}\right)Nbp^m = (1+\varepsilon)Nbp^m,$$

hence also $|y-\gamma|_\infty > (1+\varepsilon)Nbp^m$. □

LEMMA (8.15). *Let* $m \in \mathbb{Z}_{>0}$ *and* $\varepsilon \in \mathbb{R}$ *with* $0 < \varepsilon < \frac{1}{16}$. *Suppose that for each* $n \in \mathbb{Z}$ *with* $0 \le n < m$ *there exists* $y_n \in \mathbb{C}$ *such that (8.12) holds. Let* $e, f \in \mathbb{Z}$ *be such that there is a basis* α, β *of* bp^m *with*

$$|\alpha|_\infty = eNbp^m,$$

$$\beta = \frac{f+\sqrt{\Delta}}{2e}\alpha \quad \textit{and}$$

$$bp^{m-1} = \mathbb{Z}\cdot\tfrac{1}{2}\alpha + \mathbb{Z}\beta\,.$$

If $16 \le e < \frac{|\Delta|}{16(1+\varepsilon)}$ *then there exists* $y_m \in \mathbb{C}$ *such that (8.12) holds for* $n = m$.

PROOF. First we show that when $4|e$ we necessarily have $ap^{m-2} = \mathbb{Z}\cdot\frac{1}{4}\alpha + \mathbb{Z}\beta$. The other two possibilities are $ap^{m-2} = \mathbb{Z}\cdot\frac{1}{2}\alpha + \mathbb{Z}\cdot\frac{1}{2}\beta$ and $ap^{m-2} = \mathbb{Z}\cdot\frac{1}{2}\alpha + \mathbb{Z}\cdot(\frac{1}{4}\alpha + \frac{1}{2}\beta)$. In the first case we get $p^2 = 2\mathcal{O}$, a contradiction. In the latter case we have $|\frac{1}{4}\alpha + \frac{1}{2}\beta|_\infty = (\frac{1}{16}e + \frac{1}{8}f + \frac{1}{4}g)Nbp^m = (\frac{1}{4}e + \frac{1}{2}f + g)Nbp^{m-2}$, where g is the integer such that $|\beta|_\infty = gNbp^m$. Because $f^2 - 4eg = \Delta$ we have $f \equiv 1 \bmod 2$, also we have $\frac{1}{4}e + \frac{1}{2}f + g \in \mathbb{Z}$ hence $e \equiv 2 \bmod 4$, a contradiction as well.

If $e = 16$ and $m = 1$ we take $y = y_1 = (\frac{1}{4} + \frac{\sqrt{\Delta}}{4e})\alpha$. In the other cases we take $y = y_{m-1} \in \mathbb{C}$ such that (8.12) holds for $n = m-1$. Shifting y by a suitable element of bp^{m-1} we may suppose that

$$\left|\operatorname{Im}\frac{y}{\alpha}\right| \le \frac{\sqrt{|\Delta|}}{4e}$$

and

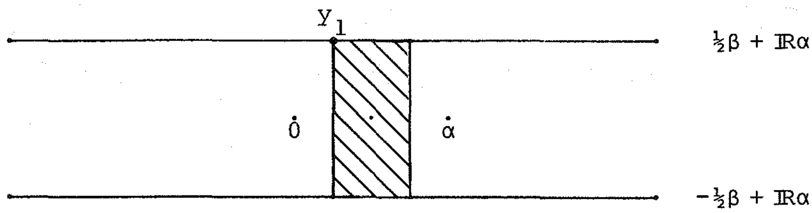


fig. 14

$$\frac{1}{4} \le \mathrm{Re}\,\frac{y}{\alpha} \le \frac{3}{4},$$

cf. fig. 14. We show that y satisfies (8.12) for $n = m$. If $e \neq 16$ or $m \neq 1$ we only have to check (8.12) for $r = m$. If $e = 16$ and $m = 1$ we also have to check (8.12) for $r = m - 1 = 0$.

First assume that $e \neq 16$. Then $e \ge 17 > 16(1+\varepsilon)$. Take $\gamma \in bp^m$, then

$$|y-\gamma|_\infty \ge \min\{\frac{|\Delta|}{16e^2}\,|\alpha|_\infty,\ \frac{1}{16}\,|\alpha|_\infty\}.$$

Now

$$\frac{|\Delta|}{16e^2}\,|\alpha|_\infty = \frac{|\Delta|}{16e}\,Nbp^m > (1+\varepsilon)Nbp^m$$

and

$$\frac{1}{16}\,|\alpha|_\infty = \frac{e}{16}\,Nbp^m > (1+\varepsilon)Nbp^m,$$

by assumption, hence also $|y-\gamma|_\infty > (1+\varepsilon)Nbp^m$.

If $e = 16$ and $m = 1$ we have for all $\gamma \in b$ that

$$|y-\gamma|_\infty \geq \frac{|\Delta|}{16e^2}|\alpha|_\infty > (1+\varepsilon)Nbp.$$

Since $b \supset bp$ this finishes the proof for this case.

Finally suppose that $e = 16$ and $m \geq 2$. Above we have seen that $\frac{1}{4}\alpha \in bp^{m-2}$, hence

$$|y-\tfrac{1}{4}\alpha|_\infty > (1+\varepsilon)Nbp^{m-2} > \tfrac{1}{4}Nbp^m,$$

by assumption. Similarly we have $|y-\frac{3}{4}\alpha|_\infty > \frac{1}{4}Nbp^m$. This shows that $|y|_\infty > |\frac{1}{4}\alpha|_\infty + \frac{1}{4}Nbp^m = \frac{5}{4}Nbp^m$ and similarly $|y-\alpha|_\infty > \frac{5}{4}Nbp^m$. Hence for all $\gamma \in bp^m$ we have

$$|y-\gamma|_\infty > \min\{\frac{|\Delta|}{16e^2}|\alpha|_\infty, \tfrac{5}{4}Nbp^m\} > (1+\varepsilon)Nbp^m. \quad \square$$

PROPOSITION (8.16). *Suppose that* $K = \mathbb{Q}(\sqrt{\Delta})$ *with* $\Delta \equiv 1 \bmod 8$. *Let* p *be a prime of* K *of norm* 2 *and suppose that* $A = A_S$ *with* $S = \{p,\infty\}$. *Let* b *be an* O-*ideal. Denote for* $n \in \mathbb{Z}$ *the reduced quadratic form corresponding to* bp^n *by* (a_n, b_n, c_n). *If for all* $n \in \mathbb{Z}$ *the following conditions are satisfied then* $a = bA$ *is* not *Euclidean.*

(a) *If* $2|a_n$ *then*

$$a_n < \frac{|\Delta|}{64} \quad or \quad 8 \leq a_n < \frac{|\Delta|}{32} \quad or \quad 16 \leq a_n < \frac{|\Delta|}{16};$$

(b) *If* $2|c_n$ *then*

$$a_n < \frac{|\Delta|}{64} \quad or \quad 8 \leq c_n < \frac{|\Delta|}{32} \quad or \quad 16 \leq c_n < \frac{|\Delta|}{16};$$

(c) *If* $2\nmid(a_n+c_n)$ *then*

$$a_n < \frac{|\Delta|}{64} \quad or \quad 8 \leq a_n - |b_n| + c_n < \frac{|\Delta|}{32} \quad or$$

$$16 \leq a_n - |b_n| + c_n < \frac{|\Delta|}{16}.$$

PROOF. Assume that (a), (b) and (c) are satisfied. The sequence of (a_n,b_n,c_n) is periodic modulo the order of $[p]$ in $Cl(\mathcal{O})$. Hence there exists $\varepsilon \in \mathbb{R}_{>0}$ such that $\varepsilon < \frac{1}{16}$ and all strict inequalities in (a), (b) and (c) remain valid if the left hand sides are multiplied by $(1+2\varepsilon)$. It is easily checked that (a), (b) and (c) are not satisfied for $\Delta > -23$, so we may assume that $\Delta \le -23$. Then the covering radius of b is greater than 1. Hence if we have chosen ε small enough there exists y_0 such that (8.12) is satisfied for $n = 0$. Therefore it suffices to prove that for each $m \in \mathbb{Z}_{>0}$ we may use one of the lemma's (8.13), (8.14) or (8.15).

Take $m \in \mathbb{Z}_{>0}$. If $a_m < \frac{|\Delta|}{64}$ we may use (8.13). So suppose that $a_m \ge \frac{|\Delta|}{64}$. Choose $\alpha_m, \beta_m \in bp^m$ in such a way that $|\alpha_m|_\infty = a_m Nbp^m$ and $\beta_m = (b_m + \sqrt{\Delta})\alpha_m/2a_m$. If $bp^{m-1} = \mathbb{Z}\cdot\frac{1}{2}\alpha_m + \mathbb{Z}\beta_m$, the a_m must be even. By (a) we may use (8.14) or (8.15) with $\alpha = \alpha_m$ and $e = a_m$. If $bp^{m-1} = \mathbb{Z}\alpha_m + \mathbb{Z}\cdot\frac{1}{2}\beta_m$, then c_m must be even. By (b) we may use (8.14) or (8.15) with $\alpha = \beta_m$ and $e = c_m$. Finally if $bp^{m-1} = \mathbb{Z}\alpha_m + \mathbb{Z}\cdot\frac{1}{2}(\alpha_m+\beta_m)$, then $a_m + b_m + c_m$ must be even and thus $a_m + c_m$ must be odd. By (c) we may use (8.14) or (8.15) with $\alpha = \alpha_m + \beta_m$ or $\alpha = \alpha_m - \beta_m$ and $e = a_m - |b_m| + c_m$.
□

REMARK (8.17). Because $\Delta \equiv 1 \bmod 8$ we have for each $n \in \mathbb{Z}$ that $a_n c_n \equiv 0 \bmod 2$. This shows that for each $n \in \mathbb{Z}$ exactly two of (a), (b) and (c) give a non-empty condition. In the proof of (8.16) we only use one condition for a given quadratic form. However we need both conditions, because when one of them is necessary for (a,b,c) the other is necessary for $(a,-b,c)$.

COROLLARY (8.18). *If* $|\Delta| > 448$ *or* $\Delta = -407$ *then* Δ *has no Euclidean ideal class.*

PROOF. We show that for these Δ the conditions (a), (b) and (c) are satisfied.

First suppose that $|\Delta| > 448$. Then $\frac{|\Delta|}{64} > 7$ and $\frac{|\Delta|}{32} > 14$. Take $n \in \mathbb{Z}$. If $a_n < \frac{|\Delta|}{64}$ then (a), (b) and (c) are satisfied. In the other case we have $a_n \ge 8$. Because $a_n - |b_n| + c_n$ is even, if $a_n + c_n$ is odd, and $a_n \le c_n \le a_n - |b_n| + c_n$, we find that (a), (b) and (c) are satisfied if $a_n - |b_n| + c_n < |\Delta|/16$. Because $|\Delta| > 448$ we have

$$8 \le a_n < \sqrt{\frac{|\Delta|}{3}} < \frac{|\Delta|}{\sqrt{1344}} < \frac{|\Delta|}{32} .$$

This gives

$$a_n - |b_n| + c_n = a_n - |b_n| + \frac{|\Delta| + b_n^2}{4a_n} = \frac{(2a_n - |b_n|)^2}{4a_n} + \frac{|\Delta|}{4a_n} \le$$

$$\le a_n + \frac{|\Delta|}{32} < \frac{|\Delta|}{16}.$$

Now suppose $\Delta = -407$. The only reduced quadratic forms (a,b,c) that satisfy $a > \frac{|\Delta|}{64} = 6.36$ are $(8,\pm 3,13)$, $(9,\pm 5,12)$ and $(11,11,12)$. It is easily checked that they satisfy (a), (b) and (c). □

At the end of chapter 7 there were 240 rings for which the existence of a Euclidean ideal class was not yet determined. In section (8.2) we dealt with 65 rings of discriminant -23 and with 18 other rings. In this section we dealt with 19 rings with $N\mathfrak{p} = 2$. So 138 rings remain to be investigated.

CHAPTER 9 THE END OF THE PROOFS FOR THE IMAGINARY QUADRATIC CASE

As we remarked in chapter 8 there are still 138 rings in case (#2$^-$) for which we have to decide whether there is a Euclidean ideal class. In this chapter we consider these rings. We show that we may decide, with the help of a computer, for each individual ring whether or not it has a Euclidean ideal class. The possibility that none of (6.6)(a), (b) and (6.7) can be applied did not occur.

In section (9.1) we deal with the rings without Euclidean ideal class. We give two examples to illustrate the method. Table 17 contains data that the reader may use to check that 93 rings have no Euclidean ideal class.

In section (9.2) we deal with the remaining 45 rings. These are the rings with a Euclidean ideal class; they are listed in the tables 1 and 2 and also in table 18. We give examples how we can prove that such a ring has a Euclidean ideal class. The proofs for the other rings are not given, but they run along the same lines.

§(9.1) Rings without a Euclidean ideal class

Let $A = A_{\{p,\infty\}}$ be a subring of an imaginary quadratic field K and let a be an A-ideal. Let b be an $\mathcal{O}$-ideal such that $a = bA$. We fix a unit η of A, such that $|\eta|_p < 1$. Let $h \in \mathbb{Z}_{>0}$ be such that $\eta\mathcal{O} = p^h$. For most applications we take η to be a fundamental unit. However we will not use that explicitly. Notice that $h = h(\mathcal{O})/h(A)$ if η is a fundamental unit.

In this section we show how we can construct an element $\alpha \in K$ with $\eta\alpha \equiv \alpha \bmod b$, for which it is likely that $\alpha \notin \bigcup_{n=0}^{h-1} W_1(bp^{-n})$. If we find that indeed $\alpha \notin \bigcup_{n=0}^{h-1} W_1(bp^{-n})$ we may apply (6.7) to show that a is not Euclidean. Notice that we have changed the notation of (6.7) somewhat. This is for convenience in the discussion below.

First we illustrate by means of two examples how α can be constructed. Then we show that it can be checked by a finite computation whether $\alpha \notin \bigcup_{n=0}^{h-1} W_1(bp^{-n})$. Finally we give a list of all rings for which

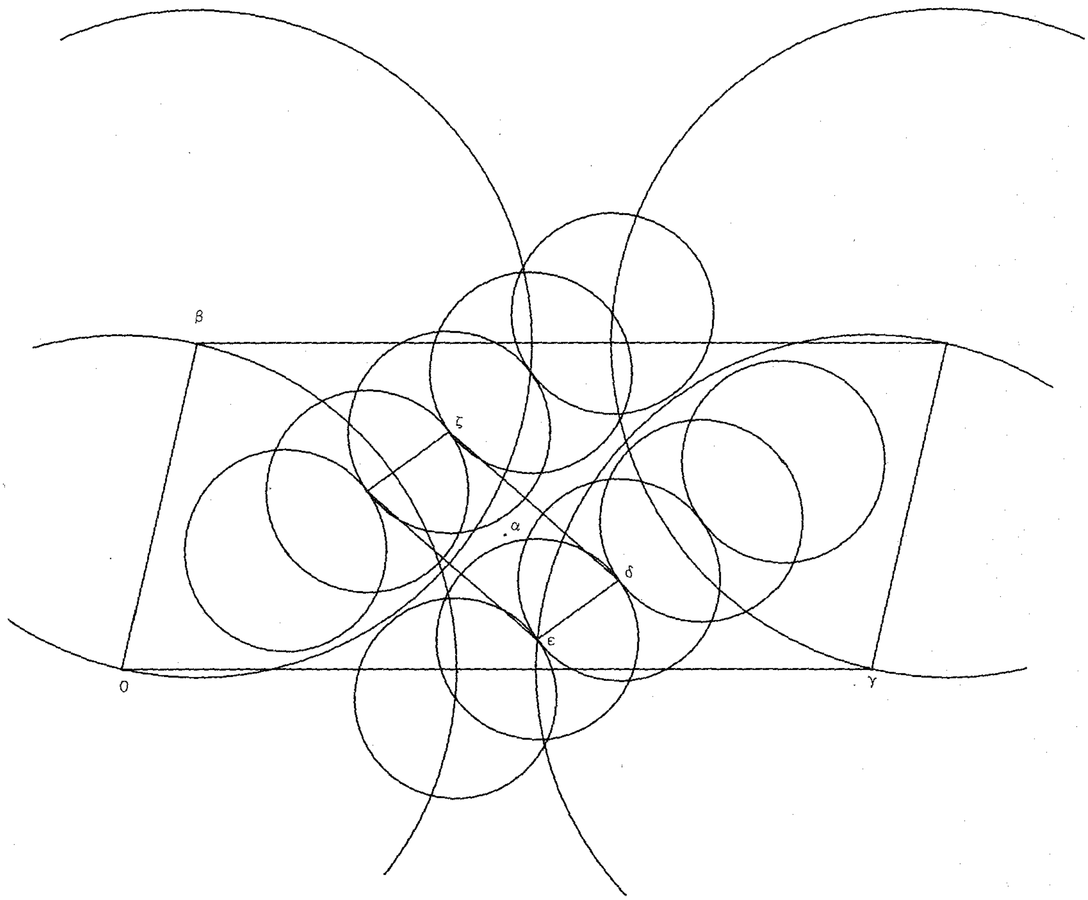


fig. 15

we disproved the existence of a Euclidean ideal class in this way.

EXAMPLE (9.1). $\Delta = -19$; $Np = 11$, cf. fig. 15. We have $h(\mathcal{O}) = 1$. Write $\omega = \frac{1}{2}(1+\sqrt{-19})$. We take $p = \mathbb{Z}\cdot 11 + \mathbb{Z}\cdot(2+\omega)$ and $b = p^2 = \mathbb{Z}\cdot\beta + \mathbb{Z}\cdot\gamma$, with $\beta = -1+5\omega$ and $\gamma = 24+\omega$, cf. fig. 15. Let F be the parallelogram with vertices $0, \beta, \gamma$ and $\beta+\gamma$. Then F is a fundamental domain for b. Figure 15 shows F together with discs contained in $W_1(b)$ and $W_1(bp^{-1})$ that partially cover it. However F is not completely covered by these discs. In particular F_1 is not covered, where F_1 is the parallelogram with vertices $\delta, \varepsilon, \zeta$ and $\varepsilon+\zeta-\delta$, with $\delta = 15+2\omega$, $\varepsilon = 13+\omega$ and $\zeta = 8+4\omega$. The parallelogram F_1 is a fundamental domain for bp^{-1}. A fundamental unit of A is given by $\eta = -2-\omega$. We have $\eta\mathcal{O} = p$ and $F_1 = \delta + \eta^{-1}F$. Let φ be the affine map given by $\varphi(x) = \delta + \eta^{-1}x$, then φ maps $W_1(bp^r)$ bijectively onto $W_1(bp^{r-1})$ for all $r \in \mathbb{Z}_{\le 0}$. Because $F_1 = \varphi(F)$ is not completely covered by $W_1(b) \cup W_1(bp^{-1})$ we may expect that for all $n \in \mathbb{Z}_{\ge 0}$ the region $\varphi^n(F)$ is not completely covered by $\bigcup_{i=0}^{n} W_1(bp^{-i})$. Let α be the fixed point of φ, i.e. $\alpha = \frac{1}{17}(185+43\omega)$, then we may expect that $\alpha \notin \bigcup_{n=0}^{\infty} W_1(bp^{-n})$. By construction we have $\eta\alpha \equiv \alpha \bmod b$, hence to show that $a = bA$ is not Euclidean we only have to show that $\alpha \notin \bigcup_{n=0}^{h-1} W_1(bp^{-n}) = W_1(b)$, cf. (6.7). This is indeed the case and we will show below how this can be proven.

For several other rings the reasoning proceeds in an analogous way. However, if h or Np is large we need more than one picture, as we will see in the next example.

EXAMPLE (9.2). $\Delta = -39$; $Np = 11$, cf. fig. 16. We have $h(\mathcal{O}) = 4$. Write $\omega = \frac{1}{2}(1+\sqrt{-39})$. We take $p = \mathbb{Z}\cdot 11 + \mathbb{Z}\cdot(3+\omega)$. Consider the $\mathcal{O}$-ideals $b_i = \mathbb{Z}\cdot\beta_i + \mathbb{Z}\cdot\gamma_i$, for $0 \le i \le 3$, with

$$\beta_0 = 20-19\omega\,; \qquad \gamma_0 = 17+2\omega\,;$$
$$\beta_1 = 18-5\omega\,; \qquad \gamma_1 = 16+9\omega\,;$$
$$\beta_2 = 18-5\omega\,; \qquad \gamma_2 = 17+2\omega\,;$$
$$\beta_3 = 35-3\omega\,; \qquad \gamma_3 = -1+7\omega\,,$$

cf. fig. 16. Notice that $[b_i] = [p^{-i}]$. The parallelograms F_i with vertices $0, \beta_i, \gamma_i$ and $\beta_i+\gamma_i$ are fundamental domains for the ideals b_i, for $0 \le i \le 3$. These parallelograms F_i are not completely contained

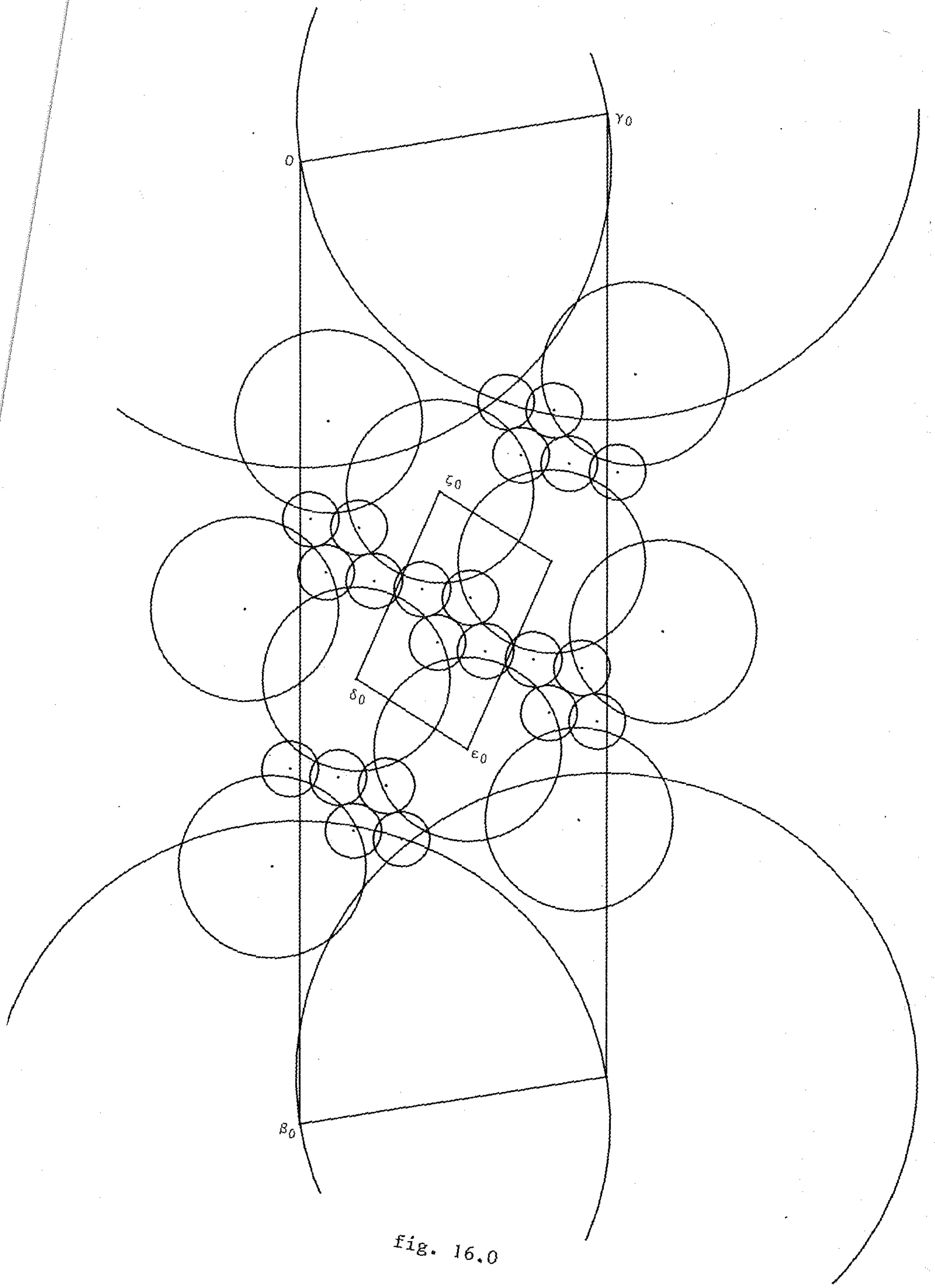


fig. 16.0

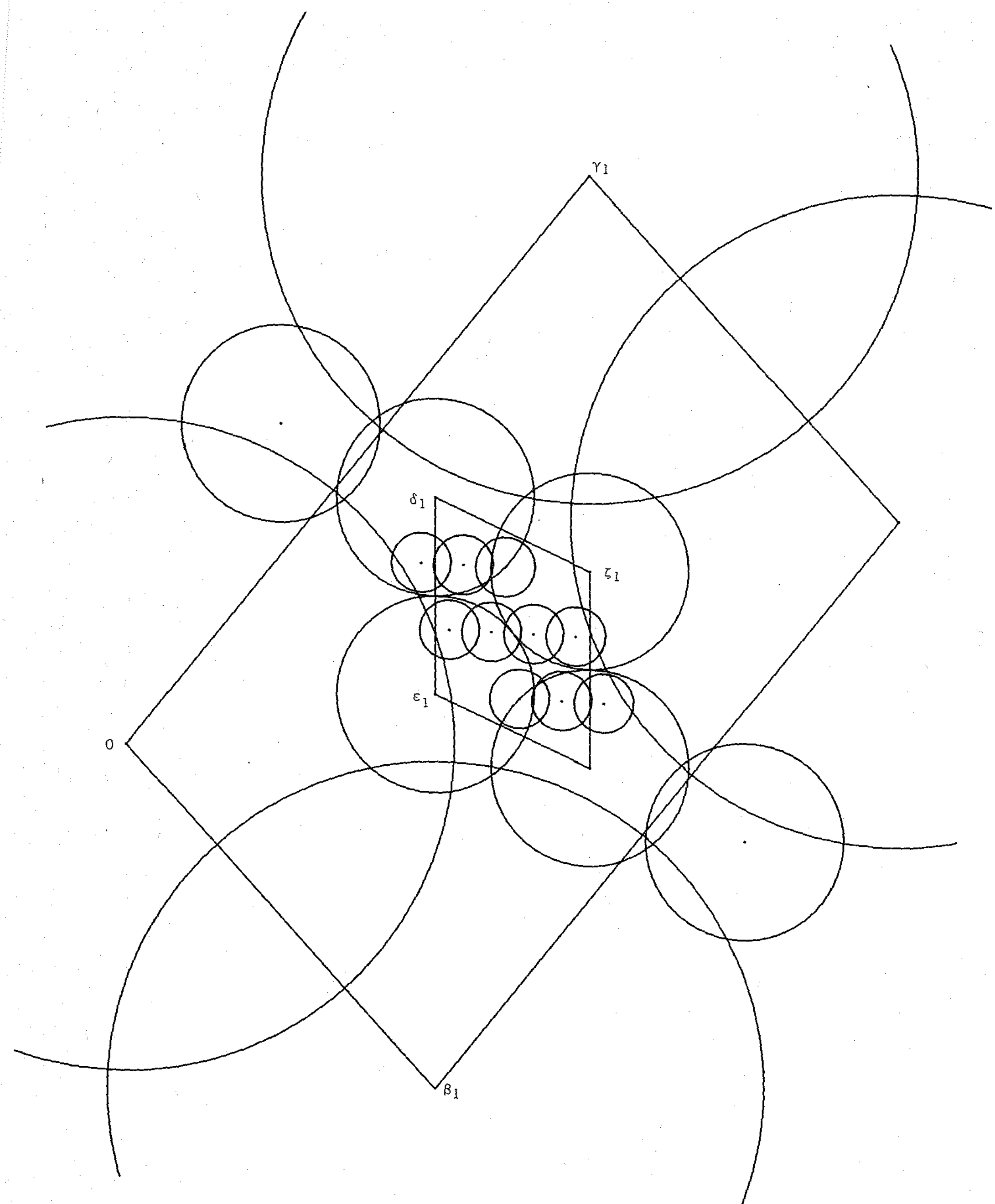


fig. 16.1

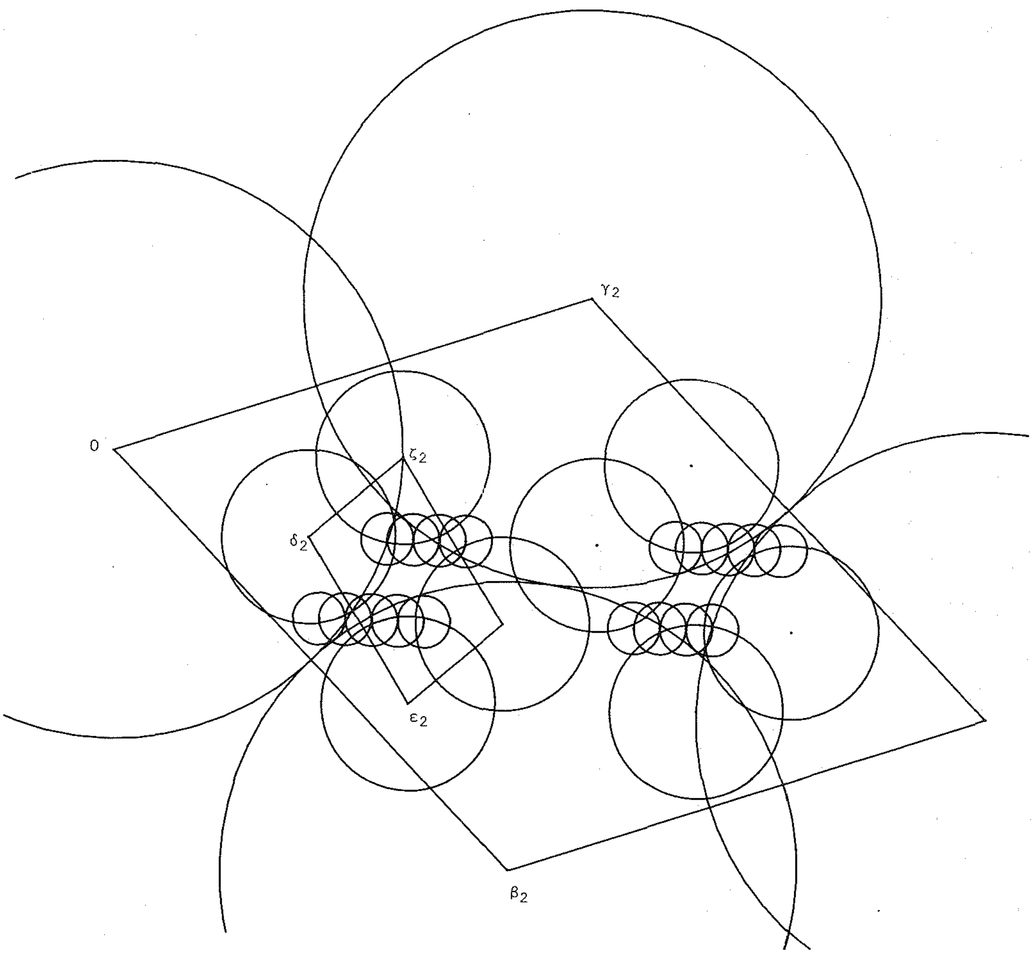


fig. 16.2

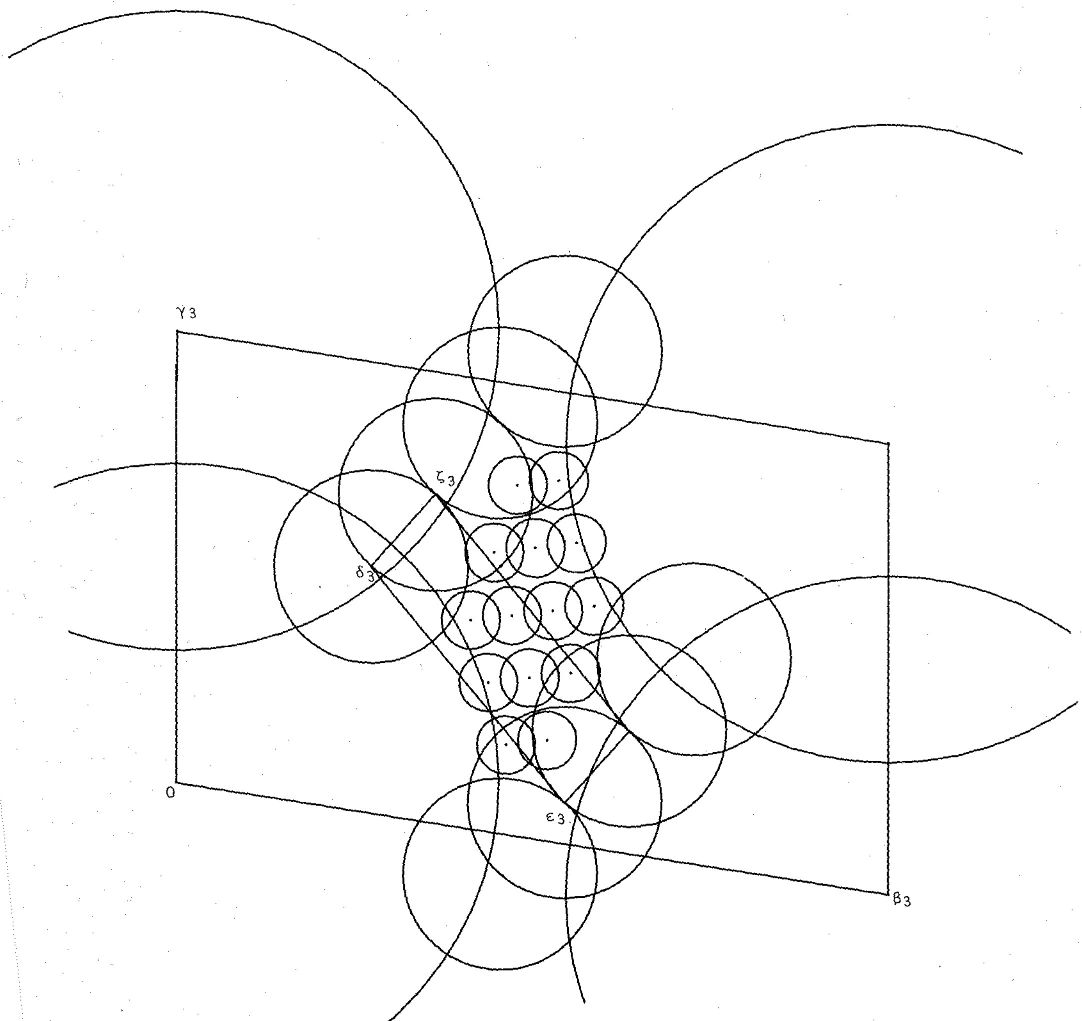


fig. 16.3

in $\bigcup_{n=0}^{2} W_1(b_i p^{-n})$. In each F_{i-1} we have chosen a parallelogram $\mathcal{G}_i$, which is a fundamental domain of $b_i p^{-1}$ that is not completely covered by $\bigcup_{n=0}^{2} W_1(b_i p^{-n})$. The $\mathcal{G}_i$ are drawn as small parallelograms inside the F_i in fig. 16. The parallelograms $\mathcal{G}_i$ have vertices δ_i, ε_i, ζ_i and $\varepsilon_i + \zeta_i - \delta_i$, where

$$\delta_0 = 14 - 10\omega\,, \quad \varepsilon_0 = 22 - 11\omega\,, \quad \zeta_0 = 15 - 6\omega\,;$$

$$\delta_1 = 12 + 4\omega\,, \quad \varepsilon_1 = 14 + \omega\,, \quad \zeta_1 = 20 + 3\omega\,;$$

$$\delta_2 = 8 - \omega\,, \quad \varepsilon_2 = 13 - 3\omega\,, \quad \zeta_2 = 11\,;$$

$$\delta_3 = 9 + 3\omega\,, \quad \varepsilon_3 = 19 - \omega\,, \quad \zeta_3 = 12 + 4\omega\,.$$

For $0 \le i \le 3$ let φ_i be the affine map that maps $0, \beta_i, \gamma_i$ to δ_{i-1}, ε_{i-1}, ζ_{i-1} (in the same order), hence φ_i maps F_i onto $\mathcal{G}_{i-1}$, where $i-1$ is regarded mod 4. Then φ_i also maps b_i bijectively onto $b_{i-1}p^{-1}$. We have

$$\varphi_0(x) = 9 + 3\omega + \frac{7+\omega}{33}\,x\,,$$

$$\varphi_1(x) = 14 - 10\omega + \frac{7+\omega}{22}\,x\,,$$

$$\varphi_2(x) = 12 + 4\omega + \frac{4-\omega}{11}\,x\,,$$

$$\varphi_3(x) = 8 - \omega + \frac{4-\omega}{22}\,x\,.$$

Let φ be the combined map $\varphi_1\varphi_2\varphi_3\varphi_0$, then φ maps b_0 bijectively onto b_0p^{-4} and $\varphi(F_0)$ is contained in $\mathcal{G}_0$. The map φ is given by $\varphi(x) = \frac{1}{121}(2125 - 1007\omega) + \eta^{-1}x$, where $\eta = 83 + 24\omega$ is a fundamental unit of A. The fixed point α of φ is given by $\alpha = \frac{1}{14452}(253670 - 121378\omega)$. By construction we have $\eta\alpha \equiv \alpha \bmod b_0$. Also $\alpha \in \mathcal{G}_0$, $\varphi_0\alpha \in \mathcal{G}_3$, $\varphi_3\varphi_0\alpha \in \mathcal{G}_2$ and $\varphi_2\varphi_3\varphi_0\alpha \in \mathcal{G}_1$, so there is a great chance that $\alpha \notin \bigcup_{n=0}^{3} W_1(b_0p^{-n})$. Because we are able to show that indeed $\alpha \notin \bigcup_{n=0}^{3} W_1(b_0p^{-n})$, see below, we conclude from (6.7) that A has no Euclidean ideal class.

For each of the 93 rings we are considering, we found in a similar way an element α with $\eta\alpha \equiv \alpha \bmod b$ for which it is very likely that $\alpha \notin \bigcup_{n=0}^{h} W_1(bp^{-n})$. Now we will show how we may decide by means of a finite computation whether $\alpha \in W_1(bp^{-n})$ for a given n. Of course it suffices to compute $\min\{|\alpha - \beta|_\infty : \beta \in bp^{-n}\}$. This can be done by computing $|\alpha - \beta|_\infty$ for only 4 values of $\beta \in bp^{-n}$.

LEMMA (9.3). *Let* $\mathfrak{c}$ *be an* $\mathcal{O}$*-ideal and let* (a,b,c) *be the reduced quadratic form corresponding to it, cf. section (3.1). Let* $\alpha, \beta \in \mathfrak{c}$ *be such that* $|\alpha|_\infty = aN\mathfrak{c}$ and $\beta = \frac{b+\sqrt{\Delta}}{2a}\alpha$. *Let* $x = u\alpha + v\beta$ *be an element of* $\mathbb{C}$ *and let* $m, n \in \mathbb{Z}$ *be such that* $m \le u \le m+1$ *and* $n \le v \le n+1$. *Then*

$$\min\{|x-\gamma|_\infty : \gamma \in \mathfrak{c}\} =$$

$$\min\{|x-m\alpha-n\beta|_\infty,\ |x-m\alpha-(n+1)\beta|_\infty,\ |x-(m+1)\alpha-n\beta|_\infty,\ |x-(m+1)\alpha-(n+1)\beta|_\infty\}.$$

PROOF. We may assume that $m = n = 0$. Let $w\cdot\alpha$ be the orthogonal projection of x on the line $\mathbb{R}\alpha$. Then, since $|b| \le a$ and $0 \le u, v \le 1$ we have $-\frac{1}{2} \le w \le \frac{3}{2}$. Hence

$$\min\{|x-\gamma|_\infty : \gamma \in \mathbb{Z}\alpha\} =$$
$$= \min\{|x|_\infty, |x-\alpha|_\infty\} \le (\tfrac{1}{4}a + v^2 \tfrac{|\Delta|}{4a})N\mathfrak{c}\ .$$

In an analogous way we get

$$\min\{|x-\gamma|_\infty : \gamma \in \beta + \mathbb{Z}\alpha\} =$$
$$= \min\{|x-\beta|_\infty, |x-\alpha-\beta|_\infty\} \le (\tfrac{1}{4}a + (1-v)^2 \tfrac{|\Delta|}{4a})N\mathfrak{c}\ .$$

Take $\gamma = k\alpha + \ell\beta \in \mathfrak{c}$. If $\ell < 0$ then

$$|x-\gamma|_\infty \ge (\ell - v)^2 \frac{|\Delta|}{4a} N\mathfrak{c} \ge (1+v^2)\frac{|\Delta|}{4a} N\mathfrak{c} > (\tfrac{1}{4}a + v^2\tfrac{|\Delta|}{4a})N\mathfrak{c},$$

because $a^2 < |\Delta|$. If $\ell > 1$ then

$$|x-\gamma|_\infty \ge (\ell - v)^2 \frac{|\Delta|}{4a} N\mathfrak{c} \ge (1+(1-v)^2)\frac{|\Delta|}{4a} N\mathfrak{c} >$$
$$> (\tfrac{1}{4}a + (1-v)^2\tfrac{|\Delta|}{4a})N\mathfrak{c}.$$

This proves the lemma. □

The 93 rings for which the method works are listed in table 17. This table is organized as follows. The first column '#' counts the number of rings in the table. The second column gives the discriminant Δ of K. The third column gives the norm of $\mathfrak{p}$. In the fourth column 'h' we find the order of $[p]$ in $Cl(\mathcal{O})$. In all rings in this list this is equal to the class number of $\mathcal{O}$. Because in the next section we show that the remaining rings have a Euclidean ideal class this shows that all rings A, with $h(A) = 2$ and for which there is no Euclidean ideal class, were already considered in a previous chapter. In the fifth column we find a fundamental unit η of A. For η we have $|\eta|_\infty = Np^h$. This is the unit for which the method described above works. In the sixth column we find $|\eta - 1|_\infty$. The seventh column gives $\alpha|\eta - 1|_\infty \in \mathcal{O}$. Here α is such that $\eta\alpha \equiv \alpha \bmod \mathcal{O}$ and $\alpha \notin \bigcup_{n=0}^{h-1} W_1(p^{-n})$. Because for all rings in the list we have $h(A) = 1$ this suffices to prove that A has no Euclidean ideal class. The last column gives the least $t \in \mathbb{R}$ such that $\alpha \notin \bigcup_{n=0}^{h-1} W_t(p^{-n})$; here t is rounded off to 4 decimals. For $\Delta = -19$ and $Np = 5$ or $Np = 7$ we have $t = 1$. This shows that for these cases we need (6.7) with $t = 1$. These rings cannot be handled with the theorem of Barnes and Swinnerton-Dyer, cf. (5.2) and (6.5).

REMARK (9.4). For each choice of Δ and Np in table 17 we considered only one prime p of this norm. The conjugate q of p gives rise to an isomorphic ring, hence it need not be considered. The prime p can be distinguished from its conjugate by the value of η, which is in p but not in q.

TABLE 17. Rings $A_{\{p,\infty\}} \subset \mathbb{Q}(\sqrt{\Delta})$ without Euclidean ideal class. We write $\omega = \frac{1}{2}\sqrt{\Delta}$ if Δ is even and $\omega = \frac{1}{2}(1+\sqrt{\Delta})$ if Δ is odd.

#	Δ	Np	h	η	$\lvert\eta-1\rvert_\infty$	$\alpha\lvert\eta-1\rvert_\infty$	t
1	−19	5	1	−ω	7	1+3ω	1
2		7	1	−1−ω	11	4+6ω	1
3		11	1	−2−ω	17	2+8ω	1.1765
4	−23	139	3	−133+678ω	2685208	909044+984600ω	1.0017
5		151	3	−1721−174ω	3446568	1039620−1609644ω	1.0021
6		179	3	−1783+818ω	5738088	2723916−2386052ω	1.0042
7		277	3	−23+1884ω	21252096	1373592−9583656ω	1.0203
8		311	3	−1961−1934ω	30086088	11607648+12369852ω	1.0045
9		331	3	−6025+6ω	36276736	12200844+13395986ω	1.0123
10		349	3	−3955−1812ω	42518272	16664728−18629020ω	1.0004
11		397	3	7043+996ω	62555692	8619734+30956882ω	1.0032
12		439	3	5405−3522ω	84597232	9440140+39107892ω	1.0060
13		461	3	−3601+4076ω	97975308	15109230+41013414ω	1.0002
14		491	3	−9631−1414ω	118391448	37633764−59115084ω	1.0067
15		509	3	6227−4492ω	131864268	62541768−63764354ω	1.0070
16		541	3	−3089+5244ω	158341356	9064998+71803650ω	1.0096
17		577	3	−9101−3576ω	192121812	2053182−91366458ω	1.0027
18		587	3	1883−5914ω	202264152	98902296−82761930ω	1.0071
19		601	3	2909−6144ω	217082128	29989768+103054308ω	1.0095
20		647	3	16001−3394ω	270811416	8966310−112754906ω	1.0006
21		673	3	−15797−1992ω	304854804	43268922−128980320ω	1.0001
22		739	3	17995−5442ω	403552872	199755312+201382422ω	1.0173
23		761	3	−17975−3176ω	440750208	144003264+180874440ω	1.0074
24		811	3	6485−9606ω	533408368	213467624+203782176ω	1.0063
25		857	3	−18047+8776ω	629450112	31117960+310574216ω	1.0101
26		967	3	1951−12414ω	904239576	5715492+450610470ω	1.0040
27		1013	3	25319+6308ω	1039452252	208247874−457567008ω	1.0094
28		1061	3	10235−14356ω	1194383868	590320812−595862510ω	1.0087
29		1087	3	−24991+12774ω	1284402712	4906996+530433976ω	1.0006
30		1129	3	13403−15648ω	1439058532	606793884+716876222ω	1.0095
31		1153	3	−15707+16008ω	1532823984	7450944−765460128ω	1.0080

TABLE 17. Continued.

#	Δ	Np	h	η	$\|\eta-1\|_\infty$	$\alpha\|\eta-1\|_\infty$	t
32	-23	1289	3	-19325-15632ω	2141754852	423653106-920352444ω	1.0070
33		1381	3	-30785+19524ω	2633831388	585382986-1125070128ω	1.0099
34		1409	3	-42407+16912ω	2797328832	1143007384+1096105805ω	1.0024
35		1427	3	-54673+1934ω	2905948896	657656268-1286811318ω	1.0013
36	-24	53	2	-47-10ω	2904	996+1184ω	1.0131
37	-31	19	3	83-10ω	6704	1968+2508ω	1.0925
38	-35	3	2	-ω	11	1+5ω	1.0909
39	-39	5	4	5-8ω	624	92+284ω	1.0064
40		11	4	83+24ω	14452	6590-7082ω	1.1270
41	-47	7	5	-125-6ω	17064	5328-7740ω	1.2581
42		17	5	1085+104ω	1417584	133752-635780ω	1.0733
43	-51	11	2	-1-3ω	127	32+57ω	1.1575
44	-55	7	4	43-8ω	2324	1096+668ω	1.0568
45		13	4	-101+40ω	28724	14048-13638ω	1.1202
46		17	4	-229+56ω	83924	21342+35808ω	1.1007
47	-56	5	4	-11+6ω	648	36-252ω	1.0463
48		13	4	155+18ω	28252	1918+13168ω	1.2092
49	-59	3	3	-3-ω	35	15-17ω	1.0286
50		5	3	11-ω	105	48+52ω	1.3048
51	-68	3	4	8-ω	66	5+29ω	1.0758
52	-71	5	7	277+4ω	77568	21104-24680ω	1.0061
53		19	7	-8653+6990ω	893882056	424830664-354490388ω	1.3313
54	-79	5	5	-55+4ω	3232	376+1272ω	1.1894
55	-95	2	8	-8+3ω	270	18+99ω	1.1889
56		3	8	-75+8ω	6704	1224-3208ω	1.2685
57	-103	2	5	2+ω	28	8+10ω	1.2143
58	-104	5	6	-109-12ω	15844	4404-6674ω	1.2008
59		7	6	307+30ω	117036	22878+50538ω	1.2916
60	-111	5	8	579-56ω	389524	137330+193078ω	1.2240
61	-116	3	6	2+5ω	726	214-344ω	1.3085
62	-119	3	10	-87-40ω	59264	27904-27240ω	1.0716

TABLE 17. Continued.

#	Δ	Np	h	η	$\|\eta-1\|_\infty$	$\alpha\|\eta-1\|_\infty$	t
63	-119	5	10	2465+312ω	9760384	4609352-4779432ω	1.2000
64	-127	2	5	-ω	34	12+11ω	1.2059
65	-131	3	5	15-ω	215	101+107ω	1.4651
66	-143	2	10	28-3ω	972	360-360ω	1.2099
67	-151	2	7	10-ω	110	10-40ω	1.4545
68	-159	2	10	8-5ω	1014	152+380ω	1.1874
69	-164	3	8	-40+11ω	6642	3977+3659ω	1.3868
70	-167	2	11	-2+7ω	2046	736+758ω	1.2473
71		3	11	321-46ω	176552	59008-82880ω	1.1566
72	-183	2	8	14+ω	228	68-70ω	1.1140
73	-191	2	13	80-7ω	8040	1368+2478ω	1.0276
74		3	13	1245-46ω	1591880	718468+770376ω	1.2486
75	-199	2	9	-22+ω	556	238+213ω	1.2752
76	-215	2	14	58+15ω	16254	2142-6090ω	1.0551
77		3	14	-1971-112ω	4787024	328120+2318452ω	1.3567
78	-239	2	15	-116-17ω	33018	3124+10199ω	1.2357
79	-263	2	13	-74+7ω	8334	236-2672ω	1.4130
80		3	13	-1239-22ω	1596824	233266+767774ω	1.4652
81	-271	2	11	44+ω	1960	864+604ω	1.0510
82	-287	3	14	-1791-136ω	4786688	926032-2260048ω	1.1270
83	-303	2	10	-20+3ω	1062	144-330ω	1.2015
84	-311	2	19	686-31ω	522948	48888-156806ω	1.0208
85		3	19	33585+482ω	1162193816	317231080-550275408ω	1.4224
86	-319	2	10	16+3ω	990	90+315ω	1.8636
87	-327	2	12	-6-7ω	4116	882+1323ω	1.2398
88	-335	2	18	236-51ω	261724	59564+83363ω	1.2026
89	-359	2	19	-178-73ω	524718	97596+184114ω	1.1326
90		3	19	-32517-914ω	1162327416	564924540-579190000ω	1.4427
91	-383	2	17	352+7ω	130362	11586-45744ω	1.0458
92	-439	2	15	-162-7ω	33100	6370-10387ω	1.4672
93	-447	2	14	-48-11ω	16492	788+5078ω	1.5049

§(9.2) Rings with a Euclidean ideal class

In this section we describe a method to prove that a given A - ideal $\mathfrak{a}$ is Euclidean. We will give several examples to show how this method works.

Let $\mathfrak{b}$ be an $\mathcal{O}$ - ideal such that $\mathfrak{a} = \mathfrak{b}A$. By (6.6)(b) it suffices to find $n \in \mathbb{Z}_{\geq 0}$, such that $\mathbb{C} = \bigcup_{i=0}^{n} W_1(\mathfrak{b}\mathfrak{p}^{-i})$. Because $\mathfrak{b} \subset \mathfrak{b}\mathfrak{p}^{-i}$ for $i \in \mathbb{Z}_{\geq 0}$ it suffices to show that $F \subset \bigcup_{i=0}^{n} W_1(\mathfrak{b}\mathfrak{p}^{-i})$ for some fundamental domain F of $\mathfrak{b}$. In most cases this will be done by partitioning F into triangles that have vertices in $\mathfrak{b}\mathfrak{p}^{-n}$. For each of these triangles we show that they are contained in $\bigcup_{i=0}^{n} W_1(\mathfrak{b}\mathfrak{p}^{-i})$. The next lemma is an important tool to do this.

LEMMA (9.5). *Let* T *be a triangular region in the plane with vertices* A_1, A_2 *and* A_3. *For* $i = 1, 2, 3$ *let* D_i *be an open disc in the plane with centre at* A_i. *If* $D_1 \cap D_2 \cap D_3 \neq \emptyset$, *then* $T \subset D_1 \cup D_2 \cup D_3$.

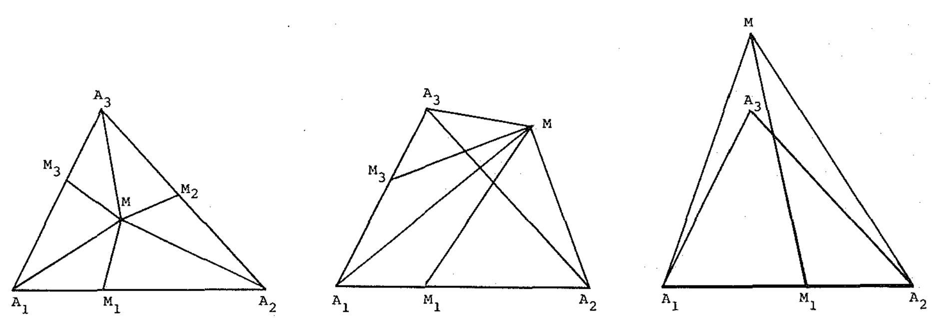


fig. 17

PROOF. Choose $M \in D_1 \cap D_2 \cap D_3$. In the following we regard the indices mod 3. Because $D_i \cap D_{i+1} \neq \emptyset$ there exists $M_i \in D_i \cap D_{i+1}$ on the line A_iA_{i+1}, between A_i and A_{i+1}. Since D_i is convex the triangles T_i with vertices A_i, M and M_i and T_i' with vertices A_i, M and M_{i-1} are contained in D_i. Because $T \subset \bigcup_{i=1}^{3} (T_i \cup T_i')$ we have $T \subset D_1 \cup D_2 \cup D_3$, cf. fig. 17. □

EXAMPLE (9.6). $\Delta = -84$; $Np = 2$, cf. fig. 18. Write $\omega = \sqrt{-21}$. We have $p = \mathbb{Z}\cdot 2 + \mathbb{Z}\cdot(\omega+1)$. We choose $b = \mathbb{Z}\cdot\alpha + \mathbb{Z}\cdot\beta$, with $\alpha = 20$ and $\beta = 8 + 4\omega$, cf. fig. 18. We have $Nb = 80$. The parallelogram F with vertices 0, α, β and $\alpha+\beta$ is a fundamental domain of b. We will show that $F \subset \bigcup_{i=0}^{3} bp^{-i}$. Let G be the group generated by the reflection in the line through 0 and $\alpha+\beta$ and by the reflection in the line through α and β. The parallelogram F is contained in the triangles T_i for $i = 1, 2, 3$ and their images under G. Here T_1 is the triangle with vertices 0, $\frac{1}{2}\alpha$ and $\frac{1}{4}(\alpha+\beta)$, the triangle T_2 has vertices $\frac{1}{2}$, $\frac{1}{4}(\alpha+\beta)$ and $\frac{1}{2}(\alpha+\beta)$ and T_3 has vertices $\frac{1}{2}\alpha$, $\frac{1}{2}(\alpha+\beta)$ and α. By using the symmetries of G we only have to show that $T_1 \cup T_2 \cup T_3$ is contained in $\bigcup_{i=0}^{3} W_1(bp^{-i})$. For this we use (9.5). As an example we show that $T_2 \subset \bigcup_{i=0}^{3} W_1(bp^{-i})$. We use (9.5) with $A_1 = \frac{1}{2}\alpha$, $A_2 = \frac{1}{4}(\alpha+\beta)$ and $A_3 = \frac{1}{2}(\alpha+\beta)$. The disc D_1 has radius $\sqrt{20}$ and is contained in $W_1(bp^{-2})$. The disc D_2 has radius $\sqrt{10}$ and is contained in $W_1(bp^{-3})$ and the disc D_3 has radius $\sqrt{40}$ and is contained in $W_1(bp^{-1})$. To show that $D_1 \cap D_2 \cap D_3 \neq \emptyset$ we only have to show that an intersection point of the circle with radius $\sqrt{10}$ and centre at A_2 and the circle with radius $\sqrt{40}$ and centre at A_3 is contained in D_1. Such an intersection point is $9 + \frac{9}{7}\omega + \frac{3-\omega}{\sqrt{7}}$, which has distance $4.162 < 4.472 = \sqrt{20}$ to A_1.

EXAMPLE (9.7). $\Delta = -23$; $Np = 131$, cf. fig. 19. Write $\omega = \frac{1}{2}(1+\sqrt{-23})$. We have $p = \mathbb{Z}\cdot 131 + \mathbb{Z}\cdot(\omega+48)$. We choose $b = \mathbb{Z}\cdot\alpha + \mathbb{Z}\cdot\beta$, with $\alpha = 22 - 5\omega$ and $\beta = 4 + 11\omega$, cf. fig. 19, then $Nb = 262$. We show that $\mathbb{C} \subset W_1(b) \cup W_1(bp^{-1})$. For this it suffices to show that $F \subset W_1(b) \cup W_1(bp^{-1})$, where F is the parallelogram with vertices 0, α, β and $\alpha+\beta$. Write $\gamma = 14 + 2\omega$. We partition F into 8 regions. These are the triangle with vertices 0, α and γ, the triangle with vertices α, γ and $\gamma+2$, the triangle with vertices α, $\gamma+2$ and $\alpha+\beta$, the polygonal region with vertices 0, γ, $\gamma+\omega$, $\gamma-2+\omega$, $\gamma-2+2\omega$ and $\gamma-4+2\omega$ and the 4 regions obtained by rotating these regions around $\frac{1}{2}(\alpha+\beta)$ over an angle π,

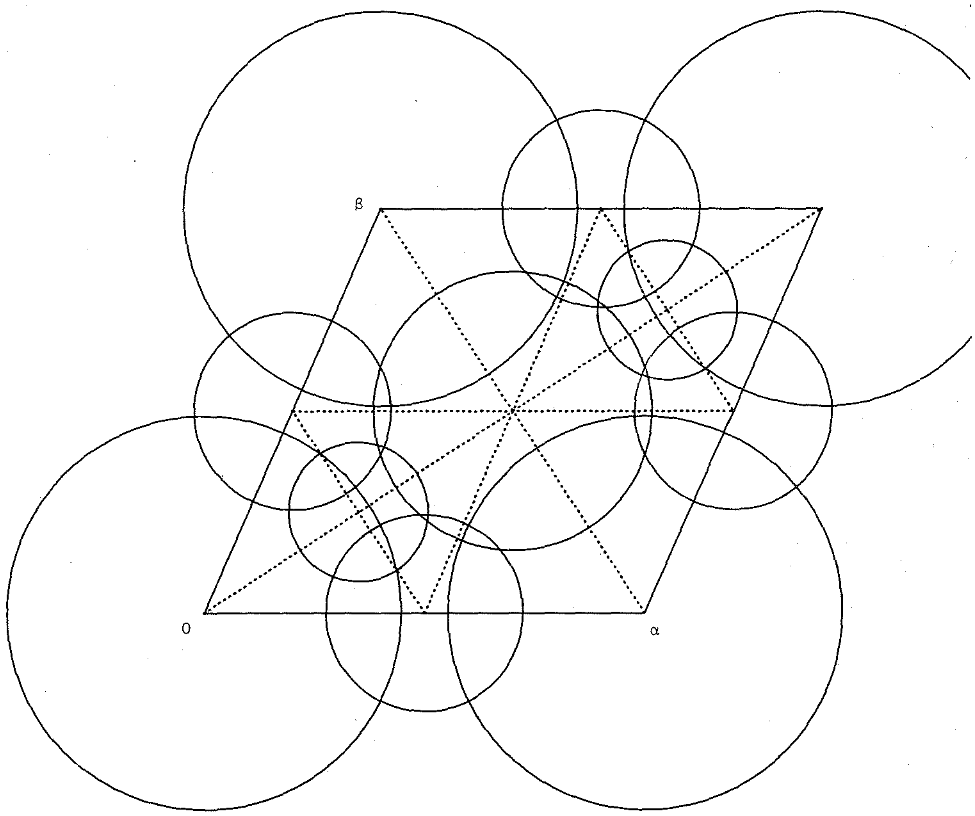


fig. 18

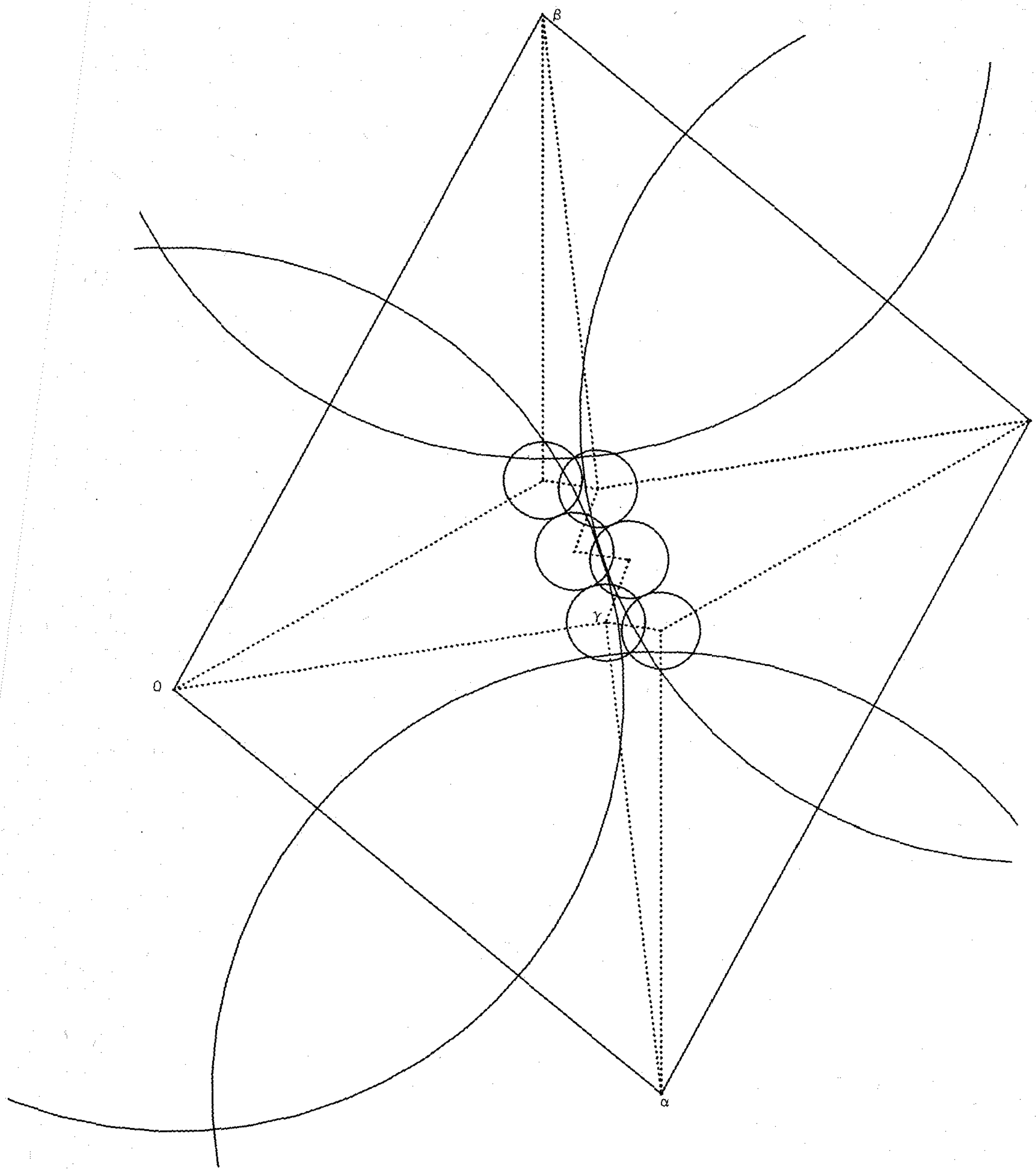


fig. 19

cf. fig. 19. We can use (9.5) to show that each of the triangular regions is contained in $W_1(b) \cup W_1(bp^{-1})$. The polygonal regions can be divided into a collection of triangular regions by adding the diagonals from 0 and $\alpha+\beta$. For each of these triangles we may use (9.5) to show that it is contained in $W_1(b) \cup W_1(bp^{-1})$. As an illustration we show that the triangle with vertices α, γ and $\gamma+2$ is contained in $W_1(b) \cup W_1(bp^{-1})$. Take $z = \gamma + 1 - i$, then z is on the edge of the discs with radius $\sqrt{2}$ and vertices at γ and $\gamma+2$. These discs are contained in $W_1(bp^{-1})$. To complete the proof it suffices to show that $|z-\alpha|_\infty < 262$. In fact: $|z-\alpha|_\infty = 261.43 < 262$.

EXAMPLE (9.8). $\Delta = -136$; $Np = 2$, cf. fig. 20. Write $\omega = \sqrt{-34}$. We have $p = \mathbb{Z}\cdot 2 + \mathbb{Z}\cdot\omega$. We choose $b = \mathbb{Z}\cdot\alpha + \mathbb{Z}\cdot\beta$, with $\alpha = 80$ and $\beta = 16 + 16\omega$, then $Nb = 1280$. We show that $\mathbb{C} = \bigcup_{i=0}^{7} W_1(bp^{-i})$. For this it suffices to show that $F \subset \bigcup_{i=0}^{7} W_1(bp^{-i})$, where F is the parallelogram with vertices $0, \alpha, \beta$ and $\alpha+\beta$. Write $\gamma = 20 + 10\omega = \frac{1}{8}\alpha + \frac{5}{8}\beta$, $\delta = 26 + 6\omega = \frac{1}{4}\alpha + \frac{3}{8}\beta$ and $\varepsilon = 38 + 3\omega = \frac{7}{16}\alpha + \frac{3}{16}\beta$. Then $\gamma \in bp^{-5}$, $\delta \in bp^{-6}$ and $\varepsilon \in bp^{-7}$. We divide F into 7 regions, each of which may be divided into triangles such that (9.5) may be used. The first two regions are the polygonal regions with vertices 0, $\frac{1}{2}\alpha$, ε, $\frac{1}{2}\alpha + \frac{1}{4}\beta$, $\frac{1}{4}(\alpha+\beta)$, δ and $\frac{1}{2}\beta$ and its mirror image in $\frac{1}{2}(\alpha+\beta)$. By adding the diagonals from $\frac{1}{4}(\alpha+\beta)$, resp. $\frac{3}{4}(\alpha+\beta)$, we obtain the triangular regions for which (9.5) may be used. Next we have the region with vertices $\frac{1}{2}\alpha$, ε, $\frac{1}{2}\alpha + \frac{1}{4}\beta$ and α and its mirror image in $\frac{1}{2}(\alpha+\beta)$. By adding the diagonal from $\frac{1}{2}\alpha$ to $\frac{1}{2}\alpha + \frac{1}{4}\beta$, resp. from $\frac{1}{2}\alpha + \beta$ to $\frac{1}{2}\alpha + \frac{3}{4}\beta$, we obtain 4 triangles for which (9.5) may be used. Next we have the triangle with vertices $\frac{1}{2}\beta$, γ and β and its mirror image in $\frac{1}{2}(\alpha+\beta)$. For these triangles we may use (9.5). Finally we have a star shaped region with vertices β, γ, $\frac{1}{2}\beta$, δ, $\frac{1}{4}(\alpha+\beta)$, $\frac{1}{2}\alpha + \frac{1}{4}\beta$, α, $\alpha+\beta-\gamma$, $\alpha + \frac{1}{2}\beta$, $\alpha+\beta-\delta$, $\frac{3}{4}(\alpha+\beta)$ and $\frac{1}{2}\alpha + \frac{3}{4}\beta$. By adding the lines from $\frac{1}{2}(\alpha+\beta)$ to all vertices of this region we obtain the triangles for which (9.5) may be used.

EXAMPLE (9.9). $\Delta = -79$; $Np = 2$, cf. fig. 21. Write $\omega = \frac{1}{2}(1+\sqrt{-79})$. We have $p = \mathbb{Z}\cdot 2 + \mathbb{Z}\cdot\omega$. We choose $b = \mathbb{Z}\cdot\alpha + \mathbb{Z}\cdot\beta$, with $\alpha = 32$ and $\beta = 8\omega$, then $Np = 256$. We show that $\mathbb{C} = \bigcup_{i=0}^{5} W_1(bp^{-i})$. For this it suffices to show that $F \subset \bigcup_{i=0}^{5} W_1(bp^{-i})$, where F is the parallelogram with vertices $0, \alpha, \beta$ and $\alpha+\beta$. Write $\gamma = 12 + 4\omega$, $\delta = 14 + 2\omega$ and $\varepsilon = 9 + 3\omega$, then $\gamma \in bp^{-3}$, $\delta \in bp^{-1}$ and $\varepsilon \in bp^{-5}$. We partition F into 7 regions, each of which is contained in $\bigcup_{i=0}^{5} W_1(bp^{-i})$, as we will show.

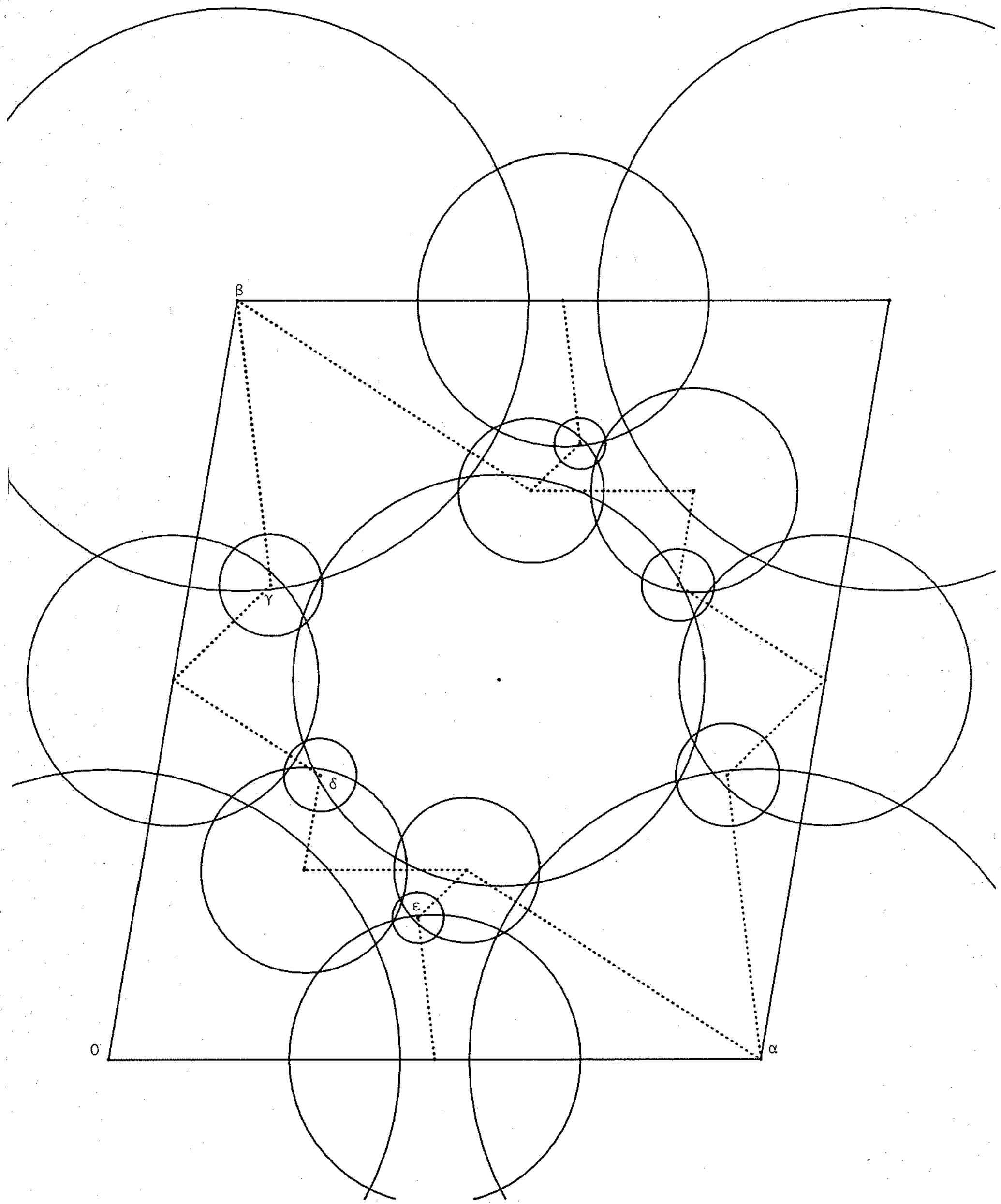


fig. 20

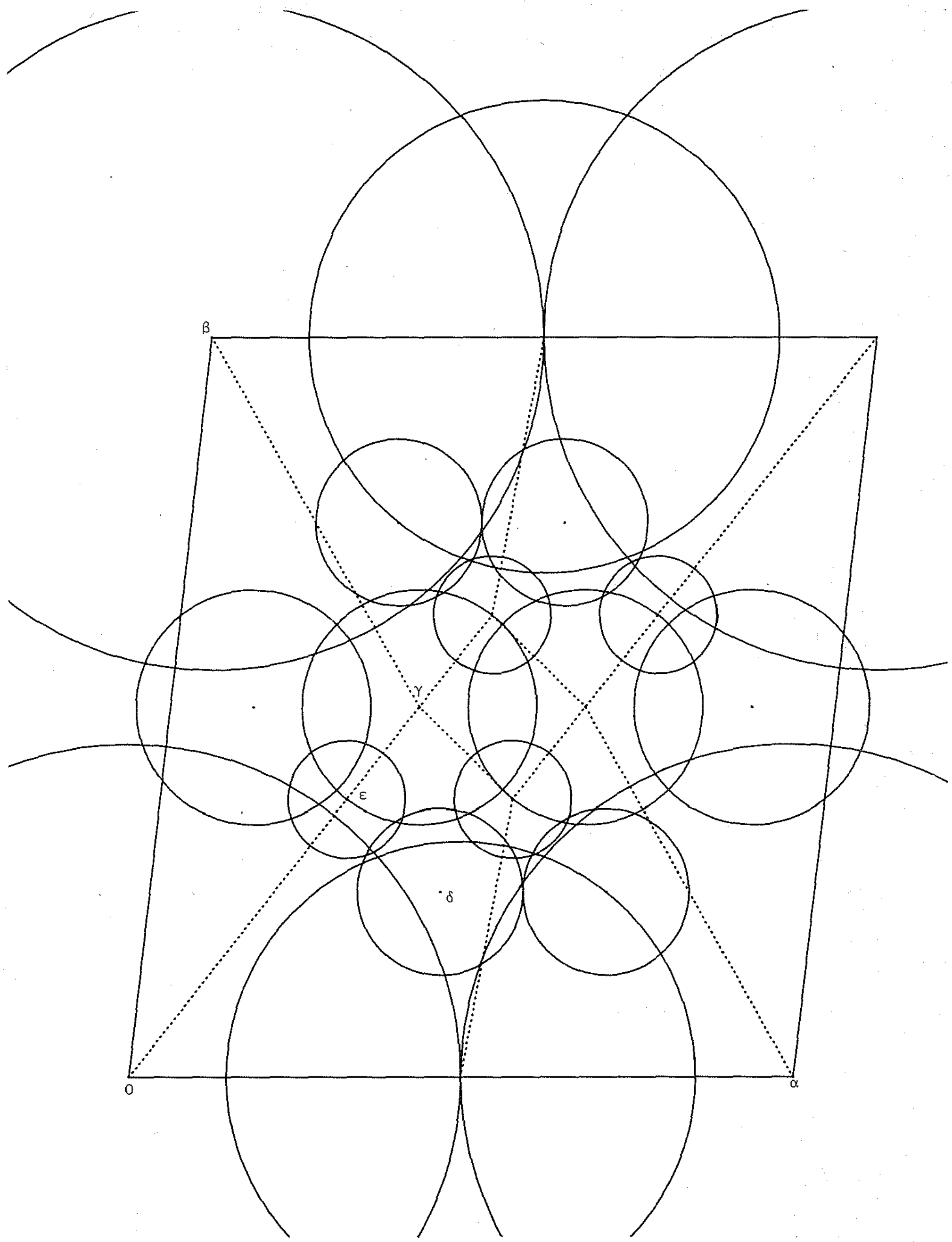


fig. 21

First we have the region with vertices 0, $\frac{1}{2}\alpha$, $\varepsilon + \frac{1}{4}\alpha$ and γ. By adding the lines from δ to the vertices of this region and to ε we obtain triangular regions for which (9.5) may be used. Similarly we may treat the mirror image of this region in the point $\frac{1}{2}(\alpha+\beta)$. Next we have the region with vertices $\frac{1}{2}\alpha$, α, $\gamma + \frac{1}{4}\alpha$ and $\varepsilon + \frac{1}{4}\alpha$. By adding the lines from $\delta + \frac{1}{4}\alpha$ to the vertices of this region we obtain triangular regions for which (9.5) may be used. Similarly we may treat the mirror image of this region in the point $\frac{1}{2}(\alpha+\beta)$. Next we have the region with vertices γ, $\varepsilon + \frac{1}{4}\alpha$, $\gamma + \frac{1}{4}\alpha$ and $\frac{3}{4}\alpha + \beta - \varepsilon$. By adding the diagonal from γ to $\gamma + \frac{1}{4}\alpha$ we obtain two triangular regions for which (9.5) may be used. Finally we are left with two triangular regions with vertices 0, γ and β resp. α, $\gamma + \frac{1}{4}\alpha$ and $\alpha + \beta$. They are mirror images of each other in the point $\frac{1}{2}(\alpha+\beta)$, hence we only have to treat the first of these regions. By adding the lines from $\gamma - \frac{1}{4}\alpha$ to the vertices of this region and to ε we obtain triangular regions for which (9.5) may be used, except for the region with vertices 0, $\gamma - \frac{1}{4}\alpha$ and β. This triangle may be treated by observing that the intersection points of the line from 0 to β with the circle around γ with radius $\sqrt{32}$ are strictly inside the circles around 0 and β respectively with radius $\sqrt{256}$.

<u>EXAMPLE (9.10)</u>. $\Delta = -23$; $Np = 233$, cf. fig. 22. Write $\omega = \frac{1}{2}(1+\sqrt{-23})$. We have $p = \mathbb{Z}\cdot 233 + \mathbb{Z}\cdot(103+\omega)$. We choose $b = \mathbb{Z}\cdot\alpha + \mathbb{Z}\cdot\beta$, with $\alpha = 32 - 11\omega$ and $\beta = 22 + 7\omega$, cf. fig. 22. We have $Nb = 466$. We will show that $\mathbb{C} = W_1(b) \cup W_1(bp^{-1})$. For this it suffices to show that $F \subset W_1(b) \cup W_1(bp^{-1})$, where F is the parallelogram with vertices 0, α, β and $\alpha+\beta$. This example can be treated in a way that is easier than the previous examples.

The discs with radii $\sqrt{466}$ and centres at 0, α, β and $\alpha+\beta$ cover almost all of F. These discs are part of $W_1(b)$. The strip $S = \{x \in \mathbb{C} : |\mathrm{Im}(x+2\omega)| < 1\}$ is completely contained in $W_1(bp^{-1})$. We will show that the part of F that is not contained in $W_1(b)$ is completely contained in S. Using the symmetry obtained by reflecting in $\frac{1}{2}(\alpha+\beta)$ we only have to show that

(a) $|\mathrm{Im}(z_1+2\omega)| < 1$, where z_1 is the intersection inside F of the circles with radii $\sqrt{466}$ and centres at 0 and α;

(b) $|\mathrm{Im}(z_2+2\omega)| < 1$, where z_2 is the intersection inside F of the circles with radii $\sqrt{466}$ and centres at 0 and β.

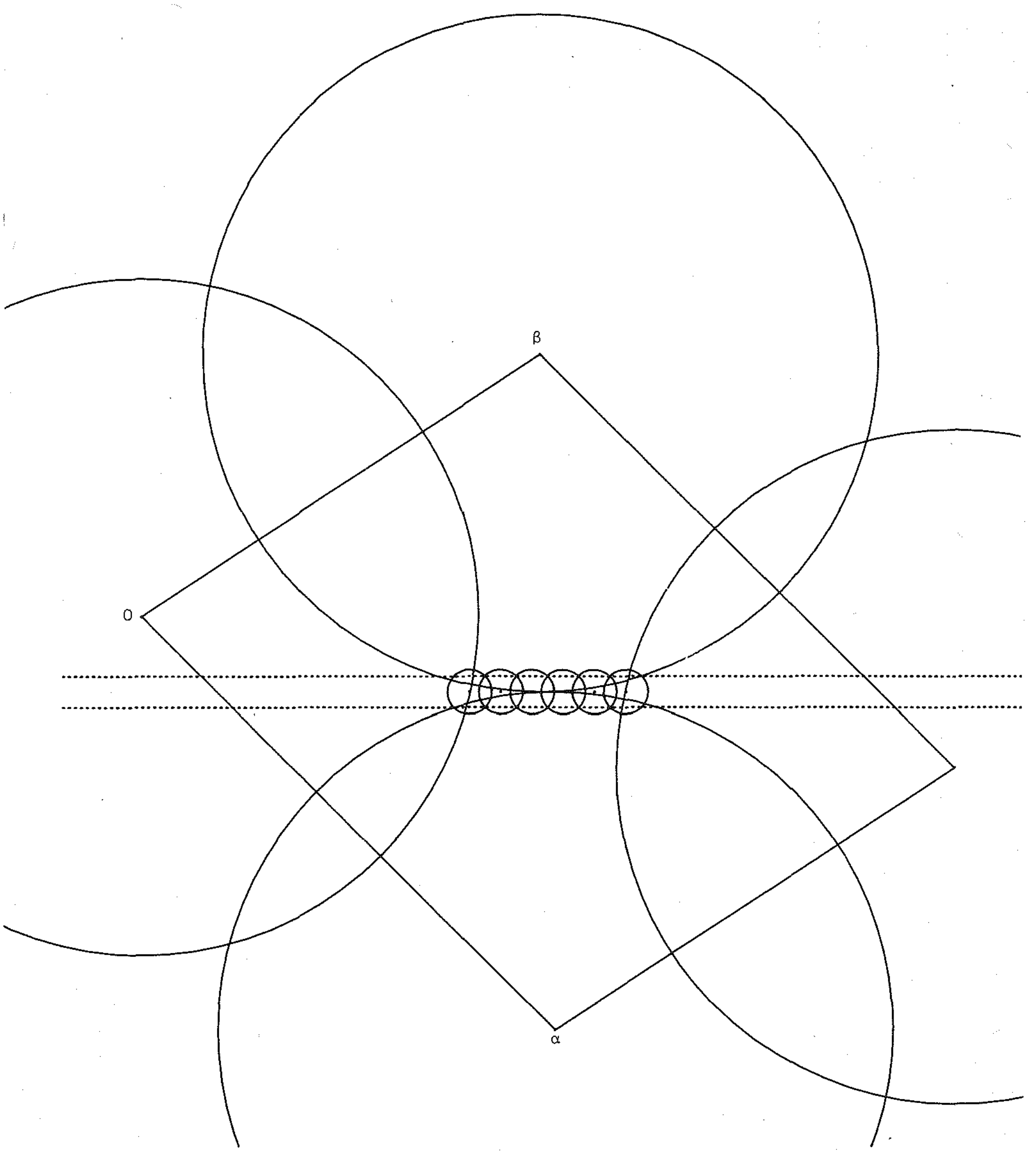


fig. 22

For (a) we have $z_1 = (\frac{1}{2}+\frac{1}{6}\sqrt{-3})\alpha = 22.02 - 2.31\omega$, hence $|\mathrm{Im}(z_1 + 2\omega)| = 0.74 < 1$.
For (b) we have $z_2 = \frac{1-i}{2}\beta = 22.05 - 1.82\omega$, hence $|\mathrm{Im}(z_2 + 2\omega)| = 0.44 < 1$.

TABLE 18. Rings with a Euclidean ideal class.

Δ	*Np*	*b*	n	Δ	*Np*	*b*	n
-19	4	(1,1,5)	1	-31	2	(1,1,8)	1
-23	2	(2,-1,3)	1		5	(2,-1,4)	2
	3	(2,-1,3)	1		7	(2,1,4)	3
	13	(2,-1,3)	1	-35	4	(3,1,3)	1
	29	(2,-1,3)	1		5	(3,1,3)	1
	31	(2,-1,3)	1		7	(3,1,3)	1
	41	(2,-1,3)	1		11	(3,1,3)	1
	47	(2,-1,3)	2	-39	2	(2,-1,5)	1
	71	(2,-1,3)	1	-40	2	(2,0,5)	2
	73	(2,-1,3)	1	-47	2	(3,-1,4)	3
	127	(2,-1,3)	1		3	(3,-1,4)	5
	131	(2,-1,3)	1	-55	2	(2,-1,7)	4
	163	(2,-1,3)	1	-56	2	(3,2,5)	2
	193	(2,-1,3)	1	-68	2	(3,2,6)	3
	233	(2,-1,3)	1	-71	2	(2,1,9)	8
	239	(2,-1,3)	2		3	(2,1,9)	9
	257	(2,-1,3)	3	-79	2	(4,1,5)	5
	353	(2,-1,3)	3	-84	2	(5,4,5)	3
	443	(2,-1,3)	1	-87	2	(4,3,6)	11
	487	(2,-1,3)	1	-111	2	(3,3,10)	6
-24	2	(1,0,6)	1	-136	2	(5,2,7)	7
	5	(2,0,3)	1				
	7	(2,0,3)	1				
	29	(2,0,3)	2				

Table 18 lists the 45 rings that have a Euclidean ideal class. It gives an ideal b and an integer $n \in \mathbb{Z}_{>0}$, such that $\mathbb{C} = \bigcup_{i=0}^{n} W_1(bp^{-i})$. For the ideal b only the reduced quadratic form is given, because the proof works for each b corresponding to this quadratic form. If there are two primes of $\mathcal{O}$ with the given norm, we always used that one for which the reduced quadratic form (a,b,c) has $b \geq 0$. If this does not distinguish between the primes one of them is picked at random. In all cases pictures like figures 18 - 22 can be drawn and corresponding proofs can be given. However it may occur, e.g. if $\Delta = -23$ and $N\mathfrak{p} = 353$, that the relative sizes of the largest and the smallest circles differ too much. In these cases one may first draw the largest circles in the picture and enlarge several regions in which the smallest circles may be drawn. Only in a few cases we may speed up the argument by using an argument like (9.10).

This finishes the proof of case (#2$^-$) of (0.19) and (1.10). Only the class number bounds for the cases (#3) and (#4) remain to be proven. This will be done in the next chapter.

CHAPTER 10 CUBIC AND QUARTIC FIELDS

In chapters 6 - 9 we completely determined all rings with a Euclidean ideal class in the case $(\#2^-)$. In the present chapter we consider the cases $(\#3)$ and $(\#4)$. We do not obtain a complete determination of the rings with a Euclidean ideal class. This is mainly due to the fact that in these cases the upper bounds for the discriminants in (5.19) are prohibitively large.

In section (10.1) we obtain restrictions on the class group of $\mathcal{O}(K)$ if there is a Euclidean ideal class. These restrictions are stronger than those proved in (2.5) and (2.9). As a diversion from our main topic we prove that all cyclotomic fields for which the ring of integers has a Euclidean ideal class are contained in a given set of 32 fields.

In sections (10.2) and (10.3) we improve the discriminant bounds of (5.19) for quadratic extensions of quadratic fields. In sections (10.4) and (10.5) we apply these results to quartic fields that are Galois extensions of $\mathbb{Q}$. We find that for these fields we have $h(K) \leq 2$ if $\mathcal{O}(K)$ has a Euclidean ideal class. For the case that $Gal(K/\mathbb{Q})$ is cyclic we find that precisely two rings of integers have a Euclidean ideal class.

Finally in section (10.6) we give a list of known rings in the cases $(\#3)$ and $(\#4)$ that have a Euclidean ideal class.

§(10.1) Bounds on the class number

Let A be the ring of integers of a number field K. Suppose that A has a Euclidean ideal class. We will prove that $h(A) \leq 4$ if K is a cubic field and that $h(A) \leq 6$ if K is a quartic field. If K is a quadratic extension of a number field K_0 we will prove that $\mathrm{Index}[Cl(A) : \iota Cl(\mathcal{O}(K_0))] \leq 2$, where ι is the natural map $\iota : Cl(\mathcal{O}(K_0)) \to Cl(A)$. This is a generalization of (2.12). For certain quartic fields this is an extra restriction on the class group. The same result can be used to show that we must have $h(K) \leq 2$ if K is a cyclotomic field.

<u>THEOREM (10.1)</u>. *Let* $K/\mathbb{Q}$ *be a cubic extension. Suppose that* $A = \mathcal{O}(K)$ *has a Euclidean ideal class, then*

(i) $h(A) \le 4$;

(ii) *if all primes over* 2 *have norm* 2 , *then we have* $h(A) \mid 3$;

(iii) *if there is no ideal of norm* 3, *then we have* $h(A) \le 3$.

<u>PROOF</u>. We distinguish between the possible prime decompositions of $2A$. Let $[\mathfrak{a}]$ be a Euclidean ideal class of A.
(a) Suppose that $2A = \mathfrak{p}\mathfrak{q}\mathfrak{r}$, with $N\mathfrak{p} = N\mathfrak{q} = N\mathfrak{r} = 2$. Then $[\mathfrak{p}] = [\mathfrak{q}] = [\mathfrak{r}] = [\mathfrak{a}]$ by (2.3), hence $[\mathfrak{a}]^3 = [A]$ and $h(A) \mid 3$.
(b) Suppose that $2A = \mathfrak{p}\mathfrak{q}$, with $N\mathfrak{p} = 2$ and $N\mathfrak{q} = 4$. Then $[\mathfrak{p}] = [\mathfrak{a}]$ by (2.3) and $[\mathfrak{q}] = [\mathfrak{a}]^{-1}$. From (2.9) we derive that $[\mathfrak{q}] = [\mathfrak{a}]^{\ell}$ with $1 \le \ell \le 3$, hence $h(A) \mid \ell+1 \le 4$. If there is no ideal of norm 3 we even have $\ell \le 2$, hence $h(A) \le 3$.
(c) Finally suppose that $2A$ is prime. From (2.9) we derive that $[2A] = [\mathfrak{a}]^{\ell}$ with $1 \le \ell \le 4$, hence $h(A) \mid \ell \le 4$. If there is no ideal of norm 3 we even have $\ell \le 3$, hence $h(A) \le 3$. □

<u>THEOREM (10.2)</u>. *Suppose* $[K:\mathbb{Q}] = 4$. *If* $A = \mathcal{O}(K)$ *has a Euclidean ideal class we must have*

(i) $h(A) \le 6$, *and if* $h(A) = 6$ *there is a prime of norm* 7 ;

(ii) *if all primes over* 2 *have norm* 2, *then* $h(A) \mid 4$;

(iii) *if all primes over* 2 *have norm* 4, *then* $h(A) \le 4$;

(iv) *if* $K/\mathbb{Q}$ *is a Galois extension, then* $h(A) \mid 4$.

<u>REMARK (10.3)</u>. With different techniques we show in sections (10.4) and (10.5) that (iv) may be improved to $h(A) \mid 2$.

<u>PROOF</u>. Part (iv) follows directly from (2.11). To prove parts (i) - (iii) we distinguish between the possible prime decompositions of $2A$ and $3A$. Let $[\mathfrak{a}]$ be a Euclidean ideal class of A.

(a) Suppose that $2A = \mathfrak{pqrs}$, with $N\mathfrak{p} = N\mathfrak{q} = N\mathfrak{r} = N\mathfrak{s} = 2$. Then $[\mathfrak{p}] = [\mathfrak{q}] = [\mathfrak{r}] = [\mathfrak{s}] = [\mathfrak{a}]$ by (2.3), hence $[\mathfrak{a}]^4 = [A]$ and $h(A)|4$.

(b) Suppose that $2A = \mathfrak{pqr}$, with $N\mathfrak{p} = N\mathfrak{q} = 2$ and $N\mathfrak{r} = 4$. Then $[\mathfrak{p}] = [\mathfrak{q}] = [\mathfrak{a}]$ by (2.3) and $[\mathfrak{r}] = [\mathfrak{a}]^{-2}$. From (2.9) we derive that $[\mathfrak{r}] = [\mathfrak{a}]^{\ell}$ with $1 \le \ell \le 3$, hence $h(A) \le 5$.

(c) Suppose that $2A = \mathfrak{pq}$, with $N\mathfrak{p} = 2$ and $N\mathfrak{q} = 8$. Then $[\mathfrak{p}] = [\mathfrak{a}]$ and $[\mathfrak{q}] = [\mathfrak{a}]^{-1}$. Using (2.1) repeatedly we derive that $[\mathfrak{q}] = [\mathfrak{a}]^{\ell}$ with $1 \le \ell \le 5$, hence $h(A) \le 6$. If there is no ideal of norm 7 we even have $\ell \le 4$, hence $h(A) \le 5$.

(d) Suppose that $2A = \mathfrak{pq}$, with $N\mathfrak{p} = N\mathfrak{q} = 4$. From (2.9) we derive that $[\mathfrak{p}] = [\mathfrak{a}]^m$ and $[\mathfrak{q}] = [\mathfrak{a}]^n$ with $m, n \in \{1,2\}$, hence $h(A)|m+n \le 4$.

(e) Suppose that $2A$ is prime and $3A = \mathfrak{pqrs}$, with $N\mathfrak{p} = N\mathfrak{q} = N\mathfrak{r} = N\mathfrak{s} = 3$. Then $[\mathfrak{p}] = [\mathfrak{q}] = [\mathfrak{r}] = [\mathfrak{s}] = [\mathfrak{a}]$ and $h(A)|4$.

(f) Suppose that $2A$ is prime and $3A = \mathfrak{pqr}$, with $N\mathfrak{p} = N\mathfrak{q} = 3$ and $N\mathfrak{r} = 9$. Then $[\mathfrak{p}] = [\mathfrak{q}] = [\mathfrak{a}]$ and $[\mathfrak{r}] = [\mathfrak{a}]^{-2}$. From (2.9) we derive that $[\mathfrak{r}] = [\mathfrak{a}]^{\ell}$ with $1 \le \ell \le 4$, hence $h(A) \le 6$. If there is no prime of norm 7 we even have $\ell \le 3$, hence $h(A) \le 5$.

(g) Suppose that $2A$ is prime and $3A = \mathfrak{pq}$, with $N\mathfrak{p} = 3$ and $N\mathfrak{q} = 27$, then $[\mathfrak{p}] = [\mathfrak{a}]$. Using (2.1) repeatedly we find that $[2A] = [\mathfrak{a}]^{\ell}$ with $1 \le \ell \le 6$, hence $h(A) \le 6$. If there is no prime of norm 7 we even have $\ell \le 5$, hence $h(A) \le 5$.

(h) Suppose that $2A$ is prime and $3A = \mathfrak{pq}$, with $N\mathfrak{p} = N\mathfrak{q} = 9$. From (2.9) we derive that $[\mathfrak{p}] = [\mathfrak{a}]^m$ and $[\mathfrak{q}] = [\mathfrak{a}]^n$, with $1 \le m, n \le 3$, hence $h(A)|m+n \le 6$. If there is no prime of norm 7 we even have $m, n \le 2$, hence $h(A) \le 4$.

(i) Finally suppose that $2A$ and $3A$ are prime. Then we may use (2.9) to derive that $h(A) \le 5$. □

<u>REMARK (10.4)</u>. Notice that the bounds of (10.1) and (10.2) are better than those that may be derived directly from (2.9), which are 6 and 10 respectively. Also if we have information about the splitting of 2A, 3A, 5A, 7A, 11A and 13A we may get better bounds on $h(A)$ by inspecting the proofs of (10.1) and (10.2).

The bounds on the class numbers in (1.10) (#3) and (#4) are implied by theorems (10.1) and (10.2). This finishes the proof of (1.10).

PROPOSITION (10.5). *Let* K/K_0 *be a quadratic extension and let* $\iota : Cl(\mathcal{O}(K_0)) \to Cl(\mathcal{O}(K))$ *be the map given by* $\iota([a]) = [a\mathcal{O}(K)]$. *If* $\mathcal{O}(K)$ *has a Euclidean ideal class, then*

$$\mathrm{Index}[Cl(\mathcal{O}(K)) : \iota Cl(\mathcal{O}(K_0))] \leq 2.$$

PROOF. Essentially this is the same proof as that of (2.12). Let σ be the generator of $Gal(K/K_0)$. If a is an $\mathcal{O}(K)$-ideal of least norm $\neq 1$, then a is Euclidean by (2.3). Also σa is Euclidean, hence $[a] = [\sigma a]$. This shows that $[a]^2 = [a\sigma a] \in \iota Cl(\mathcal{O}(K_0))$. Because $Cl(\mathcal{O}(K))$ is generated by $[a]$ we get $\mathrm{Index}[Cl(\mathcal{O}(K)) : Cl(\mathcal{O}(K_0))] \leq 2$. □

As a corollary of (10.5) we get a finite list of cyclotomic fields, that contain all those fields that have a Euclidean ideal class. For the definition of ζ_m see section (0.1).

PROPOSITION (10.6). *Let* $m \in \mathbb{Z}_{>0}$ *be such that* $m \not\equiv 2 \bmod 4$. *If the cyclotomic field* $\mathbb{Q}(\zeta_m)$ *has a Euclidean ideal class then* $h(\mathbb{Q}(\zeta_m)) \leq 2$, *and this occurs only for*

$$m = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21,$$
$$24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84,$$

for which $h(\mathbb{Q}(\zeta_m)) = 1$, *and for*

$$m = 39, 56,$$

for which $h(\mathbb{Q}(\zeta_m)) = 2$.

PROOF. Write $K = \mathbb{Q}(\zeta_m)$ and $K_0 = K \cap \mathbb{R}$. Using (10.5) we find that $h^- \leq 2$, where h^- is defined by $h(K) = h^- \cdot h(K_0)$. Masley has shown that this implies that $h(K_0) = 1$, cf. [M2], Main theorem. In particular we have $h(K) \leq 2$. The same theorem of Masley shows that $h(K) = 2$ if and only if $m = 39$ or $m = 56$. Together with Montgomery [MM] he proved that $h(K) = 1$ if and only if m is one of the other given values. □

In section (0.6) we have seen that for 13 values of m, i.e. $m \in \{1,3,4,5,7,8,9,11,12,15,16,20,24\}$, the ring of integers is Euclidean. Furthermore it can be shown that for $m = 32$ the ring of integers is not Euclidean, cf. [L6]. For the remaining 18 rings the existence of a Euclidean ideal class remains undecided.

§(10.2) Quadratic extensions of imaginary quadratic fields

This section and the subsequent three are devoted to quartic fields that have a quadratic subfield. We begin by establishing the notation to be used.

By K_0 we denote a quadratic extension of $\mathbb{Q}$ and by K a totally imaginary quadratic extension of K_0. The rings of integers of K_0 and K are denoted by A_0 and A respectively. The element and ideal norms of K_0 with respect to S_∞ are denoted by N_0, those of K with respect to S_∞ by N, cf. (0.14) and (0.15).

Let σ be the generator of $\mathrm{Gal}(K/K_0)$. For an element α of K_0 the relative norm $\tilde{N}(\alpha)$ is given by $\tilde{N}(\alpha) = \alpha\cdot\sigma\alpha \in K_0$. The relative ideal norm $\tilde{N}\mathfrak{a}$ of an A-ideal is given by $\tilde{N}\mathfrak{a} = \mathfrak{a}\cdot\sigma\mathfrak{a} \cap K_0$. We have $N = N_0 \circ \tilde{N}$, cf. [CF] ch.II app.A. The element norm, as defined by (1.7), will be denoted by $\mathcal{N}$ for K and $\mathcal{N}_0$ for K_0 respectively. We have $\mathcal{N} = \mathcal{N}_0 \circ \tilde{N}$. Notice that $N = \mathcal{N}$ because K is totally complex.

The relative different $\mathcal{D}(K/K_0)$ of K/K_0 is the A-ideal defined by

$$\mathcal{D}(K/K_0)^{-1} = \{x \in K : \mathrm{Tr}(x\alpha) \in A_0 \text{ for all } \alpha \in A\},$$

where $\mathrm{Tr} : K \to K_0$ is the trace function. The relative discriminant $\Delta(K/K_0)$ is defined to be $\tilde{N}(\mathcal{D}(K/K_0))$, cf. [W] 4-8-11. If Δ is the discriminant of K and Δ_0 is the discriminant of K_0 we have a product formula

$$\Delta = N_0(\Delta(K/K_0))\cdot\Delta_0^2 \tag{10.7}$$

cf. [W] 4-8-12.

In the rest of this section we take K_0 to be an *imaginary* quadratic field. Let $S = S_\infty$ be the set of archimedean primes of K, and $|\cdot|_1$ and $|\cdot|_2$ the two normalized valuations in S, cf. (1.2) (c). When restricted to K_0 the two valuations $|\cdot|_1$ and $|\cdot|_2$ coincide with the archimedean valuation $|\cdot|_\infty$ of K_0. The ring K_S is isomorphic to $\mathbb{C}\times\mathbb{C}$, cf. (3.13). As before we regard K as being embedded along the diagonal in K_S. The subfield K_0 lies dense in the plane $\{(x,x) \in \mathbb{C} \times \mathbb{C} : x \in \mathbb{C}\}$.

As we have seen in section (3.6) every A-ideal is a lattice in K_S. For every A-ideal $\mathcal{C}$ we will construct $\bar{x} \in K_S/\mathcal{C}$, such that for each $x \in \bar{x}$ we have $N(x) \geq M \cdot N\mathcal{C}$ for some $M \in \mathbb{R}_{>0}$ that tends to ∞ with $\max\{|\Delta_0|, N_0(\Delta(K/K_0))\}$. As in section (5.4) this will lead to an upperbound on Δ if A has a Euclidean ideal class. The new bound is better than that of Cassels, cf. (5.19) (#4), but for $|\Delta_0| \to \infty$ it approaches Cassels' bound.

For the remainder of this section we take an A_0-ideal $\mathcal{a}$ fixed. For our applications the choice $\mathcal{a} = A_0$ will be sufficient. For $x \in \mathbb{C}$ we define

$$(10.8) \qquad \|x\| = \min\{|x-\alpha|_\infty : \alpha \in \mathcal{a}\}.$$

Notice that $\|x\| \leq \rho N_0 \mathcal{a}$ for all $x \in \mathbb{C}$, where ρ is the covering radius of $\mathcal{a}$, cf. (3.4).

Let $Tr : K \longrightarrow K_0$ be the trace function. We extend it to $Tr : K_S = \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ by $Tr((x_1,x_2)) = x_1 + x_2$ for $(x_1,x_2) \in \mathbb{C} \times \mathbb{C}$.

For an A-ideal $\mathcal{C}$ we define the *polar* $\mathcal{C}^\wedge$ with respect to $\mathcal{a}$ by

$$(10.9) \qquad \mathcal{C}^\wedge = \{x \in K_S : Tr(x\gamma) \in \mathcal{a} \text{ for all } \gamma \in \mathcal{C}\}.$$

Notice the resemblance with $\mathcal{C}^\perp$, cf. (3.17). Using the results of [W] §4-8 it can be shown that $\mathcal{C}^\wedge = \mathcal{a}\mathcal{C}^{-1}\mathcal{D}(K/K_0)^{-1}$. This shows that the determinants satisfy

$$(10.10) \qquad \nu(\mathcal{C})\nu(\mathcal{C}^\wedge) = N_0\mathcal{a}^2 N\mathcal{D}(K/K_0)^{-1}\Delta = N_0\mathcal{a}^2 \cdot |\Delta_0|^2,$$

cf. (3.18), (3.21), (3.22) and (10.7).

<u>PROPOSITION (10.11)</u>. *Let* $k \in \mathbb{R}_{>1}$ *and let* $(\alpha_n)_{n \in \mathbb{Z}}$ *be a sequence in* $\mathcal{C}^\wedge$ *satisfying (5.7) with* k *replaced by* k^2, *i.e.*

(a) $\qquad |\alpha_n|_1 \leq k^{-2}|\alpha_{n-1}|_1$ *for all* $n \in \mathbb{Z}$;

(b) $\qquad |\alpha_n|_2|\alpha_{n-1}|_1 \leq \frac{2k^2}{\pi\sqrt{3}}\nu(\mathcal{C}^\wedge)$ *for all* $n \in \mathbb{Z}$;

(c) $\qquad \lim_{n\to\infty} |\alpha_n|_1 = \lim_{n\to-\infty} |\alpha_n|_2 = 0$;

(d) $$\lim_{n\to-\infty} |\alpha_n|_1 = \lim_{n\to\infty} |\alpha_n|_2 = \infty .$$

Then there exists $\bar{x} \in K_S/\mathcal{C}$ *such that for all* $x \in \bar{x}$ *we have*

(10.12) $$\|\mathrm{Tr}(x\alpha_n)\| \geq \rho N_0 a\left(\frac{k-2}{k-1}\right)^2 \quad \textit{for all} \quad n \in \mathbb{Z} .$$

PROOF. By the definition of $\mathcal{C}^\wedge$ we have $\mathrm{Tr}(\gamma\alpha_n) \in a$ for all $\gamma \in \mathcal{C}$. Thus, because Tr is additive, the value of $\|\mathrm{Tr}(x\alpha_n)\|$ does not depend on the choice of $x \in \bar{x}$. Because $K_S/\mathcal{C}$ is compact it suffices to construct, for each pair $m_1, m_2 \in \mathbb{Z}$, an element $x \in K_S$ such that (10.12) holds for all $n \in \mathbb{Z}$ with $m_1 \leq n \leq m_2$. Shifting the indices we may suppose that $m_2 = 0$ and $m_1 = m \leq 0$. Hence it suffices to prove, by induction on $m \in \mathbb{Z}_{\leq 0}$, that there exists $x_m \in K_S$ such that

(10.13) $$\|\mathrm{Tr}(x_m\alpha_n)\| \geq \rho N_0 a\left(\frac{k-2+k^{m-n}}{k-1}\right)^2 \quad \text{if} \quad m \leq n \leq 0.$$

Because Tr is surjective we can find $x_0 \in K_S$, such that (10.13) holds for $m = 0$. Now suppose that $m < 0$. From (3.4) we derive that there exists $y \in \mathbb{C}$ such that $|y|_\infty \leq \rho N_0 a$ and $\|\mathrm{Tr}(x_{m+1}\alpha_m) + y\| = \rho N_0 a$. Take $x_m = x_{m+1} + (y,0)\alpha_m^{-1} \in K_S$. Then (10.13) holds for $n = m$ by construction. If $m < n \leq 0$ we have

$$\begin{aligned}
\|\mathrm{Tr}(x_m\alpha_n)\| &= \| \mathrm{Tr}(x_{m+1}\alpha_n) + \mathrm{Tr}((y,0)\alpha_n\alpha_m^{-1}) \| \geq \\
&\geq (\| \mathrm{Tr}(x_{m+1}\alpha_n)\|^{\frac{1}{2}} - |y|_\infty^{\frac{1}{2}}|\alpha_n\alpha_m^{-1}|_1^{\frac{1}{2}})^2 \geq \\
&\geq \rho N_0 a\left(\frac{k-2+k^{m-n+1}}{k-1} - k^{m-n}\right)^2 = \\
&= \rho N_0 a\left(\frac{k-2+k^{m-n}}{k-1}\right)^2. \quad \square
\end{aligned}$$

PROPOSITION (10.14). *Let* $(\alpha_n)_{n\in\mathbb{Z}}$ *be a sequence in* $\mathcal{C}^\wedge$ *such that the conditions of (10.11) hold and let* $\bar{x} \in K_S/\mathcal{C}^\wedge$ *be such that (10.12) holds. Then for all* $x \in \bar{x}$ *we have*

$$N(x) \geq \frac{\pi\sqrt{3}}{2}\left(\frac{k-2}{k^2-1}\right)^4 k^2\rho^2|\Delta_0|^{-2}|\Delta|^{\frac{1}{2}}\cdot N\mathcal{C} .$$

PROOF. Take $x \in \bar{x}$. As in (5.13) we derive from (10.11)(c) and (d) and (10.12) that $N(x) \neq 0$. Hence there exists $n \in \mathbb{Z}$ such that

$$|\alpha_n x|_1 \leq (\frac{2k^2}{\pi\sqrt{3}} \nu(c^\wedge)N(x))^{\frac{1}{2}} < |\alpha_{n-1}x|_1 .$$

From (10.11)(b) we derive that

$$|\alpha_n x|_2 \leq (\frac{2k^2}{\pi\sqrt{3}} \nu(c^\wedge)N(x))^{\frac{1}{2}} .$$

Multiplying (10.11)(a) by (10.11)(b) gives

$$|\alpha_n x|_1 |\alpha_n x|_2 \leq \frac{2}{\pi\sqrt{3}} \nu(c^\wedge)N(x).$$

Hence, using (5.14), we get

$$|\alpha_n x|_1^{\frac{1}{2}} + |\alpha_n x|_2^{\frac{1}{2}} \leq (\frac{2}{\pi\sqrt{3}} \nu(c^\wedge)N(x))^{\frac{1}{4}} k^{-\frac{1}{2}}(k+1).$$

Because

$$\rho N_0 a(\frac{k-2}{k-1})^2 \leq \| \mathrm{Tr}(x\alpha_n) \| \leq (|\alpha_n x|_1^{\frac{1}{2}} + |\alpha_n x|_2^{\frac{1}{2}})^2$$

we get

$$\rho^2 N_0 a^2 (\frac{k-2}{k-1})^4 \leq \frac{2}{\pi\sqrt{3}} \nu(c^\wedge)N(x)k^{-2}(k+1)^4.$$

Combining this with (10.10), (3.21), (3.22) and (10.7) gives

$$N(x) \geq \frac{\pi\sqrt{3}}{2} \rho^2 \left(\frac{k-2}{k^2-1}\right)^4 k^2 |\Delta_0|^{-2} \nu(c) =$$

$$= \frac{\pi\sqrt{3}}{2} \rho^2 \left(\frac{k-2}{k^2-1}\right)^4 k^2 |\Delta_0|^{-2} |\Delta|^{\frac{1}{2}} Nc. \quad \square$$

As in (5.19) we may derive an upper bound for $N_0(\Delta(K/K_0))$ if A has a Euclidean ideal class. This upper bound will be better if ρ is larger. The largest value of ρ is obtained by taking $a = A_0$.

THEOREM (10.15). *Let* K_0 *be an imaginary quadratic field of discriminant* Δ_0, *and* K *a quadratic extension of* K_0 *with discriminant* Δ *over* $\mathbb{Q}$. *Suppose that* $A = \mathcal{O}(K)$ *has a Euclidean ideal class. Then*

$$\Delta \le \kappa \cdot r(\Delta_0),$$

with $\kappa = 230202117.8$ *and*

$$r(\Delta_0) = \begin{cases} \left(\frac{|\Delta_0|}{|\Delta_0|+1}\right)^8 & \text{if } \Delta_0 \text{ is odd} \\ \left(\frac{|\Delta_0|}{|\Delta_0|+4}\right)^4 & \text{if } \Delta_0 \text{ is even.} \end{cases}$$

PROOF. We take $\mathfrak{a} = A_0$, then $\rho = \frac{1}{16}|\Delta_0| r(\Delta_0)^{-\frac{1}{4}}$. If $\mathfrak{c}$ is a Euclidean ideal of A we derive from (10.14) and (5.5)(b) that

$$\frac{\pi\sqrt{3}}{2}\left(\frac{k-2}{k^2-1}\right)^4 k^2 \rho^2 |\Delta_0|^{-2} |\Delta|^{\frac{1}{2}} \le 1$$

i.e.

$$\Delta = |\Delta| \le |\Delta_0|^4 \frac{2^2}{3\pi^2} \left(\frac{k^2-1}{k-2}\right)^8 k^{-4} \rho^{-4} = \frac{2^{18}}{3\pi^2} \left(\frac{k^2-1}{k-2}\right)^8 k^{-4} r(\Delta_0).$$

As a function of k this has a minimum near $k = \frac{16567}{3000}$. For $k = \frac{16567}{3000}$ we get

$$\Delta \le r(\Delta_0) \cdot 230202117.8 \quad . \quad \square$$

REMARK (10.16). In (5.19) (#4) we found that $\Delta \le \kappa$. Since $r(\Delta_0) < 1$ our present bound is better. For even and odd Δ_0 separately $r(\Delta_0)$ is monotonically increasing to 1 for $\Delta_0 \to \infty$.

COROLLARY (10.17). *Let* K_0 *be an imaginary quadratic field of discriminant* Δ_0 *and* K *a quadratic extension field of* K_0 *of discriminant* Δ *over* $\mathbb{Q}$. *If* $A = \mathcal{O}(K)$ *has a Euclidean ideal class, then*

$$\Delta \le 229713301 ;$$

if moreover Δ_0 *is even and at least one prime ramifies in* K/K_0 *then*

$$\Delta \leq 227897232 .$$

PROOF. First suppose that K/K_0 is unramified. Let L be the normal closure of $K/\mathbb{Q}$, then also L/K_0 is unramified. Checking the various possibilities for $\mathrm{Gal}(L/\mathbb{Q})$ and using that by Minkowski's theorem ([W] 5-4-10) the inertia groups of the finite primes generate $\mathrm{Gal}(L/\mathbb{Q})$ one finds that $K = L$, $\mathrm{Gal}(K/\mathbb{Q}) = V_4$ and that at least one prime ramifies in K/K_1, where K_1 is the other imaginary quadratic subfield of K. Hence we may replace K_0 by K_1. This shows that we may assume that at least one prime ramifies in K/K_0. This implies that $h(K_0)|h(K)$, cf. [Wa] prop.4.11, hence $h(K_0) \leq 6$ by (10.2). From [Bu] we derive that for odd Δ_0 we have $|\Delta_0| \leq 3763$ and for even Δ_0 we have $|\Delta_0| \leq 1588$. By the monotonicity of $r(\Delta_0)$, cf. (10.14), we get $\Delta \leq \kappa \cdot r(-3763) = 229713301.3$ if Δ_0 is odd and $\Delta \leq \kappa \cdot r(-1588) = 227897233.7$ if Δ_0 is even. □

Table 19 lists for all $\Delta_0 > -100$, except for $\Delta_0 = -71$ upper bounds for $N_0(\Delta(K/K_0))$ and Δ in the case that A has a Euclidean ideal class.

TABLE 19. Upper bounds for the discriminant Δ of a quadratic extension of $\mathbb{Q}(\sqrt{\Delta_0})$, for which the ring of integers has a Euclidean ideal class.

Δ_0	$N_0(\Delta(K/K_0)) \leq$	$\Delta \leq$	Δ_0	$N_0(\Delta(K/K_0)) \leq$	$\Delta \leq$
-3	2560684	23046156	-47	88056	194515704
-4	899225	14387600	-51	75769	197075169
-7	1614272	79099328	-52	63293	171144272
-8	710492	45471488	-55	65884	199299100
-11	948432	114760272	-56	55696	174662656
-15	610504	137363400	-59	57809	201233129
-19	423044	152718884	-67	45533	204397637
-20	277532	111012800	-68	39601	183115024
-23	309588	163772052	-79	33349	208131109
-24	215724	124257024	-83	30333	208964037
-31	185797	178550917	-84	1	7056
-35	149969	183712025	-87	27756	210085164
-39	123596	187989516	-88	24884	192701696
-40	98249	157198400	-91	25469	210908789
-43	103568	191497232	-95	23448	211618200

These bounds are derived from (10.15) and (10.7). We have not included $\Delta_0 = -71$, because in this case we have $h(K_0) = 7$, hence $7|h(K)$, which implies that A has no Euclidean ideal class, cf. (10.2)(i). The bounds on $N_0(\Delta(K/K_0))$ are rounded downwards, keeping in mind that $N_0(\Delta(K/K_0)) \equiv \equiv 0,1 \bmod 4$ and $v_p(\Delta(K/K_0)) \leq 1$ if p is an odd prime of K, cf. [Ma] app.II and [CF] Ch.I §5 thm.2. Notice that for $\Delta_0 = -84$ we have $N_0(\Delta(K/K_0)) \leq 1$. This follows because if $N_0(\Delta(K/K_0)) > 1$ we have by class field theory that $N : Cl(A) \longrightarrow Cl(A_0)$ is surjective, but in this case $Cl(A_0) \simeq V_4$, which is not an image of a cyclic group of order ≤ 6.

§(10.3) Quadratic extensions of real quadratic fields

In this section we use the notation established at the beginning of section (10.2). In contrast to section (10.2) we take K_0 to be a *real* quadratic field, and we assume that K is a *totally complex* quadratic extension of K_0. Let $S = S_\infty$ be the set of archimedean primes of K and let $|\cdot|_1$ and $|\cdot|_2$ be the normalized valuations in S, cf. (1.2). The restrictions of $|\cdot|_1$ and $|\cdot|_2$ to K_0 give the squares of the normalized archimedean valuations of K_0. As in chapter 3 we regard K as being embedded along the diagonal in $K_S = \mathbb{C} \times \mathbb{C}$. The subfield K_0 lies dense in the plane $\mathbb{R} \times \mathbb{R} \subset \mathbb{C} \times \mathbb{C}$.

The determinant of a lattice Γ in K_S will be denoted by $\nu(\Gamma)$, cf. (3.18). We denote the determinant of a lattice $\Gamma_r \subset \mathbb{R} \times \mathbb{R}$ with respect to the usual measure by $\nu_r(\Gamma_r)$ and that of a lattice $\Gamma_i \subset i\mathbb{R} \times i\mathbb{R}$ by $\nu_i(\Gamma_i)$. Because μ_S is 4 times the usual measure on $\mathbb{C} \times \mathbb{C}$ we get

$$\nu(\Gamma_r \times \Gamma_i) = 4\nu_r(\Gamma_r)\nu_i(\Gamma_i). \tag{10.18}$$

Let π_r denote the orthogonal projection of $\mathbb{C} \times \mathbb{C}$ onto $\mathbb{R} \times \mathbb{R}$ and let π_i denote the orthogonal projection of $\mathbb{C} \times \mathbb{C}$ onto $i\mathbb{R} \times i\mathbb{R}$. For an A-ideal $\mathfrak{a}$ we write $\mathfrak{a}_r = \mathfrak{a} \cap (\mathbb{R} \times \mathbb{R})$ and $\mathfrak{a}_i = \mathfrak{a} \cap (i\mathbb{R} \times i\mathbb{R})$.

LEMMA (10.19). *Let $\mathfrak{a}$ be an A-ideal. Then $\pi_r\mathfrak{a}$ and $\mathfrak{a}_r$ are lattices in $\mathbb{R} \times \mathbb{R}$ and $\pi_i\mathfrak{a}$ and $\mathfrak{a}_i$ are lattices in $i\mathbb{R} \times i\mathbb{R}$. Moreover*

$$\nu(\mathfrak{a}) = 4\nu_r(\mathfrak{a}_r)\nu_i(\pi_i\mathfrak{a}) = 4\nu_i(\mathfrak{a}_i)\nu_r(\pi_r\mathfrak{a}).$$

PROOF. Both $\pi_r\mathfrak{a}$ and $\mathfrak{a}_r$ are A_0-ideals, hence they are lattices in $\mathbb{R} \times \mathbb{R}$. Let $d \in K_0$ be such that $K = K_0(\sqrt{d})$, then $\sqrt{d}\cdot\mathfrak{a}_i$ and $\sqrt{d}\cdot\pi_i\mathfrak{a}$ are A_0-ideals, hence $\mathfrak{a}_i$ and $\pi_i\mathfrak{a}$ are lattices in $i\mathbb{R} \times i\mathbb{R}$. Let

F_r be a fundamental domain for $\mathfrak{a}_r$ and F_i one for $\pi_i\mathfrak{a}$. Then $F_r \times F_i$ is a fundamental domain for $\mathfrak{a}$, hence $\nu(\mathfrak{a}) = 4\nu_r(\mathfrak{a}_r)\nu_i(\pi_i\mathfrak{a})$. Similarly we can show that $\nu(\mathfrak{a}) = 4\nu_i(\mathfrak{a}_i)\nu_r(\pi_r\mathfrak{a})$. □

For a given A-ideal $\mathfrak{a}$ we will construct an element $x \in K_S$ such that $N(x-\alpha)$ is large for all $\alpha \in \mathfrak{a}$. This will be done by choosing $\pi_r(x)$ and $\pi_i(x)$ far with respect to the norm from $\pi_r\mathfrak{a}$ and $\pi_i\mathfrak{a}$ respectively. To show that x is far from $\mathfrak{a}$ we need the following lemma.

LEMMA (10.20). *Let* $x_1, x_2, y_1, y_2, a, b \in \mathbb{R}_{>0}$ *be such that*

$$x_1x_2 \geq a \quad \textit{and} \quad y_1y_2 \geq b.$$

Then

$$(x_1+y_1)(x_2+y_2) \geq (\sqrt{a}+\sqrt{b})^2.$$

PROOF. Because $(\sqrt{x_1y_2}-\sqrt{y_1x_2})^2 \geq 0$ we have

$$x_1y_2+y_1x_2 \geq 2\sqrt{x_1y_2}\sqrt{y_1x_2} \geq 2\sqrt{ab},$$

hence

$$(x_1+y_1)(x_2+y_2) = x_1x_2+y_1y_2+x_1y_2+y_1x_2 \geq$$

$$\geq a+b+2\sqrt{ab} = (\sqrt{a}+\sqrt{b})^2. \quad \square$$

LEMMA (10.21). *For any* A-*ideal* $\mathfrak{a}$ *there exists* $x \in K_S = \mathbb{C} \times \mathbb{C}$, *such that for each* $\alpha \in \mathfrak{a}$ *we have*

$$N(x-\alpha) \geq (16+6\sqrt{6})^{-2}(\nu_r(\pi_r\mathfrak{a})+\nu_i(\pi_i\mathfrak{a}))^2.$$

PROOF. Ennola ([E] thm.1) showed that there exists $x_r \in \mathbb{R} \times \mathbb{R}$ and $x_i \in i\mathbb{R} \times i\mathbb{R}$ such that for all $\beta_r \in \pi_r(\mathfrak{a})$ and all $\beta_i \in \pi_i(\mathfrak{a})$ we have

$$|x_r-\beta_r|_1|x_r-\beta_r|_2 \geq (16+6\sqrt{6})^{-2}\nu_r(\pi_r(\mathfrak{a}))^2 ;$$

$$|x_i-\beta_i|_1|x_i-\beta_i|_2 \geq (16+6\sqrt{6})^{-2}\nu_i(\pi_i(\mathfrak{a}))^2 ,$$

cf. (5.20). Take $x \in K_S$, such that $\pi_r x = x_r$ and $\pi_i x = x_i$. Because $\mathfrak{a} \subset \pi_r(\mathfrak{a}) \times \pi_i(\mathfrak{a})$ it follows from (10.20) that for each $\alpha \in \mathfrak{a}$ we have

$$N(x-\alpha) = |x-\alpha|_1 |x-\alpha|_2 \geq (16+6\sqrt{6})^{-2}(\nu_r(\pi_r(\mathfrak{a})) + \nu_i(\pi_i(\mathfrak{a})))^2.$$

□

<u>LEMMA (10.22)</u>. *Let* $\mathfrak{a}$ *be an* A*-ideal that is invariant under* $\mathrm{Gal}(K/K_0)$. *Write*

$$q(\mathfrak{a}) = (N\mathfrak{a})^{-\frac{1}{2}} \cdot N_0(\mathfrak{a}_r),$$

where $\mathfrak{a}_r = \mathfrak{a} \cap K_0$, *and*

$$\kappa = 4(16+6\sqrt{6}).$$

If $\mathfrak{a}$ *is a Euclidean* A*-ideal we have*

$$\Delta_0(q(\mathfrak{a}) + q(\mathfrak{a})^{-1}\sqrt{N_0(\Delta(K/K_0))})^2 \leq \kappa^2.$$

<u>PROOF.</u> Because $\mathfrak{a}$ is invariant under $\mathrm{Gal}(K/K_0)$ we have for all $\alpha \in \mathfrak{a}$ that

$$\pi_r(\alpha) = \tfrac{1}{2}\mathrm{Tr}(\alpha) \in \tfrac{1}{2}\mathfrak{a}_r,$$

where $\mathrm{Tr}: K \longrightarrow K_0$ is the trace function. This shows that $\nu_r(\pi_r(\mathfrak{a})) \geq$ $\geq \frac{1}{4}\nu_r(\mathfrak{a}_r)$. If $\mathfrak{a}$ is Euclidean we derive from (10.21) and (10.19) that

$$N\mathfrak{a} \geq (16+6\sqrt{6})^{-2}(\tfrac{1}{4}\nu_r(\mathfrak{a}_r) + \tfrac{1}{4}\frac{\nu(\mathfrak{a})}{\nu_r(\mathfrak{a}_r)})^2 =$$

$$= \kappa^{-2}(N_0(\mathfrak{a}_r)\sqrt{\Delta_0} + \frac{N\mathfrak{a}}{N_0(\mathfrak{a}_r)}\sqrt{N_0(\Delta(K/K_0))\cdot\Delta_0})^2,$$

i.e.

$$\kappa^2 \geq (q(\mathfrak{a}) + q(\mathfrak{a})^{-1}\sqrt{N_0(\Delta(K/K_0))}\,)^2\Delta_0. \quad \square$$

PROPOSITION (10.23). *If* A *has a Euclidean ideal that is invariant under* $Gal(K/K_0)$, *then*

$$\Delta \le 14206929.$$

PROOF. Let a be a Galois-invariant Euclidean A-ideal. From (10.22) and the inequality of the means we get

$$\kappa^2 \ge 4\sqrt{N_0(\Delta(K/K_0))\cdot\Delta_0} = 4\sqrt{\Delta}.$$

Hence $\Delta \le \kappa^4/16 = 14206929.9$. □

The bound on Δ, as given in (10.23), is more than a factor 16 better than the bound of (5.19) (#4). However, it only applies when there is a Euclidean ideal class that is invariant under $Gal(K/K_0)$.

Now we investigate for which fields (10.23) may be applied.

LEMMA (10.24). *Suppose that the prime* p *of least norm in* K_0 *ramifies in* K/K_0, *and that* A *has a Euclidean ideal class. Then this ideal class contains an ideal that is invariant under* $Gal(K/K_0)$. *We have* $N_0 p \le 4$ *and*

$$\Delta \le 14197824 \quad \textit{if} \quad N_0 p = 2\,;$$

$$\Delta \le 14197824 \quad \textit{if} \quad N_0 p = 3\,;$$

$$\Delta \le 14167696 \quad \textit{if} \quad N_0 p = 4\,.$$

PROOF. Let P be the prime ideal of A that lies over p. Then P is an integral A-ideal of least norm $\ne 1$. If A has a Euclidean ideal class, then P must be Euclidean by (2.3). Also P is invariant under $Gal(K/K_0)$. Because $NP = N_0 p$ we have $q(P) = N_0 p^{\frac{1}{2}}$. Let r be the A_0-ideal such that $\Delta(K/K_0) = p\cdot r$. Then from (10.22) we derive that

$$\Delta_0 \le \kappa^2(N_0 p^{\frac{1}{2}} + N_0 r^{\frac{1}{2}})^{-2},$$

hence

$$\Delta \le \kappa^4\left\{\left(\frac{N_0 p}{N_0 r}\right)^{\frac{1}{4}} + \left(\frac{N_0 r}{N_0 p}\right)^{\frac{1}{4}}\right\}^{-4} .$$

Because $N_0(2A_0) = 4$ we have $N_0 p \leq 4$. If $N_0 p = N_0 r = 2$ we have $\Delta_0 \leq 1884$ and $\Delta \leq 4 \cdot 1884^2 = 14197824$. If $N_0 p = 2$ and $N_0 r \neq 2$, then $N_0(r) \geq 4$ because $p^2 | \Delta(K/K_0)$, cf. [W] 3-7-23, hence $\Delta \leq \kappa^4(2^{-\frac{1}{4}} + 2^{\frac{1}{4}})^{-4} <$ < 14197824. If $N_0 p = N_0 r = 3$ we have $\Delta_0 \leq 1256$ and $\Delta \leq 9 \cdot 1256^2 =$ $= 14197824$. If $N_0 p = 3$ and $N_0 r \neq 3$, then $N_0 r \geq 7$, since $N_0 pr \equiv$ $\equiv 0,1 \bmod 4$ (cf. [Ma] app.II) hence $\Delta \leq \kappa^4((3/7)^{\frac{1}{4}} + (7/3)^{\frac{1}{4}})^{-4} < 14197824$. If $N_0 p = N_0 r = 4$ we have $\Delta_0 \leq 941$ and $\Delta \leq 16 \cdot 941^2 = 14167696$. Finally if $N_0 p = 4$ and $N_0 r \neq 4$, then $N_0 r \geq 16$ because $p^2 | \Delta(K/K_0)$, cf. [W] 3-7-23, hence $\Delta \leq \kappa^4(4^{-\frac{1}{4}} + 4^{\frac{1}{4}})^{-4} < 14167696$. □

LEMMA (10.25). *Suppose that* h(K) *is odd. If* A *has a Euclidean ideal class* $[a]$, *then there is an ideal* $c \in [a]$ *that is invariant under* $\mathrm{Gal}(K/K_0)$.

PROOF. Take $c = (a\sigma a)^{\frac{1}{2}(h(K)+1)}$. □

In the next proposition we will see that the existence of a Galois-invariant ideal in the Euclidean ideal class depends on the number of primes ramified in K/K_0, on the quotient $h(K)/h(K_0)$ and on the relation between A^* and A_0^*. We give a more precise result than needed here, with a view to an application in the next section.

If G is the Galois group of K/K_0 and M is a G-module we write

$$M^G = \{x \in M : \sigma x = x \text{ for all } \sigma \in G\}.$$

PROPOSITION (10.26). *Let* K_0 *be a real quadratic field and let* K *be a totally complex quadratic extension field of* K_0. *Denote by* A_0 *and* A *the rings of integers of* K_0 *and* K *respectively. Let* W *be the group of roots of unity of* K *and* $Q = \mathrm{Index}[A^* : WA_0^*]$. *Let* H *be the group of ideal classes of* K *that contain an ideal that is invariant under the Galois group* G *of* K/K_0. *Suppose that* $\mathrm{Cl}(A)^G = \mathrm{Cl}(A)$ *and that* $\mathrm{Index}[\mathrm{Cl}(A) : \iota\mathrm{Cl}(A_0)] \leq 2$, *then we have the following* 6 *possibilities:*

	Index[Cl(A) : H]	$\frac{h(A)}{h(A_0)}$	Q	#finite primes ramified in K/K_0
(i)	1	1	2	0
(ii)	1	1	1	1

	Index[Cl(A) : H]	$\frac{h(A)}{h(A_0)}$	Q	#finite primes ramified in K/K_0
(iii)	1	2	2	1
(iv)	1	2	1	2
(v)	2	1	1	0
(vi)	2	2	1	1

Moreover if Index[Cl(A) : H] = 2 *then* A_0 *has a fundamental unit that is totally positive.*

PROOF. Let I(A) be the ideal group of A and let P(A) be its subgroup of principal A-ideals. Consider the exact sequence

$$(10.27) \qquad 0 \longrightarrow A^* \longrightarrow K^* \longrightarrow P(A) \longrightarrow 0.$$

The cohomology with respect to G ([CF] ch.IV §8) gives the following exact sequence

$$0 \longrightarrow A_0^* \longrightarrow K_0^* \longrightarrow P(A)^G \longrightarrow H^1(A^*) \longrightarrow 0.$$

We have $H^1(A^*) = W/A^{*(\sigma-1)} \simeq Q\mathbb{Z}/2\mathbb{Z}$, where σ denotes the generator of G. Because $K_0^*/A_0^* \simeq P(A_0)$ and $I(A)^G/I(A_0) \simeq (\mathbb{Z}/2\mathbb{Z})^r$, where r is the number of ramifying primes in K/K_0, we have a diagram with exact rows and columns

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & & 0 & & C & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P(A_0) & \longrightarrow & I(A_0) & \longrightarrow & Cl(A_0) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P(A)^G & \longrightarrow & I(A)^G & \longrightarrow & H & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & Q\mathbb{Z}/2\mathbb{Z} & & (\mathbb{Z}/2\mathbb{Z})^r & & D & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

for certain groups C and D. Using the snake lemma we get $Q\cdot 2^{r-1} =$ $= \#(\mathbb{Z}/2\mathbb{Z})^r/\#(Q\mathbb{Z}/2\mathbb{Z}) = \#D/\#C = \#H/h(A_0) = \text{Index}[Cl(A):H]^{-1}\cdot h(A)/h(A_0)$. Because $h(A_0)|h(A)$, cf. [Wa] thm.4.16, $\iota Cl(A_0) \subset H$ and $\text{Index}[Cl(A):\iota Cl(A_0)] \leq 2$ we have $h(A)/h(A_0) \in \{1,2\}$. To prove the proposition it remains to show that $Q = 1$ and A_0 has a totally positive fundamental unit if $\text{Index}[Cl(A):H] = 2$.

Consider the exact sequence

$$0 \longrightarrow P(A) \longrightarrow I(A) \longrightarrow Cl(A) \longrightarrow 0$$

By taking the cohomology with respect to G we get the exact sequence

$$0 \longrightarrow P(A)^G \longrightarrow I(A)^G \longrightarrow Cl(A)^G \longrightarrow H^1(P(A)) \longrightarrow 0.$$

Because $Cl(A)^G = Cl(A)$ by assumption we have $Cl(A)/H \simeq H^1(P(A))$. By taking the cohomology of (10.27) we get $H^1(P(A)) \simeq (A_0^* \cap \tilde{N}K^*)/\tilde{N}A^*$. Hence $\text{Index}[Cl(A):H] = 2$ implies that $A_0^* \cap \tilde{N}K^* \neq \tilde{N}A^*$. This only happens if A_0 has a totally positive fundamental unit and $Q = 1$. □

Combining the results above we get the following theorem.

THEOREM (10.28). *Let* K *be a totally imaginary quadratic extension of a real quadratic field* K_0. *Let* A *be the ring of integers of* K *and let* A_0 *be the ring of integers of* K_0. *Let* W *be the group of roots of unity of* K *and let* η *be a fundamental unit of* A_0. *If* A *has a Euclidean ideal class and the discriminant* Δ *of* K *is larger than* 14206929, *then the following conditions hold.*

(a) $\Delta \leq 230202117$;

(b) $h(A) \in \{2,4,6\}$;

(c) *at most one finite prime ramifies in* K/K_0 *and such a prime is not of minimal norm ;*

(d) $\text{Index}[Cl(A):\iota Cl(A_0)] = 2$, *where* $\iota : Cl(A_0) \longrightarrow Cl(A)$ *is the natural map; moreover* ι *is injective if and only if exactly one finite prime ramifies in* K/K_0 ;

(e) $A^* = WA_0^*$ *and* $N_0(\eta) = 1$.

REMARK (10.29). Presumably there is no totally imaginary quartic field with discriminant > 14206929 for which the ring of integers has a Euclidean ideal class.

PROOF OF (10.28). The upper bound in (a) is proven in (5.19) (#4). Part (b) follows from (10.2), (10.23) and (10.25). For (c) and (e) we may apply (10.24) and (10.26) since by (10.4) we have $\mathrm{Index}[\mathrm{Cl}(A) : \iota\mathrm{Cl}(A_0)] \le 2$. Finally for (d) we use (10.26) together with the fact that $\iota\mathrm{Cl}(A_0) \subset H$.
□

§(10.4) Quartic cyclic extensions of $\mathbb{Q}$

In this section we assume that K is a totally imaginary quartic cyclic extension of $\mathbb{Q}$. The quadratic subfield $K \cap \mathbb{R}$ will be denoted by K_0. For the extension K/K_0 we adopt the notation explained at the beginning of section (10.2). Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$.

We prove the following theorem.

THEOREM (10.30). *Let* K *be a totally imaginary quartic cyclic field. The ring of integers of* K *has a Euclidean ideal class if and only if* $K = \mathbb{Q}(\zeta_5)$ *or* K *is the quartic subfield of* $\mathbb{Q}(\zeta_{13})$. *Moreover in both cases the ring of integers itself is Euclidean.*

The proof of (10.30) occupies the whole section. First we prove the 'only if' part in several stages.

LEMMA (10.31). *Suppose that* A *has a Euclidean ideal class* $[\mathfrak{a}]$, *then there exists an ideal* $\mathfrak{c} \in [\mathfrak{a}]$ *that is invariant under* $\mathrm{Gal}(K/\mathbb{Q})$.

PROOF. From (2.4) we derive that $[\mathfrak{a}]$ is invariant under $\mathrm{Gal}(K/\mathbb{Q})$. Because $[\mathfrak{a}] = [\sigma\mathfrak{a}]$ there exists $\alpha \in K^*$ such that $\sigma\mathfrak{a} = \alpha\mathfrak{a}$, hence $N\mathfrak{a} = N(\alpha)\cdot N\mathfrak{a}$. Because K is totally complex we have $\mathcal{N}(\alpha) = N(\alpha) = 1$. From Hilbert 90 ([CF] Ch.V §2.7) we conclude that there exists $\beta \in K^*$ such that $\alpha = \beta\sigma\beta^{-1}$. Then $\mathfrak{c} = \beta\mathfrak{a} \in [\mathfrak{a}]$ is invariant under $\mathrm{Gal}(K/\mathbb{Q})$.
□

PROPOSITION (10.32). *Suppose that* A *has a Euclidean ideal class. Then* K *is one of the* 17 *fields listed in table* 20.

TABLE 20. Cyclic totally imaginary quartic fields that may have a Euclidean ideal class. The discriminant of K is denoted by Δ, that of K_0 by Δ_0. The conductor of K is denoted by f, that of K_0 by f_0. In the case that h(K) = 4 the field K is not determined uniquely by f and f_0. In this case a characterization of a 4-th degree character corresponding to K is given.

h(K) = 1

Δ	f	$\Delta_0 = f_0$
$125 = 5^3$	5	5
$2048 = 2^{11}$	16	8
$2197 = 13^3$	13	13
$24389 = 29^3$	29	29
$50653 = 37^3$	37	37
$148877 = 53^3$	53	53
$226981 = 61^3$	61	61

h(K) = 2

Δ	f	$\Delta_0 = f_0$
$8000 = 2^6 \cdot 5^3$	40	5
$18432 = 2^{11} \cdot 3^2$	48	8
$21125 = 5^3 \cdot 13^2$	65	5
$36125 = 5^3 \cdot 17^2$	85	5
$51200 = 2^{11} \cdot 5^2$	80	8
$54925 = 5^2 \cdot 13^3$	65	13
$140608 = 2^6 \cdot 13^3$	104	13
$240737 = 7^2 \cdot 17^3$	119	17

h(K) = 4

Δ	f	$\Delta_0 = f_0$	χ
$256000 = 2^{11} \cdot 5^3$	80	40	$\chi(3) = -1$
$614125 = 5^3 \cdot 17^3$	85	85	$\chi(3) = -1$

PROOF. From (2.5) and (2.11) we know that the class group $Cl(A)$ is cyclic of order dividing 4. From (10.31) we know that we may use the bounds of (10.22) and that G acts trivially on $Cl(A)$. Let H be the Hilbert class field of K. By class field theory we have $Gal(H/K) \simeq Cl(A)$ and also $Gal(K/\mathbb{Q})$ acts trivially on $Gal(H/K)$. Hence $Gal(H/\mathbb{Q}) \simeq$ $\simeq Gal(K/\mathbb{Q}) \times Cl(A) \simeq \mathbb{Z}/4\mathbb{Z} \times Cl(A)$.

Let X be the group of Dirichlet-characters corresponding to K, cf. [Wa] ch.3. It is generated by a character χ of order 4 for which $\chi(-1) = -1$. Let f be the conductor of χ and let f_0 be the conductor of χ^2, then f is the conductor of K and f_0 is the conductor of K_0. By the conductor discriminant product formula, [Wa] thm.3.11, we have $\Delta = f^2f_0$ and $\Delta_0 = f_0$, hence $N_0(\Delta(K/K_0)) = f^2f_0^{-1}$ by (10.7). We write $\chi = \prod_{p|f} \chi_p$, where χ_p is a character of which the conductor is a power of p and the product is taken over the prime divisors p of f. Let X_p denote the group generated by χ_p, then the character group corresponding to H is equal to $\prod_{p|f} X_p$, cf. [Wa] ch.3. Because the character group is dual, hence isomorphic, to the Galois group we find that at most two primes ramify in $K/\mathbb{Q}$.

Write $g = ff_0^{-1}$, then $g \in \mathbb{Z}_{>0}$. Because A has a Euclidean ideal class we have by (10.22) that $f_0(q(a) + q(a)^{-1}g\sqrt{f_0})^2 \le \kappa^2$. Below we often need a bound on f_0 for given g or a bound on g for given f_0. An easy computation shows that

$$(10.33) \qquad f_0 \le \tfrac{1}{4}q(a)^2g^{-2}(-q(a) + \sqrt{q(a)^2 + 4g\kappa q(a)^{-1}}\,)^2;$$

$$g \le q(a)f_0^{-1}\kappa - q(a)^2f_0^{-\frac{1}{2}}.$$

Each A-ideal a invariant under $Gal(K/K_0)$ is of the form a_0b, where a_0 is an A_0-ideal and b is a product of different prime ideals ramifying in K/K_0. We have $q(a) = q(b) = \sqrt{Nb}$.

For the remainder of the proof we consider the three possibilities for $h(A)$ separately.

(a) Suppose that $h(A) = 1$, then $H = K$ and only one prime p divides f. Because $\chi_p(-1) = \chi(-1) = -1$ we have $p = 2$ or $p \equiv 5 \bmod 8$. If $p = 2$ we have $f = 16$, $f_0 = 8$ and $\Delta = 2048$. This field is included in table 20. If $p \equiv 5 \bmod 8$ we have $f = f_0 = p$ and $g = 1$. If A has a

Euclidean ideal class then A is itself Euclidean. We have $q(A) = 1$, hence by the first inequality of (10.33) we have

$$p \leq \frac{1}{4}(-1 + \sqrt{1+4\kappa})^2 = 112.196,$$

i.e. $p \in \{5,13,29,37,53,61,101,109\}$. From the tables of Hasse [H2] and of Yoshino and Hirabayashi [YH], or by using the analytic class number formula ([Wa] ch.4), we derive that $h(A) = 1$ only if $p \in \{5,13,29,37,53,61\}$.

(b) Suppose that $h(A) = 2$, then exactly two primes p and q divide f, where the order of χ_p is equal to 4 and the order of χ_q is equal to 2. By (10.26) at most two primes ramify in K/K_0, hence q is inert in $K_0/\mathbb{Q}$. Because the order of χ_p is 4 we have $p = 2$ or $p \equiv 1 \bmod 4$. We denote by $\mathfrak{p}$ and $\mathfrak{q}$ the primes of K lying over p and q respectively.

Let G_p and G_q be the inertia groups in Gal $(H/\mathbb{Q})$ of the primes over p and q respectively. By Minkowski's theorem ([W] 5-4-10) G_p and G_q generate $\mathrm{Gal}(H/\mathbb{Q})$. This shows that $\mathrm{Gal}(H/\mathbb{Q})/G_q$ is cyclic and that $\mathfrak{q}$ is inert in H/K. Let H_q be the fixed field of G_q. Then H_q is a quadratic extension of $\mathbb{Q}$ in which only q ramifies. From the quadratic reciprocity law we find that p is inert in $H_q/\mathbb{Q}$ (if $q = 2$ we need the extra information that $\chi(-1) = -1$). Hence $\mathfrak{p}$ is inert in H/K. This shows that both $\mathfrak{p}$ and $\mathfrak{q}$ are non-principal A-ideals. Because they are invariant under $\mathrm{Gal}(K/\mathbb{Q})$ we may take one of them for the Galois-invariant Euclidean ideal.

If $p = 2$, then $q \equiv \pm 3 \bmod 8$. The character χ_p of conductor 16 is up to taking the inverse determined by $\chi_p(-1) = -\chi_q(-1)$. We have $f_0 = 8$, $f = 16q$ and $g = 2q$. We take $\mathfrak{a} = \mathfrak{p}$, then $q(\mathfrak{a}) = \sqrt{2}$. From the second inequality of (10.33) we derive that

$$q \leq \frac{1}{16}\sqrt{2}\cdot\kappa - \frac{1}{4}\sqrt{2} = 10.499,$$

i.e. $q = 3$ or $q = 5$. From the tables in [Ha2] we find that in both cases $h(A) = 2$.

If $q = 2$ then $p \equiv 5 \bmod 8$, because 2 is inert in $K_0/\mathbb{Q}$. Hence $\chi_p(-1) = -1$ and χ_q is the even character of conductor 8. This shows that $f_0 = p$, $f = 8p$ and $g = 8$. We take $\mathfrak{a} = \mathfrak{q}$, then $q(\mathfrak{a}) = 2$. From the first inequality of (10.33) we derive that

$$p \leq \frac{1}{64}(-2 + \sqrt{4+16\kappa})^2 = 28.049,$$

i.e. $p = 5$ or $p = 13$. From the tables of [Ha2] and [YH] we find that $h(A) = 2$ in both cases.

If both p and q are odd we have $f_0 = p$, $f = pq$ and $g = q$. We take $\mathfrak{a} = \mathfrak{p}$, then $q(\mathfrak{a}) = \sqrt{p}$. From the second inequality of (10.33) we derive that

$$q \le \kappa \cdot p^{-\frac{1}{2}} - p^{\frac{1}{2}}.$$

Since $q \ge 3$ we have $p \le \frac{1}{4}(-3 + \sqrt{9+4\kappa})^2 = 93.742$. Keeping in mind that $(\frac{p}{q}) = -1$ and $\chi(-1) = -1$ we find the following possibilities for p and q: q:

p	q ≤	q
5	52.676	13, 17, 37
13	30.450	5
17	25.657	3, 7, 11, 23
29	17.416	17
37	14.103	5, 13
41	12.773	3, 7, 11
53	9.586	5
61	7.911	-
73	5.827	-
89	3.581	3

From the tables in [Ha2] and [YH] and from the analytic class number formula, cf. [Wa] ch.4, we find that $h(2) = 2$ only if $p = 5$ and $q = 13$ or 17; $p = 13$ and $q = 5$; $p = 17$ and $q = 7$.

(c) Finally suppose that $h(A) = 4$. Then exactly two primes p and q divide f. Both characters χ_p and χ_q have order 4. For given p and q the characters χ_p and χ_q are determined up to taking inverse and thus there are two possibilities for X and for K. Because $\chi_p\chi_q(-1) = -1$ we may assume that $p = 2$ and $q \equiv 1 \bmod 4$ or $p \equiv 5 \bmod 8$ and $q \equiv 1 \bmod 8$.

Let $\mathfrak{p}$ be the A-ideal of norm p and let $\mathfrak{q}$ be the A-ideal of norm q. Let $\mathfrak{a}$ be a Euclidean A-ideal that is invariant under $\mathrm{Gal}(K/K_0)$, then $\mathfrak{a} = \mathfrak{a}_0\mathfrak{b}$, where $\mathfrak{a}_0$ is an A_0-ideal and $\mathfrak{b} \in \{A, \mathfrak{p}, \mathfrak{q}, \mathfrak{pq}\}$. Then $q(\mathfrak{a}) = q(\mathfrak{b}) = \sqrt{N\mathfrak{b}}$, hence $q(\mathfrak{a}) \in \{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$.

First suppose that $p = 2$. Then $f = 16q$, $f_0 = 8q$ and $g = 2$. The character χ_p of conductor 16 is up to taking the inverse determined by $\chi_p(-1) = -\chi_q(-1)$. We may take $\mathfrak{a} = \mathfrak{p}$, the ideal of minimal norm, and $q(\mathfrak{a}) = \sqrt{2}$. From the first inequality of (10.33) we derive that

$$q \le \frac{1}{64}(-\sqrt{2} + \sqrt{2+4\kappa\sqrt{2}})^2 = 9.749,$$

hence $q = 5$. From the table in [Ha2] we find that $h(A) = 4$ only in the case that $\chi(3) = -1$.

Now suppose that $p \ne 2$. Then $f = f_0 = pq$ and $N_0(\Delta(K/K_0)) = pq$, hence $(q(\mathfrak{a}) + q(\mathfrak{a})^{-1}\sqrt{N_0(\Delta(K/K_0))}) \in \{1+\sqrt{pq}, \sqrt{p}+\sqrt{q}\}$. Because $\sqrt{p} + \sqrt{q} < 1 + \sqrt{pq}$ we have by (10.22) that

$$pq(\sqrt{p} + \sqrt{q})^2 \le \kappa^2.$$

Because $p \ge 5$ we have

$$q \le \frac{1}{4}\left(-\sqrt{5} + \sqrt{5 + \frac{4\kappa}{\sqrt{5}}}\right)^2 = 40.655,$$

hence $q = 17$. This gives

$$p \le \frac{1}{4}\left(-\sqrt{17} + \sqrt{17 + \frac{4\kappa}{\sqrt{17}}}\right)^2 = 14.228,$$

hence $p = 5$ or $p = 13$. From the tables in [Ha2] we find that $h(A) = 4$ only if $p = 5$ and $\chi(3) = -1$. □

For the proof of (10.30) it only remains to consider the fields in table 20. We first deal with the rings that do not have a Euclidean ideal class. The following lemma is similar to (5.23).

<u>LEMMA (10.34)</u>. *Let* $\mathfrak{a}$ *be a Euclidean* A*-ideal that is invariant under* $\mathrm{Gal}(K/\mathbb{Q})$. *Let* $n \in \mathbb{Z}$ *be an integer that is a 4-th power of an integer mod* $\mathfrak{a} \cap \mathbb{Z}$. *Then there exists* $\alpha \in A$ *such that* $\mathcal{N}(\alpha) \equiv n \bmod \mathfrak{a} \cap \mathbb{Z}$ *and* $0 \le \mathcal{N}(\alpha) < N\mathfrak{a}$.

<u>PROOF</u>. Let $m \in \mathbb{Z}$ be such that $m^4 \equiv n \bmod \mathfrak{a}$. Then there exists $\alpha \in A$ with $\alpha \equiv m \bmod \mathfrak{a}$ and $N(\alpha) = \mathcal{N}(\alpha) \equiv m \bmod \mathfrak{a}$. Because $\mathfrak{a}$ is invariant under $\mathrm{Gal}(K/\mathbb{Q})$ we have $\mathcal{N}(\alpha) \equiv m^4 \equiv n \bmod \mathfrak{a} \cap \mathbb{Z}$. Also we have $\mathcal{N}(\alpha) \ge 0$. □

Because the Euclidean ideal class is uniquely determined by (2.3) we may check (10.34) for the rings of integers of the fields in table 20. For seven of these rings table 21 lists the ideals and $n \in \mathbb{Z}$ for which there is no α as in (10.34).

TABLE 21. Ideals $\mathfrak{a}$ for which there is a 4-th power $n \bmod \mathfrak{a} \cap \mathbb{Z}$ and for which there is no $\alpha \in A$ with $N\alpha = n$.

f	f_0	h	$N\mathfrak{a}$	$\mathfrak{a} \cap \mathbb{Z}$	n
29	29	1	29	$29\,\mathbb{Z}$	20
37	37	1	37	$37\,\mathbb{Z}$	10
53	53	1	53	$53\,\mathbb{Z}$	10
61	61	1	61	$61\,\mathbb{Z}$	12
65	13	2	13	$13\,\mathbb{Z}$	3
104	13	2	13	$13\,\mathbb{Z}$	3
119	17	2	17	$17\,\mathbb{Z}$	13

Eight other rings may be treated with (7.1), which also applies to our situation, as the reader may check. In table 22 one finds for a given field K, with ring of integers A, an integral ideal $\mathfrak{c}$, the order k of the subgroup $A^* \bmod \mathfrak{c}$ in $(A/\mathfrak{c})^*$ and the number ℓ of integral A-ideals of norm $< N\mathfrak{c}$ in the ideal class $[\mathfrak{a}^{-1}\mathfrak{c}]$. Here $[\mathfrak{a}]$ is the ideal class that contains the integral ideals of minimal norm < 1. Because $k\ell < N\mathfrak{a} - 1$ we find that $[\mathfrak{a}]$ is not Euclidean. This finishes the proof of the 'only if' part of (10.30).

TABLE 22. Integral ideals $\mathfrak{c}$ for which the order k of $(A^* \bmod \mathfrak{c})$ in $(A/\mathfrak{c})^*$ and the number ℓ of integral ideals in $[\mathfrak{a}^{-1}\mathfrak{c}]$ of norm $< N\mathfrak{c}$ satisfy $k\ell < N\mathfrak{c} - 1$. Here $[\mathfrak{a}]$ is the ideal class that contains the integral ideals of minimal norm > 1.

f	f_0	h	$N\mathfrak{c}$	k	ℓ
16	8	1	4	1	2
40	5	2	16	3	2
48	8	2	4	1	1
65	5	2	16	3	1
85	5	2	16	3	1
80	8	2	4	1	1
80	40	4	9	2	1
85	85	4	17	4	2

It remains to prove that for the fields with conductors 5 and 13 the ring of integers A has a Euclidean ideal class. In both cases $h(A) = 1$, hence we have to prove that A is Euclidean. If $f = 5$, then $K = \mathbb{Q}(\zeta_5)$ and it is already known that A is Euclidean, cf. [K;O] and section (0.6). Hence we only have to show that the ring of integers A of the 4-th degree subfield K of $\mathbb{Q}(\zeta_{13})$ is Euclidean. This can be done with a method similar to Ojala's method for $\mathbb{Q}(\zeta_{16})$ in [Oj]. Below we describe this method.

The ring A is equal to $\mathbb{Z}\beta + \mathbb{Z}\sigma\beta + \mathbb{Z}\sigma^2\beta + \mathbb{Z}\sigma^3\beta$, where $\beta = \frac{1}{4}(-1+\sqrt{13}+\sqrt{-26+6\sqrt{13}})$ and σ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$. Notice that $\beta = \zeta + \zeta^3 + \zeta^9$, where ζ is a primitive 13-th root of unity. The unit $\eta = \frac{1}{2}(3+\sqrt{13})$ is a fundamental unit of A. Multiplication by η is given by

$$\eta \begin{pmatrix} \beta \\ \sigma\beta \\ \sigma^2\beta \\ \sigma^3\beta \end{pmatrix} = \begin{pmatrix} -1 & -1 & -1 & -2 \\ 2 & 4 & 1 & 1 \\ -1 & -2 & -1 & -1 \\ 1 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} \beta \\ \sigma\beta \\ \sigma^2\beta \\ \sigma^3\beta \end{pmatrix}.$$

This is needed in the computations described below.

We regard K as being embedded in $\mathbb{C} \times \mathbb{C}$, with $\sqrt{13} > 0$ on the first factor and $\sqrt{13} < 0$ on the second. Let $|\cdot|_1$ be the valuation on the first coordinate and let $|\cdot|_2$ be the valuation on the second coordinate. These valuations are given by

$$|a_0\beta + a_1\sigma\beta + a_2\sigma^2\beta + a_3\sigma^3\beta|_1 = (a_0^2+a_2^2)\cdot\frac{5-\sqrt{13}}{2} + (a_1^2+a_3^2)\cdot\frac{5+\sqrt{13}}{2} +$$

$$- (a_0a_1 + a_0a_2 + a_2a_3)\cdot\frac{3-\sqrt{13}}{2} - (a_1a_2 + a_1a_3 + a_0a_3)\cdot\frac{3+\sqrt{13}}{2}; \qquad (10.35)$$

$$|a_0\beta + a_1\sigma\beta + a_2\sigma^2\beta + a_3\sigma^3\beta|_2 = |a_1\beta + a_2\sigma\beta + a_3\sigma^2\beta + a_0\sigma^3\beta|_1.$$

Hence

$$(10.36) \qquad |\sum_{i=0}^{3} a_i\sigma^i\beta|_1 + |\sum_{i=0}^{3} a_i\sigma^i\beta|_2 =$$

$$= 5\cdot\sum_{i=0}^{3} a_i^2 - 3\cdot\sum_{i\neq j} a_ia_j = \frac{13}{2}\sum_{i=0}^{3} a_i^2 - \frac{3}{2}(\sum_{i=0}^{3} a_i)^2.$$

To prove that A is Euclidean it suffices to prove that for any $\gamma = \sum_{i=0}^{3} a_i\sigma^i\beta$, with $a_i \in \mathbb{R}$ and $|a_i| \le \frac{1}{2}$ there exists $n \in \mathbb{Z}$ and $\alpha \in A$ such that

$$(10.37) \qquad |\eta^n\gamma - \alpha|_1 |\eta^n\gamma - \alpha|_2 < 1.$$

To prove this we divide the region with $|a_i| \le \frac{1}{2}$ into 10000 parallelepipeds of the form

$$\{\sum_{i=0}^{3} a_i\sigma^i\beta : \frac{r_i}{10} \le a_i \le \frac{r_i+1}{10}\},$$

with $r_i \in \mathbb{Z}$, $-5 \le r_i \le 4$. We only consider those parallelepipeds for which $r_0 = \max\{r_i, -r_i-1 : 0 \le i \le 3\}$, because the others are obtained from these by action of $\mathrm{Gal}(L/\mathbb{Q})$ and multiplication by -1. The following steps are processed for each parallelepiped P.

<u>Step 1</u>. If $r_0 \le 1$ we find that (10.37) is satisfied for $\alpha = 0$ and $n = 0$ and all $\gamma \in P$ since for any $\gamma \in P$ we have by the inequality of the means and (10.36) that $|\gamma|_1|\gamma|_2 \le \frac{1}{4}(|\gamma|_1 + |\gamma|_2)^2 \le \frac{1}{4}(\frac{13}{2}\cdot 4 \cdot \frac{4}{100})^2 < 1$. In this case we stop, otherwise we go to step 2.

<u>Step 2</u>. Now we have $r_0 \in \{2,3,4\}$. If $\max\{r_i, -r_i-1 : i \ne 0\} = 0$ we find that (10.37) is satisfied for $\alpha = 0$ and $n = 0$ and all $\gamma \in P$, since for any $\gamma \in P$ we have $|\gamma|_1|\gamma|_2 \le \frac{1}{4}(|\gamma|_1 + |\gamma|_2)^2 \le \frac{1}{4}(\frac{13}{2}\cdot(\frac{1}{4} + \frac{3}{100}))^2 < 1$ by (10.36). In this case we stop, otherwise we go to step 3.

<u>Step 3</u>. Let $\mu = \sum_{i=0}^{3} m_i\sigma^i\beta$ be the centre of P, so $m_i = r_i + \frac{1}{2}$. Let T be the set of $\alpha \in A$ of the form $\sum_{i=0}^{3} a_i\sigma^i\beta$ with $|a_i - m_i| = \frac{1}{2}$ for $0 \le i \le 3$. For the $\alpha \in T$ we check whether $|\rho - \alpha|_1 + |\rho - \alpha|_2 < 2$ for all vertices ρ of P. If this is the case we know that (10.37) is satisfied for $n = 0$ and all $\gamma \in P$ since for $\gamma \in P$ we have

$$|\gamma - \alpha|_1 |\gamma - \alpha|_2 \le \frac{1}{4}(|\gamma - \alpha|_1 + |\gamma - \alpha|_2)^2 \le$$

$$\le \max\{\frac{1}{4}(|\rho - \alpha|_1 + |\rho - \alpha|_2)^2 : \rho \text{ vertex of } P\} < 1.$$

In this case we stop. If the condition is not satisfied we go to step 4.

Notice that steps 1, 2 and 3 can be performed for up to 6 different P at once, since the conditions are independent of the ordering of the r_i.

Step 4. Let T be as in step 3. For each $\alpha \in T$ we compute

$$V_1 = \max\{|\rho - \alpha|_1 : \rho \text{ vertex of } P\};$$

$$V_2 = \max\{|\rho - \alpha|_2 : \rho \text{ vertex of } P\}.$$

By convexity we have $|\gamma - \alpha|_1 \leq V_1$ and $|\gamma - \alpha|_2 \leq V_2$ for all $\gamma \in P$. If $V_1V_2 < 1$ we find that (10.37) is satisfied for $n = 0$ and all $\gamma \in P$. In this case we stop. If $V_1V_2 \geq 1$ for all choices of $\alpha \in T$ we go to step 5.

Step 5. Let μ be the centre of P and suppose that $\eta\mu = \sum_{i=0}^{3} e_i\sigma^i\beta$. Let T be the set of elements of A of the form $\sum_{i=0}^{3} a_i\sigma^i\beta$ with $|a_i - e_i| \leq 1$. For each $\alpha \in T$ we compute

$$V_1 = \max\{|\rho - \alpha|_1 : \rho \text{ vertex of } \eta P\};$$

$$V_2 = \max\{|\rho - \alpha|_2 : \rho \text{ vertex of } \eta P\}.$$

If $V_1V_2 < 1$ we find that (10.37) is satisfied for all $\gamma \in P$ and $\eta = 1$. In this case we stop. If $V_1V_2 \geq 1$ for all choices of $\alpha \in T$ we perform a similar procedure with η replaced by η^{-1}. If in this case the conditions are not satisfied we go to step 6.

Step 6. We divide P into 16 smaller parallelepipeds by cutting each edge in two halves. For each of these parallelepipeds we return to step 4.

Processing this algorithm on a computer one finds that it terminates. In fact after performing steps 1, 2 and 3 one is left with 378 of the 1800 parallelepipeds with $r_0 = \max\{r_i, -r_i - 1 : i = 0,1,2,3\}$. After step 4 there remain 108 parallelepipeds and after step 5 one is left with 71 parallelepipeds. Step 6 turns this into 1136 smaller parallelepipeds. After step 4 there are still 87 parallelepipeds left over and after step 5 there remain 3 parallelepipeds. Step 6 turns this into 48 smaller parallelepipeds and after performing step 4 for the third time no parallelepiped is left over.

This finishes the proof of (10.30).

§(10.5) Biquadratic bicyclic fields

In this section we consider the case that $Gal(K/\mathbb{Q}) \simeq V_4$. Let $K_0 = K \cap \mathbb{R}$, K_1 and K_2 be the quadratic subfields of K, let A_i be the ring of integers and Δ_i the discriminant of K_i. We have $\Delta(K) = \Delta_1 \cdot \Delta_2 \cdot \Delta_3$, cf. [Wa] thm.3.11. Let W be the group of roots of unity of K. From the analytic class number formula ([BS] Kap.V §1 Satz 2) we derive that

(10.38) $$h(A) = 1 \quad \text{if} \quad K = \mathbb{Q}(\sqrt{-4},\sqrt{8}) = \mathbb{Q}(\zeta_8);$$

$$h(A) = \tfrac{1}{2}Q \cdot h(A_0) \cdot h(A_1) \cdot h(A_2) \quad \text{else},$$

where $Q = \mathrm{Index}[A^* : WA_0^*]$. We know that A is Euclidean in the case that $K = \mathbb{Q}(\zeta_8)$, cf. section (0.6). In the sequel we will not consider this field anymore, hence we may assume that the second equality of (10.38) is valid.

In contrast to the cyclic case we do not get a complete determination of all Euclidean rings in this section. We will prove the following theorem.

THEOREM (10.39). *Let* K *be a totally imaginary field that is a Galois extension of* $\mathbb{Q}$ *with group* V_4. *If* $A = \mathcal{O}(K)$ *has a Euclidean ideal class, then* $h(A)|2$ *and* K *is contained in a list of* 124 *fields all having discriminant* $\Delta(K) \leq 9591409$.

The proof of (10.39) runs as follows. First we show that $h(A) = 4$ cannot occur. Then we treat the rings A for which the Euclidean ideal class contains an ideal invariant under $Gal(K/K_0)$ and finally we treat the remaining rings.

LEMMA (10.40). *Suppose that* $h(A) = 4$ *and that* A *has a Euclidean ideal class. Then* $Q = 1$ *and* $h(A_i) = 2$ *for* $i = 0,1,2$.

PROOF. From (10.4) we derive that $h(A_i) \geq 2$ for $i = 0,1,2$. Hence (10.38) can only be satisfied if $h(A_i) = 2$ for $i = 0,1,2$ and $Q = 1$. □

LEMMA (10.41). *Suppose that* $h(A) = 4$ *and that* A *has a Euclidean ideal class. Then* 2 *is not totally ramified in* $K/\mathbb{Q}$.

PROOF. Let H be the Hilbert class field of K. Suppose that 2 is totally ramified in $K/\mathbb{Q}$, then, considering the inertia group of 2 in

$Gal(H/\mathbb{Q})$, we find that $Gal(H/\mathbb{Q})$ is a semidirect product of $Gal(K/\mathbb{Q}) \simeq \simeq V_4$ by $Gal(H/K) \simeq Cl(A) \simeq \mathbb{Z}/4\mathbb{Z}$. Since the action of $Gal(K/\mathbb{Q})$ on $Cl(A)$ is trivial we find that this semidirect product is in fact a direct product, hence $H/\mathbb{Q}$ is abelian. This gives a contradiction because $Gal(H/\mathbb{Q})$ would be an elementary abelian 2-group if it were abelian, cf. [Wa] ch.3. □

PROPOSITION (10.42). *If* A *has a Euclidean ideal class then* $h(A) \le 2$.

PROOF. Suppose to the contrary that $h(A) = 4$. Then $h(A_i) = 2$ for $i = = 0,1,2$ by (10.40). Because no prime is totally inert in $K/\mathbb{Q}$ there are ideals of norm 4, and 2A is the product of two of them. If these ideals have minimal norm then $h(A)|2$ by (2.3), a contradiction. This shows that we have $\Delta_i \not\equiv 5 \bmod 24$ for $i = 0,1,2$.

In [St] all imaginary quadratic fields with class number equal to 2 are determined. Considering pairs of these fields and consulting a list of class numbers of real quadratic fields (e.g. [I]) we find that the restrictions of (10.40) and (10.41) are satisfied, with $\Delta_i \not\equiv 5 \bmod 24$ only for the following fields:

	Δ_0	Δ_1	Δ_2	$\Delta(K)$
(1)	40	-15	-24	14400
(2)	65	-20	-52	67600
(3)	85	-15	-51	65025
(4)	136	-24	-51	166464
(5)	205	-15	-123	378225
(6)	185	-20	-148	547600
(7)	481	-52	-148	3701776
(8)	712	-24	-267	4562496
(9)	1513	-51	-267	20602521
(10)	3649	-123	-267	119836809

The fields (9) and (10) belong to the case (iv) of (10.26) but their discriminants do not satisfy the bound of (10.23), hence A has no Euclidean ideal class. For the fields (2), (4), (5) and (8) there is an element $\alpha \in A$ with $N(\alpha) = n^2$, where n is the least integer > 1 that occurs as the norm of an integral A-ideal. This shows that (2.3) is not satisfied and that A has no Euclidean ideal class.

For the fields (6) and (7) there are two prime ideals p and q of norm 2 and there is no ideal of norm 3. Because A^* acts trivially on A/pq we conclude that A has no Euclidean ideal class by (7.1), which also applies to this situation.

For the field (1) there are 2 primes p_2 and q_2 of norm 2 and two primes p_3 and q_3 of norm 3, all in the same ideal class that generates Cl(A). The two ideals of norm 5 are in the inverse ideal class. This enables us to show that there is no element in A of norm < 32 that is $\equiv 2 \bmod p_2^3$ and $\equiv 1 \bmod q_2^2$. This last observation shows that the ideal $p_2^3 q_2^2$ of norm 32, which is in the ideal class of p_2, is not Euclidean and A has no Euclidean ideal class.

Finally we consider the field (3). The integral ideals of minimal norm > 1 are two ideals p and q of norm 3. The action of A^* on A/p^2 has order 2. There are only 12 ideals of norm $< 27 = Np^3$ in the ideal class $[p^2]$. By (7.1), which also applies to this situation, we find that A has no Euclidean ideal class. □

PROPOSITION (10.43). *Suppose that* A *has a Euclidean ideal class that contains an ideal that is invariant under* $\mathrm{Gal}(K/K_0)$, *then* K *is contained in a list of* 93 *fields all having discriminant* $\Delta(K) \leq 9591409$.

PROOF. By (10.42) we know that $h(A) \leq 2$ and by (10.23) we know that $\Delta(K) \leq 14206929$. We are in one of the cases (i), (ii), (iii) or (iv) of (10.26). All fields with $h(A) \leq 2$ and $\Delta(K) \leq 14206929$ are listed in [BP] and [BWW]. For these fields we checked the discriminant bound (10.22) and whether they are in one of the cases (i), (ii), (iii) or (iv) of (10.26). There remained 93 fields all having $\Delta(K) \leq 9591409$. □

PROPOSITION (10.44). *Suppose that* A *has a Euclidean ideal class that does not contain an ideal that is invariant under* $\mathrm{Gal}(K/K_0)$, *then* K *is contained in a list of* 31 *fields, all having discriminant* $\Delta(K) \leq$ ≤ 7958041.

PROOF. We are in one of the cases (v) or (vi) of (10.26). Hence $Q = 1$ and $h(A) = \frac{1}{2}h(A_0)\cdot h(A_1)\cdot h(A_2)$. Also we have $h(A) = 2$ by (10.25) and (10.42). By (10.29)(a) we have $\Delta(K) \leq 230202117$. The fields with $h(A) = 2$ that satisfy this bound are all listed in [BWW]. For these fields we checked whether they are in one of the cases (v) or (vi) of (10.26) and whether the fundamental unit of K_0 is totally positive, cf. (10.26). Also we checked whether an integral A-ideal of minimal norm > 1 is invariant under $Gal(K/K_0)$, since such an ideal must be Euclidean by (2.3). There remained 31 fields all having $\Delta(K) \leq 7958041$. □

The proof of (10.39) now follows by combining (10.42), (10.43) and (10.44).

§(10.6) Examples

In this section we list all known examples of rings with a Euclidean ideal class in the cases (#3) and (#4). Most of these examples have $h(\mathcal{O}) = 1$, i.e. the ring itself is Euclidean. Except the quartic cyclic field of conductor 13 all examples with $h(\mathcal{O}) = 1$ appeared already in the literature. For each of the cases (#3) and (#4) we have an example with $h(\mathcal{O}) = 2$. In the case (#3) this is a new example. In the case (#4) the example is due to Lenstra [L5].

In table 23 the examples in case (#3) are listed. Also $h = h(\mathcal{O})$ is given. All fields are determined by their discriminants. The examples with $\Delta \geq -152$ are due to Godwin [Go], the other examples, except the one with $\Delta = -283$, are due to Taylor [T]. The field with $\Delta = -283$ has class number 2. Below we show that its ring of integers has a Euclidean ideal class.

TABLE 23. Rings with a Euclidean ideal class in the case (#3).

Δ	h	Δ	h	Δ	h
-23	1	-204	1	-424	1
-31	1	-211	1	-431	1
-44	1	-212	1	-440	1
-59	1	-216	1	-451	1
-76	1	-231	1	-460	1
-83	1	-239	1	-472	1
-87	1	-243	1	-484	1
-104	1	-244	1	-492	1
-107	1	-247	1	-499	1
-108	1	-255	1	-503	1
-116	1	-268	1	-515	1
-135	1	-283	2	-516	1
-139	1	-300	1	-519	1
-140	1	-324	1	-543	1
-152	1	-356	1	-628	1
-172	1	-379	1	-652	1
-175	1	-411	1	-687	1
-200	1	-419	1		

In table 24 the examples in case (#4) are listed. Of these fields are given the discriminant Δ, the class number h, the discriminants Δ_i of all quadratic subfields and the Galois group G of the normal closure of the field over $\mathbb{Q}$. In this list D_4 denotes the dihedral group of order 8 and S_4 denotes the symmetric group on 4 elements. Notice that we have not found an example for which this Galois group is equal to the alternating group A_4. The cyclotomic fields $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\zeta_{12})$ and $\mathbb{Q}(\zeta_8)$ are the fields with $\Delta = 125, 144$ and 256 respectively. In section (0.6) we saw that they have a Euclidean ring of integers. The other fields, except those with $\Delta = 229, 1372, 1521, 2048$ and 2197 are due to Lakein [Lk]. He used a method that resembles Perron's method for the real quadratic case, cf. [P]. Cioffari [Ci] has shown that the ring of integers of $\mathbb{Q}(\sqrt[4]{-2})$ and $\mathbb{Q}(\sqrt[4]{-7})$, with discriminants 2048 and 1372, are Euclidean. He also proved that $\mathbb{Q}(\sqrt[4]{-3})$, of discriminant 432, has a Euclidean ring of integers, but that field also occurs in Lakein's list. The examples with $\Delta = 229$ and 1521 are due to Lenstra [L3;L5]. For the latter, with $h(\mathcal{O}) = 2$, he used Lakein's method. The field with $\Delta = 2197$ is the field with conductor 13. In section (10.5) we proved that its ring of integers is Euclidean.

TABLE 24. Rings with a Euclidean ideal class in the case (#4).

Δ	h	Δ_i	G
117	1	-3	D_4
125	1	5	$\mathbb{Z}/4\mathbb{Z}$
144	1	-3, -4, 12	V_4
189	1	-3	D_4
225	1	-3, -15, 5	V_4
229	1		S_4
256	1	-4, -8, 8	V_4
272	1	-4	D_4
320	1	-4	D_4
333	1	-3	D_4
392	1	-7	D_4
400	1	-4, -20, 5	V_4
432	1	-3	D_4
441	1	-3, -7, 21	V_4
512	1	-4	D_4
513	1	-3	D_4
549	1	-3	D_4
576	1	-3, -8, 24	V_4
576	1	-3, -24, 8	V_4
656	1	-4	D_4
657	1	-3	D_4
784	1	-4, -7, 28	V_4
832	1	-4	D_4
837	1	-3	D_4
873	1	-3	D_4
981	1	-3	D_4
1008	1	-3	D_4
1008	1	-3	D_4
1089	1	-3, -11, 33	V_4
1161	1	-3	D_4
1197	1	-3	D_4
1197	1	-3	D_4
1372	1	-7	D_4
1521	2	-3, -39, 13	V_4
2048	1	-8	D_4
2197	1	13	$\mathbb{Z}/4\mathbb{Z}$

To close this section we show that the ring of integers A of the cubic field K with discriminant -283 has a Euclidean ideal class. We have $h(A) = 2$. The ring A is given by $A = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2$, with $\theta^3 + 4\theta + 1 = 0$. The ideal p of norm 2 is non-principal and it is given by $p = \mathbb{Z}\cdot 2 + \mathbb{Z}(\theta + 1) + \mathbb{Z}(\theta^2 + 1)$.

As usual we embed K in $K_S = \mathbb{R} \times \mathbb{C}$, where $S = S_\infty$. The $\mathbb{R}$-coordinate of an element $\alpha \in K_S$ will be denoted by α_r, the $\mathbb{C}$-coordinate by α_c. We have $\theta_r = -0.24626617$ and $\theta_c = 0.12313309 + i \times 2.01133917$.

The orthogonal projection of K_S onto $\mathbb{C}$ will be denoted by π. Let V be the plane in K_S, spanned by 1 and θ. The ideal p intersects V in a lattice Γ of V, spanned by 2 and $1 + \theta$. The projection $\pi\Gamma$ is a lattice of $\mathbb{C}$ and the fundamental hexagon of $\pi\Gamma$ will be denoted by H, cf. (3.4). The measure $\mu(H)$ is equal to $4|\mathrm{Im}\,\theta_c| = 8.04535668$, where μ is the measure on $\mathbb{C}$ defined by (3.12)(a), i.e. twice the usual measure. Let H' be the inverse image of H in V. Consider the set $B = H' + \{(x,0) \in \mathbb{R} \times \mathbb{C} : |x| \le c\}$, with $c = \sqrt{283}\cdot\mu(H)^{-1} = 2.09097055$. We have $B + \Gamma = V + \{(x,0) \in \mathbb{R} \times \mathbb{C} : |x| \le c\}$. Because $\mu_S(B) = 2\sqrt{283}$ the set B is a fundamental domain of p.

Figure 23 shows the sets B and H. It is a central projection of $\mathbb{R} \times \mathbb{C}$ from the point $M = (13, 2.8 - 15i)$ onto a plane perpendicular to the line OM. Figure 23 also gives the basis points 2, $\theta + 1$ and $\theta^2 + 1$ of p and their projections onto $\mathbb{C}$ and onto the real axis of $\mathbb{C}$. The cylinder depicted in figure 23 will be discussed below.

We will show that B is contained in $V_2 + p = \{x \in K_S : \exists\, \alpha \in p$ such that $N(x-\alpha) < 2\}$. This proves that p is Euclidean. For each $\alpha \in p$ let T_α be the largest open cylinder in K_S, of which the axis passes through α and is parallel to the $\mathbb{R}$-axis, and such that $T_\alpha \cap (B+V)$ is contained in $\alpha + V_2$. Figure 23 shows how such a cylinder T_α should look like. It will be enough to show that $B \subset \bigcup_{\alpha\in p} T_\alpha$. Let C_α be the disc that is the intersection of T_α with the $\mathbb{C}$-plane. We have $B \subset \bigcup_{\alpha\in p} T_\alpha$ if and only if $H \subset \bigcup_{\alpha\in p} C_\alpha$. In figure 24 we see that we already have $H \subset \bigcup_{\alpha\in T} C_\alpha$, where T consists of the 11 elements of p listed in table 25 and their negatives. We conclude that p is Euclidean.

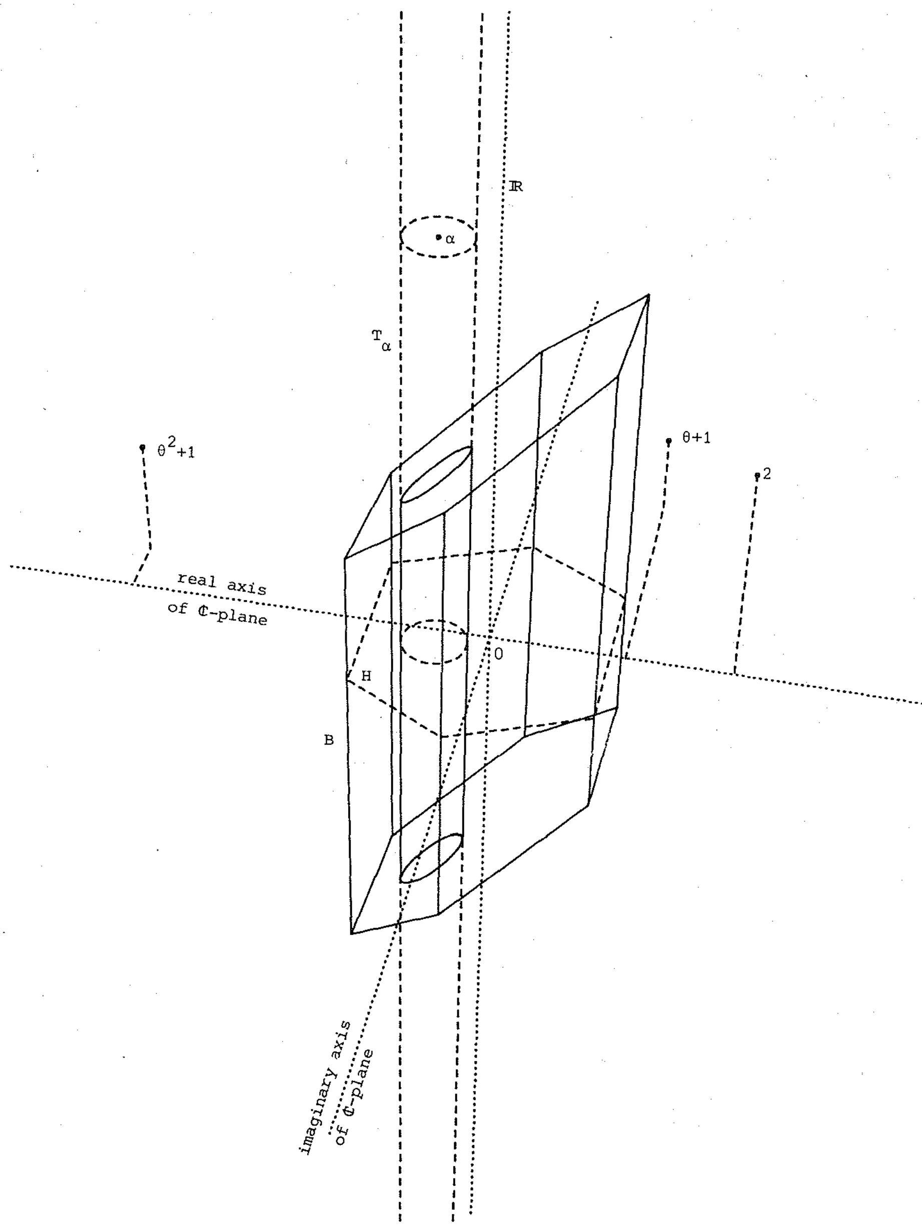
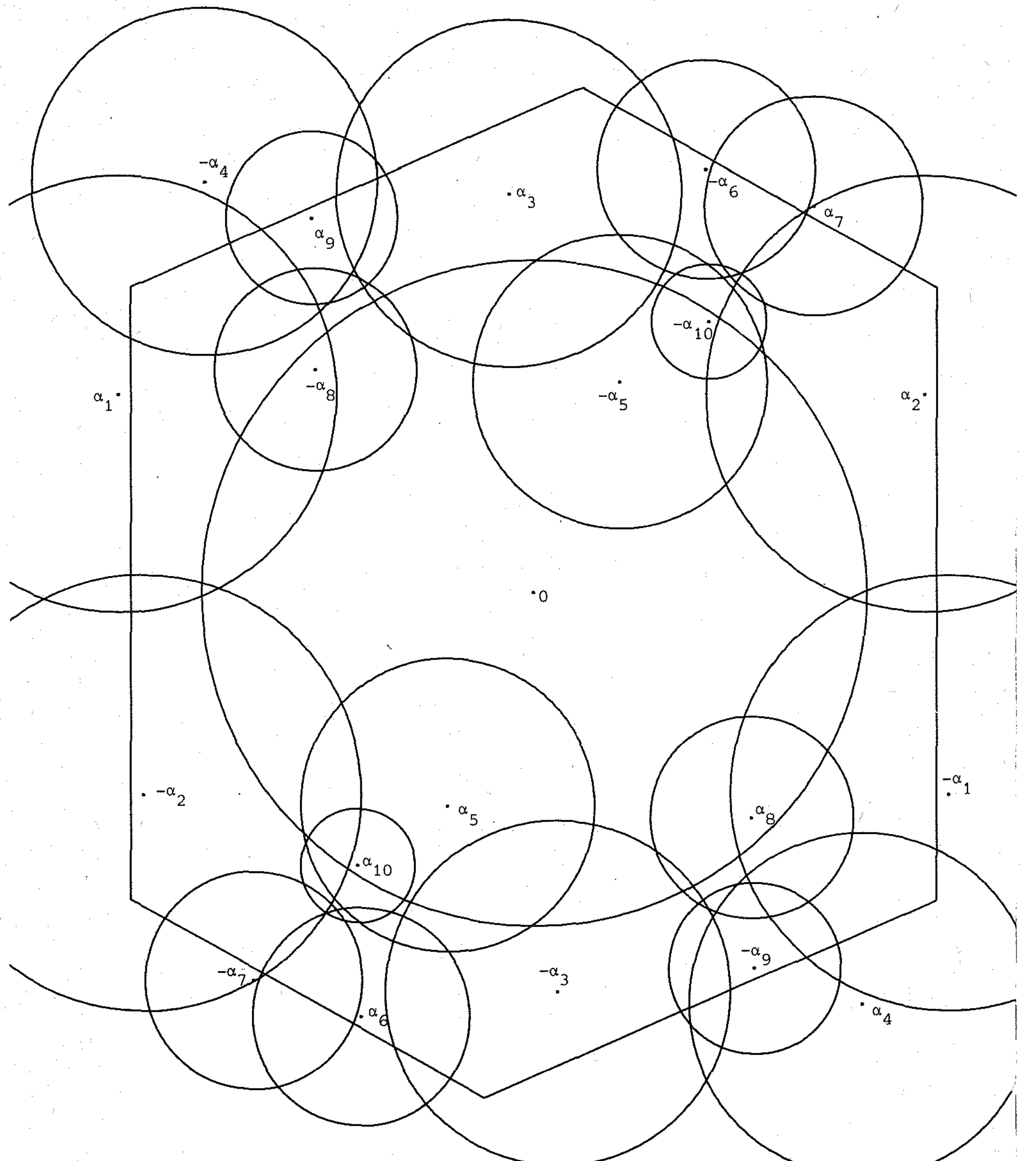

ℝ
α
T_α
θ^2+1
θ+1
2
real axis
of ℂ-plane
0
H
B
imaginary axis
of ℂ-plane

fig. 23



$-\alpha_4$
α_9
α_3
$-\alpha_6$
α_7
$-\alpha_{10}$
$-\alpha_8$
α_1
$-\alpha_5$
α_2
0
$-\alpha_1$
$-\alpha_2$
α_5
α_8
α_{10}
$-\alpha_7$
$-\alpha_3$
$-\alpha_9$
α_6
α_4

fig. 24

TABLE 25. Elements and circles in figure 24.

element	real	complex	radius
0	0	0	0.8445
$\alpha_1 = 3 + \theta^2$	3.0606	$-1.0303 + 0.4953\,i$	0.5514
$\alpha_2 = 5 + \theta^2$	5.0606	$0.9697 + 0.4953\,i$	0.5514
$\alpha_3 = 8 + 2\theta^2$	8.1213	$-0.0606 + 0.9906\,i$	0.4335
$\alpha_4 = 9 - \theta + 2\theta^2$	9.3676	$0.8162 - 1.0207\,i$	0.4335
$\alpha_5 = 12 - \theta + 3\theta^2$	12.4282	$-0.2141 - 0.5254\,i$	0.3680
$\alpha_6 = 24 - 2\theta + 6\theta^2$	24.8564	$-0.4282 - 1.0507\,i$	0.2709
$\alpha_7 = 25 - \theta + 6\theta^2$	25.6101	$0.6949 + 0.9606\,i$	0.2709
$\alpha_8 = 29 - 2\theta + 7\theta^2$	29.9171	$0.5415 - 0.5554\,i$	0.2523
$\alpha_9 = 40 - 2\theta + 10\theta^2$	41.0990	$-0.5495 + 0.9306\,i$	0.2133
$\alpha_{10} = 93 - 6\theta + 23\theta^2$	95.8725	$-0.4362 - 0.6756\,i$	0.1426

REFERENCES

An asterisk (*) marks that the work has not been available to the author. The pages where a paper is quoted are given by the number following the word Cit.

[Ar1] ARMITAGE, J.V., *Euclid's algorithm in certain algebraic function fields,* proc. Lond. Math. Soc. (3) 7 498-509 (1957). Cit. 4.

[Ar2] ARMITAGE, J.V., *Euclid's algorithm in algebraic function fields,* J. Lond. Math. Soc. 38 55-59 (1963). Cit. 4.

[AT] ARTIN, E., - Tate, J., *Class field theory,* New York: Benjamin (1967). Cit. 50.

[BSD1] BARNES, E.S. - SWINNERTON-DYER, H.P.F., *The inhomogeneous minima of binary quadratic forms (I),* Acta Math. 87 259-323 (1952). Cit. 3; 15; 25; 57.

[BSD2] BARNES, E.S. - SWINNERTON-DYER, H.P.F., *The inhomogeneous minima of binary quadratic forms (II),* Acta Math. 88 279-316 (1952). Cit. 25; 57.

[BR] BEHRBOHM, H. - RÉDEI, L., *Der Euklidische Algorithmus in quadratischen Körpern,* J. reine angew. Math. 174 192-205 (1936). Cit. 15; 16.

[Be] BERG, E., *Über die Existenz eines Euklidischen Algorithmus in quadratischen Zahlkörpern,* Kungl. Fysiogr. Sällsk. i Lund Förh. 5 nr.5 53-58 (1935). Cit. 15.

[BS] BOREWICS, S.I. - ŠAFAREVIČ, I.R., *Zahlentheorie,* German translation by H. Koch from Russian original, Basel: Birkhäuser Verlag (1966). Cit. 7; 33; 35; 96; 181.

[Br] BRAUER, A., *On the non-existence of the Euclidean algorithm in certain quadratic number fields,* Am. J. Math. 62 697-716 (1940). Cit. 16.

[BP] BROWN, E., - PARRY, C.J., *The imaginary bicyclic biquadratic fields with class number 1,* J. reine angew. Math. 266 (1974) 118-120. Cit. 183.

[Bu] BUELL, D.A., *Small class numbers and extreme values of L-functions of quadratic fields,* Math. Comput. 31 786-796 (1977). Cit. 163.

[BWW] BUELL, D.A. - WILLIAMS, H.C. - WILLIAMS, K.S., *On the imaginary bicyclic biquadratic fields with class-number 2*, Math. Comput. 31 1034-1042 (1977). Cit. 182.

[Ca] CAYLEY, A., *Tables des formes quadratiques binaires pour les déterminants négatifs depuis* D = -1 *jusqu'à* D = -100, *pour les déterminants positifs non carrés depuis* D = 2 *jusque'à* D = 99 *et pour les treize déterminants négatifs irréguliers qui se trouvent dans le premier millier*, J. reine angew. Math. 60 357-372 (1862); Collected papers 5 141-156, Cambridge University Press (1892). Cit. 35.

[C1] CASSELS, J.W.S., *The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms*, Proc. Camb. Philos. Soc. 48 72-86/519-20 (1952). Cit. 4; 17; 60; 70.

[C2] CASSELS, J.W.S., *An introduction to the geometry of numbers*, Berlin-Heidelberg-New York: Springer Verlag (1971^2). Cit. 35; 45.

[CF] CASSELS, J.W.S. - FRÖHLICH, A. (eds.), *Algebraic number theory*, London-New York: Academic Press (1967). Cit. 7; 20; 25; 27; 29; 38; 41; 43; 44; 78; 158; 164; 169; 171.

[Č] ČEBOTAREV, N. (TSCHEBOTAREFF, N.), *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. 95 191-228 (1925/6). Cit. 25.

[Ch] CHATLAND, H., *On the Euclidean algorithm in quadratic number fields*, Bull. Am. Math. Soc. 55 948-953 (1949). Cit. 17.

[CD] CHATLAND, H. - DAVENPORT, H., *Euclids algorithm in real quadratic fields*, Can. J. Math. 2 289-296 (1950); H. Davenports collected works I, London-New York-San Francisco: Academic Press 366-373 (1977). Cit. 3; 17; 24.

[Cv] CHEVALLEY, C., *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys VI, New York: Am. Math. Soc. (1951). Cit. 4.

[Ci] CIOFFARI, V.G., *The Euclidean condition in pure cubic and complex quartic fields*, Math. Comput. 33 389-398 (1979). Cit. 17; 185.

[Da1] DAVENPORT, H., *Indefinite binary quadratic forms*, Q.J. Math. Oxf. (2) 1 54-62 (1950); Collected works I, London-New York-San Francisco: Academic Press 395-403 (1977). Cit. 17.

[Da2] DAVENPORT, H., *L'algorithme d'Euclide dans certains corps algébriques*, Coll. intern. du Centre de la recherche sci. XXIV, Algèbre et théorie des nombres, Paris 25 sept. - 1 oct. 1949, CNRS, Paris 41-43 (1950). Cit. 3.

[Da3] DAVENPORT, H., *Euclid's algorithm in cubic fields of negative discriminant*, Acta Math. 84 159-179 (1950); Collected works I, London-New York-San Francisco: Academic Press 374-394 (1977). Cit. 3.

[Da4] DAVENPORT, H., *Euclid's algorithm in certain quartic fields*, Trans. Am. Math. Soc. 68 508-532 (1950); Collected works I, London-New York-San Francisco: Academic Press 404-428 (1977). Cit. 3.

[Da5] DAVENPORT, H., *Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields*, Proc. Lond. Math. Soc. (2) 53 65-82 (1951); Collected works I, London-New York-San Francisco: Academic Press 344-361 (1977). Cit. 3; 17.

[De] DEURING, M., *Lectures on the theory of algebraic functions of one variable*, Berlin-Heidelberg-New York: Springer Verlag LNM 314 (1973). Cit. 4; 6; 50.

[Di] DICKSON, L.E., *Algebren und ihre Zahlentheorie*, German translation of English original by J.J. Burckhardt and E. Schubarth, Zürich-Leipzig: Orell Füssli Verlag (1927). Cit. 3; 14.

[D1] DIRICHLET, P.G. LEJEUNE, *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes*, J. reine angew. Math. 24 291-371 (1842); Werke I, Berlin: Georg Reimer 533-618 (1889). Cit. 14.

[D2] DIRICHLET, P.G. LEJEUNE, *Über die Reduction der positiven quadratischen Formen mit drei unbestimmten ganzen Zahlen*, J. reine angew. Math. 40 209-277 (1850); Werke II, Berlin: Georg Reimer 27-48 (1897). Cit. 35.

[D3] DIRICHLET, P.G. LEJEUNE, *Vorlesungen über Zahlentheorie*, reprint of 4-th edition Braunschweig (1893), New York: Chelsea (1968). Cit. 3; 14; 15.

[Ei] EISENSTEIN, G., *Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhangt, nebst Anwendungen derselben auf die Zahlentheorie*, J. reine angew. Math. 39 224-287 (1850); Mathematische Werke II, New York: Chelsea 556-619 (1975). Cit. 14.

[E] ENNOLA, V., *On the first inhomogeneous minimum of indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields*, Ann. Univ. Turku. Ser. A I Tom. 28 (1958). Cit. 17; 72; 165.

[ECK] ERDÖS, P. - CHAO KO, *Note on the Euclidean algorithm*, J. Lond. Math. Soc. 13 3-8 (1938). Cit. 16.

[Eu] EUCLID, *The thirteen books of the elements II*, English translation by Sir Th. L. Heath. New York: Dover (1956). Cit. 1.

[F]* FOX KESTON, J., *Finiteness of the number of quadratic fields with even discriminant and Euclid algorithm*, Yale Univ. Ph.D. Thesis (1935). cf. Bull. Am. Math. Soc. 41 186 (1935). Cit. 15.

[G1] GAUSS, C.F., *Disquisitiones arithmeticae*, Werke I, Königlichen Gesellschaft der Wissenschaften: Göttingen (1870); German translation by H. Maser: *Untersuchungen über höhere Arithmetik*, New York: Chelsea (1965). Cit. 15; 34; 35.

[G2] GAUSS, C.F., *Zur Theorie der complexen Zahlen*, Werke II, Göttingen: Königlichen Gesellschaft der Wissenschaften 387-398 (1876). Cit. 2; 14.

[G3] GAUSS, C.F., *Theoria Residuorum Biquadraticorum II*, Comm. Soc. reg. sc. Gotting. recentiores VII (1832); Werke II, Göttingen: Königlichen Gesellschaft der Wissenschaften 93-148 (1876); German translation by H. Maser: *Theorie der biquadratische Reste, Untersuchungen über höhere Arithmetik*, New York: Chelsea 511-588 (1965). Cit. 2; 14.

[Go] GODWIN, H.J., *On Euclid's algorithm in some cubic fields with signature one*, Q.J. Math. Oxf. (2) 18 333-338 (1967). Cit. 184.

[HW] HARDY, G.H. - WRIGHT, E.M., *An introduction to the theory of numbers*, Oxford: Clarendon Press (1979^5). Cit. 14; 15.

[Ha] HARTSHORNE, R., *Algebraic Geometry*, New York-Heidelberg-Berlin: Springer Verlag (1977). Cit. 4; 6.

[H1] HASSE, H., *Number theory*, English translation by H.G. Zimmer, Berlin-Heidelberg-New York: Springer Verlag (1980). Cit. 7; 15; 19.

[H2] HASSE, H., *Über die Klassenzahl abelscher Zahlkörper*, Berlin: Akademie Verlag (1952). Cit. 174; 175; 176.

[He] HEILBRONN, H., *On Euclid's algorithm in real quadratic fields*, Proc. Camb. Philos. Soc. 34 521-526 (1938). Cit. 16.

[Ho] HOFREITER, N., *Quadratische Körper mit und ohne euklidischen Algorithmus*, Monatsh. Math. Phys. 42 397-400 (1935). Cit. 15.

[Hu] HUA, L.K., *On the distribution of quadratic non-residues and the Euclidean algorithm in real quadratic fields I*, Trans. Am. Math. Soc. 56 537-546 (1944). Cit. 16.

[HM] HUA, L.K. - MIN, S.H., *On the distribution of quadratic non-residues and the Euclidean algorithm in real quadratic fields II*, Trans. Am. Math. Soc. 56 547-569 (1944). Cit. 17.

[HS] HUA, L.K. - SHIH, W.T., *On the lack of an Euclidean algorithm in* $R(\sqrt{61})$, Am. J. Math. 67 209-211 (1945). Cit. 17.

[Iy] IYANAGA, S., (ed), *The theory of numbers*, Amsterdam-Oxford-New York: North-Holland/American Elsevier (1975). Cit. 7; 19; 37; 38; 40; 41; 42; 44; 45; 111.

[I] INCE, E.L., *Cycles of reduced ideals in quadratic fields*, Cambridge University Press (1968). Cit. 73; 74; 75; 182.

[In] INKERI, K., *Über den Euklidischen Algorithmus in quadratischen Zahlkörpern*, Ann. Acad. Sci. Fenn. ser. A 41 1-35 (1947). Cit. 17.

[K] KUMMER, E.E., *Two letters to Kronecker, October 2 and October 16 1844*, Collected papers I, Berlin-Heidelberg-New York: Springer Verlag 87-92 (1975). Cit. 2; 14; 177.

[Lk] LAKEIN, R.B., *Euclid's algorithm in complex quartic fields*, Acta Arith. 20 393-400 (1972). Cit. 185.

[La1] LANG, S., *Diophantine geometry*, New York-London: John Wiley & Sons (1962). Cit. 9.

[La2] LANG, S., *Algebraic number theory*, Reading etc.: Addison-Wesley (1970). Cit. 7; 9; 18; 20; 25; 94.

[Le] LEKKERKERKER, C.G., *Geometry of numbers*, Amsterdam-London: North-Holland (1969). Cit. 47.

[L1] LENSTRA jr. H.W., *Lectures on Euclidean rings*, Bielefeld (1974). Cit. 25.

[L2] LENSTRA jr. H.W., *Euclid's algorithm in cyclotomic fields*, J. Lond. Math. Soc. (2) 10 457-465 (1975). Cit. 14.

[L3] LENSTRA jr. H.W., *Euclidean number fields of large degree*, Invent. Math. 38 237-254 (1977). Cit. 185.

[L4] LENSTRA jr. H.W., *Quelques exemples d'anneaux Euclidiens*, C.R. Acad. Sci., Paris 286 ser. A 683-685 (1978). Cit. 14.

[L5] LENSTRA jr. H.W., *Euclidean ideal classes*, Astérisque 61 121-131 (1979). Cit. 20; 27; 184; 185.

[L6] LENSTRA jr. H.W., *Euclidean number fields 1*, Math. Intell. 2 6-15 (1979). Cit. 158.

[L7] LENSTRA jr. H.W., *On the calculation of regulators and class numbers of quadratic fields*, J.V. Armitage (ed.), Journées Arithmétiques 1980, Cambridge University Press, LMS Lecture Notes Series 56 123-150 (1982). Cit. 35.

[Ma] MARTINET, J., *Petits discriminants des corps de nombres*, J.V. Armitage (ed.) Journées Arithmétiques 1980, Cambridge University Press, LMS Lecture Notes Series 56 151-193 (1982). Cit. 164; 168.

[M1] MASLEY, J.M., *On Euclidean rings of integers in cyclotomic fields*, J. reine angew. Math. 272 45-48 (1975). Cit. 14.

[M2] MASLEY, J.M., *Solution of small class number problems for cyclotomic fields*, Compos. Math. 33 179-186 (1976). Cit. 157.

[MM] MASLEY, J.M. - MONTGOMERY, H.L., *Cyclotomic fields with unique factorization*, J. reine angew. Math. 286/287 248-256 (1976). Cit. 14; 157.

[Oj] OJALA, T., *Euclid's algorithm in the cyclotomic field* $\mathbb{Q}(\zeta_{16})$, Math. Comput. 31 268-273 (1977). Cit. 14; 178.

[Op] OPPENHEIM, A., *Quadratic fields with and without Euclid's algorithm*, Math. Ann. 109 349-352 (1934). Cit. 14; 15.

[O] OUSPENSKY, J., *Note sur les nombres entiers dépendent d'une racine cinquième de l'unité*, Math. Ann. 66 109-112 (1909). Cit. 14; 178.

[P] PERRON, O., *Quadratische Zahlkörper mit Euklidischem Algorithmus*, Math. Ann. 107 489-495 (1933). Cit. 15; 185.

[Q] QUEEN, C.S., *Arithmetic Euclidean rings*, Acta Arith. 26 105-113 (1972). Cit. 25.

[Ré1]* RÉDEI, L., *Euklides algoritmusáról valós másodfokú számtestekben*, Mat. és Fiz. Lapok 47 78-89 (1940). Cit. 16.

[Ré2] RÉDEI, L., *Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern*, J. reine angew. Math. 183 183-192 (1941). Cit. 16.

[Ré3] RÉDEI, L., *Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern*, Math. Ann. 118 588-608 (1942). Cit. 3; 15; 16.

[R1] REMAK, R., *Über die geometrische Darstellung der indefiniten binären quadratischen Minimalformen*, Jahresber. Dtsch. Math.-Ver. 33 228-245 (1925). Cit. 14.

[R2] REMAK, R., *Über den Euklidischen Algorithmus in reell-quadratischen Zahlkörpern*, Jahresber. Dtsch. Math.-Ver. 44 238-250 (1934). Cit. 14; 15.

[S] SAMUEL, P., *About Euclidean rings*, J. Algebra 19 282-301 (1971). Cit. 6; 52.

[Sc] SCHUSTER, L., *Reellquadratische Zahlkörper ohne Euklidischen Algorithmus*, Monatsh. Math. Phys. 47 117-127 (1939). Cit. 16.

[Se] SERRE, J.-P., *Groupes algébriques et corps de classes*, Paris: Hermann (1959). Cit. 4.

[Sh] SHANKS, D., *Class number, a theory of factorization, and genera*, Proc. Symp. pure Math. 20 AMS 415-440 (1970). Cit. 35.

[St] STARK, H.M., *On complex quadratic fields with class-number two*, Math. Comput. 29 289-302 (1975). Cit. 182.

[Sv] STEVIN, Simon, *L'Arithmetique II. Livre*, in The Principal works of Simon Stevin II B, Amsterdam: Swets & Zeitlinger (1958). Cit. 13.

[T] TAYLOR, E.M., *Euclid's algorithm in cubic fields with complex conjugates*, J. Lond. Math. Soc. (2) 14 49-54 (1976). Cit. 184.

[vdW] WAERDEN VAN DER, B.L., *Algebra I*, Berlin-Heidelberg-New York: Springer Verlag (1971[8]). Cit. 12; 20.

[Wa] WASHINGTON, L.C., *Introduction to cyclotomic fields*. Berlin-Heidelberg-New York: Springer Verlag (1982). Cit. 163; 170; 173; 174; 175; 181; 182.

[We1] WEIL, A., *Basic number theory*, Berlin-Heidelberg-New York: Springer Verlag (1974[3]). Cit. 56.

[We2] WEIL, A., *Foundations of algebraic geometry*, AMS colloquium publications XXIX, New York: Am. Math. Soc. (1946). Cit. 4.

[We3] WEIL, A., *Courbes algébriques et variétés abéliennes*, Paris: Hermann (1971). Cit. 4.

[W] WEISS, E., *Algebraic number theory*, New York: Chelsea (1976[2]). Cit. 7; 9; 11; 18; 19; 20; 43; 158; 159; 163; 168; 174.

[YH] YOSHINO, K. - HIRABAYASHI, M., *On the relative class number of the imaginary abelian number field I/II*, Mem. Coll. of lib. Arts, Kanazawa Med. Univ. 9 5-53 (1981)/10 33-81 (1982). Cit. 174; 175.

[ZS] ZARISKI, O. - SAMUEL, P., *Commutative algebra II*, New York-Heidelberg-Berlin: Springer Verlag (1960). Cit. 9.

NEDERLANDSE SAMENVATTING

EUCLIDISCHE RINGEN MET TWEE ONEINDIGE PRIEMEN

In 1948 werd de bepaling van de Euclidische ringen van gehelen van reële kwadratische lichamen voltooid. Al spoedig hierna bleek dat de gebruikte methode ook toepasbaar is op ringen van gehelen van zekere 3^e en 4^e graads lichamen. De voor deze ringen verkregen grenzen zijn echter zo groot dat de volledige bepaling van Euclidische ringen ondoenlijk is. Omstreeks 1960 werd met succes dezelfde techniek gebruikt voor zekere ringen in functielichamen over een eindig lichaam.

De bovengenoemde resultaten zijn alle een gevolg van een algemene stelling, bewezen in dit proefschrift, die beperkingen oplegt aan Euclidische ringen met twee oneindige priemen in globale lichamen. De oneindige priemen van zo'n ring zijn de equivalentieklassen van valuaties van het quotiëntenlichaam die *niet* afkomstig zijn van een priemideaal van de ring. Een groot deel van het proefschrift is gewijd aan de bepaling van de Euclidische ringen met twee oneindige priemen in imaginaire kwadratische lichamen. Dit is de enige klasse van ringen met twee oneindige priemen die nog niet eerder onderzocht is. Uiteindelijk komen we met een volledige classificatie van de Euclidische ringen in deze klasse. In het laatste hoofdstuk behandelen we ringen van gehelen van enkele speciale klassen van 4^e graads lichamen. In het bijzonder bepalen we alle Euclidische ringen van gehelen van totaal imaginaire 4^e graads lichamen waarvan de Galois groep over $\mathbb{Q}$ cyclisch is.

ACKNOWLEDGEMENTS

The research for this thesis was supported by the Netherlands Organization for the Advancement of Pure Research (ZWO). I thank the Mathematical Institute of the University of Amsterdam for letting me use an office, the library and the CDC - Cyber 170-750 computer at the SARA computing centre in Amsterdam. Most computations were done on this machine. In particular most figures are drawn on the Calcomp-plotter of SARA.

I am grateful to those who helped me in transforming the manuscript into a book. These are: mrs. Irene Cannegieter and mrs. Miep Wuck, who typed the manuscript; Wieb Bosma, Peter Stevenhagen, Rob Versseput and my father C.A.M. van der Linden, who did the proof-reading; finally my sister Agnes van der Linden, who designed the front page.

I express my thanks to my supervisor prof.dr. H.W. Lenstra jr., not in the last place for his invitations to cultural and social events.

february 1984 F.J. van der Linden

INDEX

NOTATION

	page		page
A	18, 77, 158	f_p	6, 52
A_0	158, 181	$g(K)$	6,38
A^*	20	$\gcd(a,b)$	1
$\mathcal{A}_K$	41	$h(A)$	18
A_S	5, 9, 10	$h(K)$	18
$a^{\perp}$	42, 43	I	18
a_i	164	K_0	158, 164, 171, 181
a_r	164	K_p	18
C_S	47, 48	K_S	40
$C(F)$	5	N	1, 10, 19, 158
$c\hat{}$	159	N_0	158
$Cl(A)$	18	$\mathcal{N}$	20, 158
$Cl(K)$	18	$\mathcal{N}_0$	158
$\mathcal{D}(\cdot)$	37, 158	$\tilde{N}$	158
$\mathcal{D}_t$	38	$\mathcal{N}$	77
$\mathcal{D}_t(\cdot)$	44	$\mathcal{O}$	1, 77
$\deg(p)$	5	$\mathcal{O}_p$	8
$\overline{\mathbb{F}}_q$	5	$\tilde{\mathcal{O}}_p$	19
$\mathbb{F}_q((t))$	37, 38	$\mathcal{O}(K)$	1
$\mathbb{F}_q[[t]]$	37, 38	$\mathrm{ord}_p(\cdot)$	19, 20
$\hat{f}$	39	$\mathbb{P}^1$	5
f_i	110	$\tilde{p}$	19

LIST OF TABLES

LIST OF FIGURES

STELLINGEN

behorende bij het proefschrift

'Euclidean rings with two infinite primes'

van

F. J. van der Linden.

1. Zij $K = \mathbb{Q}(\cos(2\pi/m))$, met $0 < m \leq 200$. Als $\varphi(m) \leq 66$ dan geldt

$$h(K) = 2 \quad \text{als} \quad m = 136;$$
$$h(K) = 1 \quad \text{als} \quad m \neq 136;$$

hierbij is φ de Euler-functie en $h(K)$ het klassengetal van K. Stel dat de gegeneraliseerde Riemannhypothese geldt voor het Hilbertklassenlichaam van K. Als $\varphi(m) \leq 162$ dan geldt

$$h(K) = 4 \quad \text{als} \quad m = 163 \text{ of } m = 183;$$
$$h(K) = 2 \quad \text{als} \quad m = 136 \text{ of } m = 145;$$
$$h(K) = 1 \quad \text{voor de andere } m.$$

Lit. F.J. van der Linden, Class number computations of real abelian number fields. Math. Comput. 39 693-707 (1982).

2. Zij $K = \mathbb{Q}(\cos(2\pi/256))$. Als de gegeneraliseerde Riemannhypothese geldt voor het Hilbertklassenlichaam van K dan is $h(K) = 1$. In ieder geval zijn de idealen van norm ≤ 100000 hoofdidealen.

3. Een kort spel is een spel dat door twee personen gespeeld kan worden en waarvoor het aantal mogelijke zetten begrensd is, zelfs als de spelers niet om de beurt zetten. De korte spellen vormen op een natuurlijke manier een groep. De torsieondergroep hiervan is isomorf met een aftelbaar oneindige som van copieën van $\mathbb{Q}_2/\mathbb{Z}_2 \simeq \bigcup_{n\in\mathbb{Z}_{\geq 0}} (2^{-n}\,\mathbb{Z}/\mathbb{Z})$.

Lit. J.H. Conway, On numbers and games. London, New York, San Francisco: Academic Press (1977^2).

4. Zij P de verzameling priemen van $\mathbb{Q}$, i.e. P bestaat uit ∞ en de priemgetallen. Zij $a(p) \in \mathbb{Z}_{\geq 0}$ voor $p \in P$. Beschouw de topologische groep $V = \prod'_{p \in P} \mathbb{Q}_p^{a(p)}$, het beperkte directe product met betrekking tot de $\mathbb{Z}_p^{a(p)}$, waarbij $\mathbb{Q}_\infty = \mathbb{Z}_\infty = \mathbb{R}$. De groep V bevat roosters (lattices), zoals gedefinieerd in (3.16) van dit proefschrift, dan en slechts dan als $a(p) \leq a(\infty)$ voor alle $p \in P$.

5. Laat P zijn als in stelling 4 en laat $A = A_{\mathbb{Q}}$ de adèle ring van $\mathbb{Q}$ zijn (zie §(3.4) van dit proefschrift). Voor $\alpha = (\alpha_p)_{p \in P} \in A$ definiëren we $|\alpha| = \max_{p \in P} |\alpha_p|_p$. Het beperkte directe product $V = \prod'_{p \in P} \mathbb{Q}_p^{a(p)}$, met $a(p) \in \mathbb{Z}_{\geq 0}$, is door coördinaatsgewijze vermenigvuldiging een A-moduul. Voor $p \in P$ en $x \in V$ geven we met x_p de coördinaat in $\mathbb{Q}_p^{a(p)}$ aan.

Zij μ een Haarmaat op V en zij B een deelverzameling van V. We noemen B *convex* als geldt

(a) Voor alle $x,y \in B$ en alle $\lambda \in A$ met $|\lambda| \leq 1$ en $|1-\lambda| \leq 1$ geldt dat $\lambda x + (1-\lambda)y \in B$; en

Voor alle $x,y,z \in B$ met $x_3 = y_3 = z_3$ geldt dat $\frac{1}{3}(x+y+z) \in B$.

Er geldt dat een verzameling B convex is dan en slechts dan als B aan de volgende eigenschap voldoet

(b) $B = C \times D$ met $C \subset \mathbb{R}^{a(\infty)}$ convex en D een nevenklasse van een deel $\prod_{p \neq \infty} \mathbb{Z}_p$-moduul van $\prod'_{p \neq \infty} \mathbb{Q}_p^{a(p)}$.

6. Laat V zijn als in stelling 4 en laat μ een Haarmaat zijn op V. Een deelverzameling B van V heet *symmetrisch* als geldt $B = \{-x : x \in B\}$. De stelling van Minkowski kan als volgt gegeneraliseerd worden:

Zij Γ een rooster in V met determinant $\nu(\Gamma)$, zie (3.18) van dit proefschrift, en zij B een meetbare, convexe, symmetrische deelverzameling van V met $\mu(B) > 2^{a(\infty)}\nu(\Gamma)$. Dan geldt $\Gamma \cap B \neq \{0\}$.

Lit. E. Bombieri - J. Vaaler, On Siegels Lemma, Invent. Math. 73 11-32 (1983).

7. Zij q een priemmacht en zij voor $m,n \in \mathbb{Z}_{>0}$ de functie $\varphi(m,n)$ gedefiniëerd door

$$\varphi(m,n) = \#\{f \in \mathbb{F}_q[x]: \ f \text{ monisch}, \ \deg(f) = m, \ \forall\, g|f, \ g \text{ irreducibel} \Rightarrow \deg(g) \le n\}.$$

De Dickman-De Bruijn functie ρ op $\mathbb{R}$ is inductief gedefinieerd door

$$\rho(u) = 0 \quad \text{voor} \quad u < 0;$$

$$\rho(u) = 1 \quad \text{voor} \quad 0 \le u \le 1;$$

$$\rho(u) = \rho(u-1) - \int_{u-1}^{u} \frac{1}{s}\rho(s-1)ds \quad \text{voor} \quad u > 1.$$

Laten $c,d \in \mathbb{R}_{>0}$ zijn en $n(m) \in \mathbb{Z}_{>0}$ voor $m \in \mathbb{Z}_{>0}$ zodat $|m - c\cdot n(m)| < d$. Dan geldt

$$\lim_{m\to\infty} q^{-m}\varphi(m,n(m)) = \rho(c)$$

uniform op gebieden $c \le c_0$, $d \le d_0$ en uniform in q.

Lit. D.E. Knuth, L. Trabb Pardo, Analysis of a simple factorization algorithm, Theor. Comput. Sci. 3 (1976) 321-348.
N.G. de Bruijn, On the number of positive integers $\le x$ and free of prime factors $> y$, Indagationes Math. 13 (1951) 50-60.
K. Dickman, On the frequency of numbers containing prime factors of a certain relative magnitude, Ark. Nat. Astr. Fys. 22 (1930), A10, 1-14.

8. Zij K een functielichaam van een complete niet singuliere kromme E van geslacht 1 over een eindig lichaam $\mathbb{F}_q$, waarvoor de 2-torsie ondergroep van $E(\mathbb{F}_q)$ *niet* isomorf is met $\mathbb{Z}/2\mathbb{Z}$.

Laat S een niet-lege verzameling van priemen van K zijn en laat A_S de ring zijn als gedefinieerd door (0.4) in dit proefschrift.

Dan geldt:

De ring $\{f \in K[x] : f[A_S] \subset A_S\}$ heeft als A_S-moduul een basis $(f_i)_{i \in \mathbb{Z}_{\ge 0}}$, met $\deg(f_i) = i$ dan en slechts dan als de exponent van de klassengroep $Cl(A_S)$ een deler is van $\#E(\mathbb{F}_q)$.

Een analoog resultaat geldt voor het geval dat de 2-torsie ondergroep van $E(\mathbb{F}_q)$ wel isomorf is met $\mathbb{Z}/2\mathbb{Z}$.

Lit. H. Zantema, Integer valued polynomials in algebraic number theory, Proefschrift 1983.

9. Het op authentieke wijze uitvoeren van 18^e eeuwse muziek is in tegenstelling tot wat de naamgeving suggereert een moderne wijze van uitvoeren van deze muziek.

10. Bij het klokkijken komt het vaak niet op een paar minuten aan. Digitale klokken zijn geen vooruitgang omdat ze nabijgelegen tijdstippen niet met nabijgelegen visuele beelden aangeven.

11. "Doch het kon zijn - hij wist het niet stellig - dat het met den musicus eenigermate ging als met den wiskundige, die voor talen en litteratuur niet pleegt te voelen, terwijl gewoonlijk de taalkundige het tegendeel van eenzijdig is."

F. Bordewijk, Eiken van Dodona, Nijgh & Van Ditmar 1946, p.148.

Bordewijk heeft blijkbaar geen wiskundigen gekend.