Astérisque

ARMIN LEUTBECHER
JACQUES MARTINET

Lenstra's constant and euclidean number fields

Astérisque, tome 94 (1982), p. 87-131
<http://www.numdam.org/item?id=AST_1982__94__87_0>

LENSTRA'S CONSTANT AND EUCLIDEAN NUMBER FIELDS

by

Armin LEUTBECHER and Jacques MARTINET

-:-:-:-

1. - Introduction

A. Hurwitz([8]) puts at the very beginning of his "Theorie der algebraischen Zahlen" a variation of the Euclidean theorem on division of integers : "Bezeichnet x eine beliebige Zahl des Körpers K , so lassen sich die ganzen Zahlen $\lambda_1, \lambda_2, \lambda_3, \dots \lambda_m$ desselben Körpers so bestimmen, dass von den Normen der Zahlen

$$x-\lambda_1 , 2x-\lambda_2 , 3x-\lambda_3 , \dots , mx-\lambda_m$$

mindestens eine absolut genommen kleiner als 1 ist. Dabei bedeutet m eine positive ganze Zahl, die ausschliesslich von dem Körper K abhängt".

At the end of his life, he returns to this Hilfssatz ([9]), remarking that one gets an upper bound for m from Minkowski's theorem on linear forms, for instance $m < \sqrt{|d|}$, if K is of degree $n > 1$, where $d = d_K$ is the discriminant of K . The main property of the set of factors for x (i.e. 1, 2, 3, ... , m in this case), used in proving the Hilfssatz, is that, up to the sign, the difference of any two is again in that set. This gives also an easy proof of the fact that the ring $\mathfrak{o}[1/m!]$ of quotients of the ring $\mathfrak{o}$ of integers of K , is Euclidean with respect to its norm (a special case of a theorem of O'Meara, [18]).

Now, H. W. Lenstra substitutes, when possible, the factors for x by numbers $\omega_1, \omega_2, \dots, \omega_m \in \mathfrak{o}$ whose mutual differences $\omega_i - \omega_j$ are units. One then concludes that $\mathfrak{o} = \mathbb{Z}_K$ itself is Euclidean with respect to the usual norm. If I is a nontrivial ideal of $\mathbb{Z}_K$ (with minimal norm $L = L(K)$), then all the ω_i's project on different cosets in $\mathbb{Z}_K/I$. Therefore one has the upper bounds

$$m \leq L \leq 2^n \ .$$

For K , we define the constant of Lenstra $M = M(K)$ to be the maximal length m of sequences $\omega_1, \omega_2, \dots, \omega_m$ in $\mathbb{Z}_K$, for which the mutual differences $\omega_i - \omega_j$ $(i \neq j)$ are units. This constant was introduced in [10] . Using packing arguments, Lenstra actually gives there constants $\alpha_{r,s}$ (where r resp. s is the number of real resp. complex imbeddings of K) with the following property : the inequality

$$M > \alpha_{r,s} \, |d_K|^{\frac{1}{2}}$$

implies that K is Euclidean with respect to the norm. By this method, Lenstra raised the number of known Euclidean fields from 189 to 311. He first gave examples in degree n = 6 , 7 , 8 .

After Lenstra's paper, seven new Euclidean fields were discovered ; the two fields $\mathbb{Q}((-2)^{\frac{1}{4}})$, $\mathbb{Q}((-7)^{\frac{1}{4}})$ by Cioffari ([2]), the field $\mathbb{Q}(\sqrt{-3}, \sqrt{-4}, \sqrt{5})$ by Lenstra himself ([11]), and four fields by Mestre ([15]). Mestre found lower bounds for M(K) using elliptic curves, and he got a first example with signature n = 8 , r = 2 .

In this paper, we prove the existence of 114 new Euclidean fields, including examples of signatures (7,3), (7,5), (9,1), (10,0). All these fields are seen to be Euclidean by explicit construction of sequences $\omega_1, \dots, \omega_m$. They can be found in table 3 at the end of the paper.

In [10], Lenstra asks for a better upper bound of M than 2^n . Fields with unit rank $r+s-1 \leq 1$ are easily dealt with (see [10], 3.9 - 3.11). We give non-trivial upper bounds of M for fields with unit rank 2 ; in particular, for cubic fields one has $M \leq 3$ except for the two fields with discriminant -23 , 49 respectively. Moreover, there are interesting connections for cubic fields between Lenstra's constant and class numbers in the ordinary and in the narrow sense.

Lenstra's constant even is linked with fields of small discriminants : it is an experimental fact that fields K of root discriminant $|d_K|^{1/n}$ close to the lower bound given by Odlyzko under GRH have rather large M . Conversely, a search for fields with long sequences $\omega_1, \omega_2, \dots, \omega_m$ often reveals fields with small discriminants. We give such examples for n = 7 , 8 , 9 , 10 , despite the lower bound for M does not allow the conclusion that all these fields are Euclidean. So, small discriminants show that Lenstra's constant has an interest independently of its application to Euclidean fields.

In section 2, general properties of Lenstra's constant are discussed. Section 3 is devoted to lower bounds of M, whereas sections 4, 5, 6 deal with fields of degree $n \leq 6$. For some fields, we need a particular study of M (section 7). Section 8 concerns the questions of small discriminants, and a ninth section at the end of this paper contains tables. The last one is an update of Lenstra's table 11 of [10] giving the number of known Euclidean fields K according to n and $r+s$.

Some more results can be found in "Séminaire de Théorie des Nombres, Bordeaux, 1981-1982", to appear.

We acknowledge the assistance of H. J. Toussaint at Technical University of Munich in computing discriminants.

Those who know the number fields "individually" will have some pleasure in reading this paper ; they too will find several unsolved problems to deal with.

2. - Exceptional sequences

2.1. - Notation. - Throughout this paper, the fields we consider are number fields, which are subfields of an algebraic closure of $\mathbb{Q}$ chosen once for all. Given a number field K, we denote by n_K, r_K, s_K, d_K, E_K, Cl_K, Cl_K^+ the degree of K, the number of real places of K, the number of complex places of K, its discriminant, its group of units and its class groups in the ordinary and in the narrow sense. As usual, the orders of Cl_K and Cl_K^+ are denoted by h_K, and h_K^+. We write $\mathbb{Z}_K$ for the ring of integers of K. For the notation $L(K)$, G, H, $\tilde{E}_K$, $U(f)$, see below. We shall very often suppress the subscript K when there is no risk of confusion, and write simply M or L instead of $M(K)$ or $L(K)$.

2.2. - Exceptional units. - Let K be a number field and let m be an integer such that there exists a sequence $\omega_1, \omega_2, \ldots, \omega_m$ of elements of K in which all differences $\omega_j - \omega_i$ $(1 \leq i < j \leq m)$ are units. We assume $m \geq 2$; this is possible :

take $\omega_1 = 0$ and $\omega_2 = 1$. Replacing ω_i by $(\omega_i - \omega_o)/(\omega_1 - \omega_o)$, we may assume that one has $\omega_1 = 0$ and $\omega_2 = 1$. The ω_i's are then integers, and have distinct images modulo any non trivial ideal $\mathfrak{a}$ of $\mathbb{Z}_K$. Thus, one has the inequality $m \leq N_{K/\mathbb{Q}}(\mathfrak{a})$ for every ideal of K ; this proves the existence of M(K). Following Lenstra, we define L(K) to be the lower bound of the norms of the ideals of K other than (0) and $\mathbb{Z}_K$. Clearly, L(K) is a prime power, and the following inequalities hold :

$$2 \leq M(K) \leq L(K) \leq 2^n = N_{K/\mathbb{Q}}(2\mathbb{Z}_K) .$$

The inequality $M(K) \geq 3$ is equivalent to the existence of a unit x of K such that 1-x is also a unit. Such units were called exceptional by Nagell ([16]). We call $\tilde{E}_K$ the set of exceptional units of K ; it is a finite set.

Let G be the group of order 6, isomorphic to the symmetric group S_3, generated by the homographic transformations $x \mapsto 1/x$ and $x \mapsto 1-x$. This group acts on $\tilde{E}_K$, and it is easily verified that this action is faithfull, unless there is in K a primitive 6-th root of unity x, which has an orbit under the action of G containing only two elements. We thus have card $E_K \equiv 2$ (resp. 0) mod. 6 if $\sqrt{-3} \in K$ (resp. $\sqrt{-3} \notin K$).

Let x be an exceptional unit of K. Then, $N_{K/\mathbb{Q}}(x)$ and $N_{K/\mathbb{Q}}(1-x)$ take values in $\{-1, +1\}$. Hence, exceptional units in fields of degree n are defined by 4 families of polynomials depending linearly on (n-2) parameters, namely their characteristic polynomials. We denote by P_1 (resp. P_2, P_3, P_4) the polynomials for which the system $(N_{K/\mathbb{Q}}(x), N_{K/\mathbb{Q}}(1-x))$ takes the value $((-1)^n, (-1)^n)$ (resp. $(1,-1)$, $(-1,1)$, $((-1)^{n+1}, (-1)^{n+1})$). We say that x is of the first kind if some element of G x is a root of a polynomial P_1, of the second kind otherwise. If x is of the first kind, then all the units of the orbit Gx are roots of a polynomial P_1. If x is of the second kind, then the elements of Gx are by pairs roots of polynomials P_2, P_3 and P_4.

2.3. - Exceptional sequences

2.3.1. - DEFINITION. - Let K be a number field, and let $\omega_1, \ldots, \omega_m$ $(m \geq 2)$ be a sequence of elements of K. We say that this sequence is an exceptional sequence if $\omega_1 = 0$, $\omega_2 = 1$ and all the differences $\omega_j - \omega_i$ $(1 \leq i < j \leq m)$ are units.

The sequence $0, 1, \omega$ is exceptional if and only if ω is an exceptional unit ; thus, the notion of an exceptional sequence is a generalization of that of an exceptional unit.

Clearly, $0, 1, \omega_3, \dots, \omega_m$ is an exceptional sequence if and only if the following two conditions are fullfilled

(i) For $3 \leq i \leq m$, $\omega_i \in \tilde{E}_K$.

(ii) For $3 \leq i < j \leq m$, $\omega_j/\omega_i \in \tilde{E}_K$.

The group G acts on exceptional sequences : if $0, 1, \omega_3, \dots, \omega_m$ is exceptional, so is $0, 1, s\omega_3, \dots, s\omega_m$ for any $s \in G$.

2.3.2. - DEFINITION. - Let $0, 1, \omega_3, \dots, \omega_m$ and $0, 1, \omega'_3, \dots, \omega'_m$ be two exceptional sequences of a field K with the same length m . We say that they are <u>equivalent</u> if the second one can be obtained from the first one by successive transformations of one of the following forms :

(i) to replace all the ω_i's for $i \geq 3$ by their images under the action of an element $s \in G$;

(ii) to change the order of the ω_i's for $i \geq 3$;

(iii) to replace the sequence $0, 1, \omega_3, \dots, \omega_m$ by the sequence $0, 1, 1/\omega_3, \omega_4/\omega_3, \dots, \omega_m/\omega_3$.

2.4. - Some upper bounds of M . - We give in this subsection some upper bounds of M which are obtained by a study of the unit group E_K modulo its subgroups E_K^2 and $\pm E_K^2$.

2.4.1. - PROPOSITION. - Let K be a field of degree n with r real places and s complex places $(r+2s=n)$, and let $0, 1, \omega_3, \dots, \omega_m$ be an exceptional sequence of length m in K .

(i) If none of the $(m-1)(m-2)/2$ units ω_i $(3 \leq i \leq m)$, ω_j/ω_i $(3 \leq i < j \leq m)$ is a square, then $m \leq 1+2^{r+s}$.

(ii) If none of the units above is a square nor the opposite of a square, and if $\zeta_4 \notin K$, then $m \leq 1+2^{r+s-1}$.

(iii) *If no exceptional unit of* K *is a square, and if* K *has at least one real place, then* $m \leq 1+2^{r+s-1}$.

Proof. - (i) The group E_K/E_K^2 has exactly 2^{r+s} elements. If the length m of the sequence were greater than $1+2^{r+s}$, then 2 units ω_i , ω_j would have the same image in E_K/E_K^2 , and the ratio ω_j/ω_i would then be a square.

(ii) Use the same argument with $E_K/\pm E_K^2$ instead of E_K/E_K^2 .

(iii) Let v be a real place of K . The argument used to prove (i) will actually prove the inequality obtained under condition (ii) if we can show that there exists an exceptional sequence equivalent to the given one in which all the units are positive at v . This is a consequence of the following lemma :

2.4.2. - LEMMA. - *Let* K *be a number field together with a real place* v , *and let* $0 , 1 , \omega_3 , \dots , \omega_m$ *be an exceptional sequence* ; *then, there exists an exceptional sequence* $0 , 1 , \omega'_3 , \dots , \omega'_m$ *equivalent to the given one such that the units* ω'_i $(i \geq 3)$ *satisfy at the place* v *the inequalities* $0<\omega'_i<1$.

Proof. - There is nothing to prove if $m = 2$. Let m be ≥ 3 . Replacing if necessary the given sequence by the equivalent sequence $0 , 1 , 1-\omega_3 , \dots , 1-\omega_m$, we may assume that ω_3 is positive at v . Replacing then if necessary the sequence $0 , 1 , \omega_3 , \dots , \omega_m$ by the sequence $0 , 1 , 1/\omega_3 , \dots , 1/\omega_m$, we obtain the required inequality for ω_3 . Now let m' be the greatest integer for which there exists a sequence $0 , 1 , \omega'_3 , \dots , \omega'_m$ equivalent to the given one such that the units ω'_i for $3 \leq i \leq m'$ satisfy the inequality $0<\omega'_i<1$ at v . By the argument above, one has $m' \geq 3$. We show now that $m' = m$. Otherwise, consider the unit $x = \omega'_{m'+1}$. One has $x>1$ or $x<0$ at v . If x is >1 , then we replace the sequence $0 , 1 , \omega'_3 , \dots , \omega'_m$ by the sequence $0 , 1 , 1/x , \omega_3/x , \dots , \omega'_{m'}/x$, $\omega'_{m'+2}/x , \dots , \omega'_m/x$; if $x<0$, we replace the sequence $0 , 1 , \omega'_3 , \dots , \omega'_m$ by the sequence $0 , 1 , 1-\omega'_3 , \dots , 1-\omega'_m$, and apply once again the argument above.

3. - *Lower bounds for* M

3.0. - The trivial estimate $M \geq 2$ allows to conclude $\mathbb{Z}_K$ to be Euclidean for 9 quadratic fields (d= -11 , -8, -7 , -4 , -3 , 5 , 8 , 12, 13), for 4 cubic fields (d= -23 , -31 , -44 , 49) and for seven quartic fields (d= 117, 125 , 144 , 189, 225, 229, -275). Yet only the last two Euclidean fields were detected by Lenstra's method.

$M(K) = M \geq 3$ is the same as to say that $\mathbb{Z}_K$ contains an exceptional unit. In degree two one has exactly 8 exceptional units, namely $\zeta_6^{\pm 1}$, $\theta^{\pm 2}$, $\pm\theta^{\pm 1}$, the zeros of X^2-X+1, X^2-3X+1, X^2-X-1, X^2+X-1. Therefore $M(\mathbb{Q}(\sqrt{-3})) = 3$, $M(\mathbb{Q}(\sqrt{5})) = 4$ and $M = 2$ for all other quadratic fields. The exceptional sequence $0, 1, \zeta_6$ gives seven further Euclidean fields (four in degree 4 and three in degree 6) whereas $0, 1, \theta, \theta+1$ proves $\mathbb{Z}_K$ Euclidean for seven further quartic fields.

3.1. - The last two exceptional sequences are special cases of a proposition of Lenstra.

3.1.1. - DEFINITION. - Let f be a polynomial with coefficients in $\mathbb{Z}$, and let x be an algebraic number. We say that x is <u>a unit for</u> f if $f(x)$ is a unit in $\mathbb{Q}(x)$. <u>Notation</u> : $x \in U(f)$.

3.1.2. - PROPOSITION (Lenstra [10], prop. 2.4). - <u>Let</u> x <u>be an algebraic integer with minimal polynomial</u> f, <u>and let</u> K <u>be an extension of</u> $\mathbb{Q}(x)$. <u>Then</u> :

I - $M(K) \geq 3$ <u>if</u> $0, 1 \in U(f)$

II - $M(K) \geq 4$ <u>if</u> $0, 1, -1 \in U(f)$

III - $M(K) \geq 5$ <u>if</u> $0, 1, \zeta_6 \in U(f)$

IV - $M(K) \geq 5$ <u>if</u> $0, 1, -1, \theta \in U(f)$

V - $M(K) \geq 6$ <u>if</u> $0, 1, -1, \zeta_4, \zeta_3 \in U(f)$

VI - $M(K) \geq 6$ <u>if</u> $0, 1, -1, \theta, -\theta \in U(f)$ (θ, ζ_4, ζ_3 <u>are defined in table</u> 1 <u>below</u>).

To prove these inequalities, Lenstra uses the following sequences : $0, 1, x$; $0, 1, x, x+1$; $0, 1, x, 1/(1-x), (x-1)/x$; $0, 1, x, x+1, x^2$; $0, 1, x, x^2, x^3, x^4$ and $0, 1, x, x+1, x^2, x^2+x$, together with the following remarkable lemma ([10], lemma 2.5) :

3.1.3. - LEMMA. - <u>Let</u> $f, g \in \mathbb{Z}[X]$ <u>be monic polynomials</u>, <u>irreducible over</u> $\mathbb{Q}$, <u>with respective roots</u> x, y <u>in some extension of</u> $\mathbb{Q}$. <u>Then</u>, $x \in U(g) \Leftrightarrow y \in U(f)$.

3.1.4. - Remark. - The inequality $M \geq 6$ of V can be improved to $M \geq 7$ by using the following sequence :

$$V^* \quad 0\,,\,1\,,\,x\,,\,x+1\,,\,-x^2\,,\,-1/x\,,\,x/(x+1)\,.$$

Table 1

symbol	definining equation	d	L	M	reference
θ	$\theta^2-\theta-1 = 0$	5	4	4	II
α	$\alpha^3-\alpha-1 = 0$	- 23	5	5	IV
γ	$\gamma^3+\gamma-1 = 0$	- 31	3	3	I
$\varkappa$	$\varkappa^3+\varkappa^2-\varkappa+1 = 0$	- 44	2	2	-
η	$\eta^3+\eta^2-2\eta-1 = 0$	49	7	7	A or B , x^2+x
β	$\beta^4-\beta^3-\beta^2+\beta+1 = 0$	117	7	6	B
ν	$\nu^4-\nu+1 = 0$	229	3	3	I
ξ	$\xi^4-2\xi^3+\xi^2+1 = 0$	272	4	3	I
ρ	$\rho^4-2\rho^3+\rho-1 = 0$	- 275	9	9	A_2
δ	$\delta^4-\delta-1 = 0$	- 283	7	7	B_1 or V^*
ε	$\varepsilon^4-2\varepsilon^2+3\varepsilon-1 = 0$	- 331	5	5	III
σ	$\sigma^4+\sigma^3-3\sigma^2-\sigma+1 = 0$	725	11	≥ 10	C, $-1/(x^2-x-1)$

Table 1 gives twelve symbols for certain algebraic integers s . The number d is the discriminant of the ring $\mathbb{Z}[s]$, which, in these cases, is the maximal order $\mathbb{Z}_K$ of the field $K = \mathbb{Q}(s)$; $L = L(K)$ denotes the least non-trivial ideal norm and $M = M(K)$ the Lenstra constant of that field. In line 5, sequence A refers to the minimal polynomial of $-\eta$ instead of η ; the symbol ζ_m denotes a primitive m^th root of unity.

3.2. - New sequences. - Here, x is a zero of a monic irreducible polynomial $f \in \mathbb{Z}[x]$.

A $0, 1, x, x+1, x^2, x/(x-1), 1/(2-x)$ is an exceptional sequence under the conditions $0, \pm 1, 2, \theta \in U(f)$.

Example. - The polynomial $X^7+X^6-6X^5-5X^4+8X^3+5X^2-2X-1$ defines the field with $n = r = 7$ which is known to have the minimum discriminant, namely $20\,134\,393 = 71.283\,583$ ([20]). For this field, $M = L = 7$.

B $0, 1, x, x+1, x^2, (x+1)/x$ is an exceptional under the conditions $0, \pm 1, \theta, \alpha \in U(f)$.

Example.- The polynomial $X^7-X^6-X^5+X^4-X^3-X^2+2X+1$, with $n=7$, $r=1$, $s=3$ and discriminant -71^3 defines a subfield of the Hilbert class field of $\mathbb{Q}(\sqrt{-71})$, and is obtained from Weber's polynomial by the transformation $f(X) \longmapsto -X^7 f(-1/X)$ ([21], p. 723) ; the inequality $M \geq 6$ proves that the field defined by a zero of f is Euclidean.

B_1 $0, 1, x, x+1, x^2, (x+1)/x, -x/(x^2-x-1)$ is exceptional under the conditions of B together with $\eta \in U(f)$.

Example. - The equality $M = L = 7$ for the field $\mathbb{Q}(\delta)$ can be proved by applying B_1 to the polynomial X^4-X-1 (cf. table 1).

Note that B_1 is an enlargement of B ; other possible enlargements are B, x^2+x (resp. B, $x^2/(x^2-1)$ provided one has $-\theta \in U(f)$ (resp. $\sqrt{2} \in U(f)$). One can combine these conditions and obtain the very fruitful sequence :

C $0, 1, x, x+1, x^2, (x+1)/x, -x/(x^2-x-1), x^2/(x^2-1), x^2+x$,

which is exceptional of lengh 9 without any extra condition ; 20 new Euclidean fields were discovered by this sequence or some enlargements by one more term ; for instance, the enlargement by $-1/(x^2-x-1)$ proves the inequality $M \geq 10$ for $\mathbb{Q}(\sigma)$ (cf. table 1 and § 5.3.3). Trying $(x+1)/x$ of sequence B as an enlargement of sequence A gave the sequence $A_1 = A, (x+1)/x$, which is exceptional under the conditions

$$0, \pm 1, \theta, \alpha, 2, \sqrt{2} \in U(f) .$$

3.3. - Some more enlargements of sequences A, B, C

Let $f(X) = X^6-5X^5+7X^4+2X^3-9X^2+2X+1$, the norm from $\mathbb{Q}(\theta)$ to $\mathbb{Q}$ of $f_1(X) = X^3-(\theta+2)X^2+2\theta X+1 \in \mathbb{Z}[\theta, X]$, of discriminant

$-144\ 875 = -5^3.19.61$, which appears in table 3, $n = 6$, $r = 4$, $s = 1$. Sequence A shows the inequality $M \geq 7$, and a search among the exceptional units of $\mathbb{Q}(\theta)$ gave the enlargement of A by θ^2. Expressing θ^2 by a function of x and using the invariance of A under the transformation $x \mapsto 1-x$, one finds the exceptional sequence A, $(x^2-1)/(x^2-x-1)$, under the additional conditions $-\eta, -\eta^{-1}, \delta^{-2} \in U(f)$. Now, let τ be the transformation given by $x \mapsto (1-x)$ followed by $\omega \mapsto x/(1-\omega)$; then $s = \tau \circ \tau : \omega \mapsto x(\omega-1)/(\omega-x)$ is a projective transformation of $\mathbb{Q}(x)$ of order 2. We remark that A together with infinity is the union of 2 orbits under τ. Because $s((x^2-1)/(x^2-x-1)) = -x^2/(x^3-2x^2-x+1)$, we have the new exceptional sequence

$$A_2 = A,\ (x^2-1)/(x^2-x-1),\ -x^2/(x^3-2x^2-x+1)$$

under the conditions $0, \pm 1, \theta, 2, -\eta, -\eta^{-1}, \delta^{-2} \in U(f)$ and "$x^5-x^4-3x^3+2x^2+x-1$ is a unit". Despite its complication, many new euclidean fields were found by making use of A_2.

We now give some other enlargements of sequences A, B and C.

$B_2 : B_1,\ x^2/(x^2-1)$; conditions : $0, \pm 1, \theta, \alpha, \sqrt{2}, \eta \in U(f)$.
(note that B_1 and B_3 invariant under s).

$B'_2 : B,\ x^2/(x^2-1), -1/(x^2-x-1)$; conditions : $0, \pm 1, \theta, \alpha, \sqrt{2}, -1/\delta \in U(f)$.

$B_3 : B_2,\ -1/(x^2-x-1)$; conditions : $0, \pm 1, \theta, \alpha, \sqrt{2}, \eta, -1/\delta \in U(f)$.

$B'_3 : B'_2,\ (x^3-x)/(x^3-x-1)$; conditions : $0, \pm 1, \theta, \alpha, \sqrt{2}, -1/\delta, 1/\gamma, \delta^2 \in U(f)$
and "$x^5-x^4-x^3+x^2-1$ is a unit".

$B_5 : B_3,\ x/(x^2-1), (x^2-x-1)/(x^2-2)$; conditions : those of B_3 plus
"$2x^2-x-2$ and $x^4-2x^3-2x^2+3x+1$ are units".

The next sequence is obtained from C by subtituting for $x^2/(x^2-1)$ an orbit under s :

C^* : $0, 1, x, x+1, x^2, (x+1)/x, -x/(x^2-x-1), (x^3+x^2-x-1)/x,$
$(x^4+x^3-2x^2-x)/(x^3-x-1), x^2+x$; conditions : $0, \pm 1, \pm\theta,$
$\alpha, \sqrt{2}, \eta, (1-\varepsilon)/\varepsilon \in U(f)$ and "x^5-3x^3+2x+1 is a unit".

Remark. - Further enlargements of the sequences above can be found in table 3 ; some of them were found by making use of other homographic transformations, e.g. $\omega \mapsto (x^2+x)/\omega$ or $\omega \mapsto x/(x+1-\omega)$.

3.4. - Complements. - So far, all the sequences we considered made use of the conditions $0, \pm 1, \theta \in U(f)$; looking for sequences which avoid the conditions $-1 \in U(f)$ gives the following sequence

D $0, 1, x, 1/(1-x), (x-1)/x, x-x^2$, which is exceptional under the conditions $0, 1, \zeta_4, \zeta_6, \alpha^2 \in U(f)$; note that it is an enlargement of Lenstra's sequence III (cf. prop. 3.1.2.) .

3.4.1. - Remark. - All the sequences described above make use of one of the conditions $0, 1, -1 \in U(f)$ or $0, 1, \zeta_6 \in U(f)$. Proposition 3.4.2. below gives a reason for this. Recall that a sequence $0, 1, x, y$ is exceptional if and only if x, y and y/x are exceptional units. But, under these conditions, $(1-y)/(1-x)$ and $(1-1/y)/(1-1/x)$ are also exceptional units, so that we may expect to find 5 orbits under the action of G (cf. § 2.2).

3.4.2. - PROPOSITION. - If the five orbits of $x, y, y/x, (1-y)/(1-x)$ and $(1-1/y)/(1-1/x)$ are not distinct for an exceptional sequence $0, 1, x, y$, then the sequence is equivalent to a sequence $0, 1, z, t$ with $t = z+1$, z^2 or $1/(1-z)$. (There are at most 3 orbits if $t = z+1$ or $t = z^2$, those of $z, -z, z^2$ and at most 4 orbits if $t = 1/(1-z)$, those of $z, z-z^2, -(1-z)^2/z, (z-1)/z^2$.)

Since we do not use anywhere this proposition, we leave its proof to the reader. Note that there exist fields with $M \geq 4$ without any exceptional sequence involving the conditions $0, 1, -1 \in U(f)$ or $0, 1, \zeta_6 \in U(f)$

Example (see theorem 6.1.1. below). - The two polynomials (see [10], table 6) $X^6 - X^5 + 4X^4 - 5X^3 + 4X^2 - 3X + 1 = N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(X^3 + \zeta_3 X^2 + (1-\zeta_3) X - 1)$ and $X^6 - X^5 + 2X^4 - 3X^3 + 2X^2 - X + 1 = N_{\mathbb{Q}(K)/\mathbb{Q}}(X^2 + \varkappa X + 1)$, $\varkappa^3 + \varkappa^2 - \varkappa + 1 = 0$, of discriminants $-21\,168$ and $-21\,296$ respectively both have $0, 1, i, \gamma \in U(f)$. Therefore, $0, 1, x, 1/(x^2+1)$ is an exceptional sequence, and $M = L = 4$.

We now give some of the constants $\alpha_{r,s}$ refered to in the introduction (a field K is Euclidean provided one has $M(K) > \alpha_{r,s} \sqrt{|d_K|}$).

n = 6	$r=2$, $s=2$: 2.404 10^{-2} ; $r=4$, $s=1$: 1.965 10^{-2} ; $r=6$, $s=0$: 1.544 10^{-2}
n = 7	$r=1$, $s=3$ and $r=3$, $s=2$: 9.848 10^{-3} ; $r=5$, $s=1$: 7.793 10^{-3}
n = 8	$r=0$, $s=4$ and $r=2$, $s=3$: 3.955 10^{-3} ; $r=4$, $s=2$: 3.897 10^{-3}
n = 9	$r=1$, $s=4$ and $r=3$, $s=3$: 1.563 10^{-3}
n = 10	$r=0$, $s=5$ and $r=2$, $s=4$: 6.097 10^{-4} .

4. - *Cubic fields*

We discuss in this section the properties of cubic fields which are related to Lenstra's constant.

4.1. - *An upper bound for* M . - Proposition 2.4.1, (iii), gives a quick proof of the inequality $M \leq 5$ for $K \not\simeq \mathbb{Q}(\eta)$. But we can prove a sharper result, namely :

4.1.1. - THEOREM. - *Let* K *be a cubic field. Then,* $M(K) = 7$ *if* $d_K = +49$, $M(K) = 5$ *if* $d_K = -23$, *and* $M(K) = 2$ *or* 3 *otherwise.*

Proof. - There exist exactly 8 monic polynomials $f \in \mathbb{Z}[X]$ of degree 3 with $0, \pm 1 \in U(f)$; they are the minimal polynomials of $\pm \alpha^{\pm 1}$ and $\pm \eta^{\pm 1}$. Thus, if some exceptional unit is a square, $d_K = +49$ or -23, and then $M(K)$ can be found in § 3, table 1. Similarily, if $-x^2$ is exceptional for some $x \in K$, then $d_K = -23$ or -31, and one has $M = L = 3$ if $d_K = -31$. We may now assume that K does not possess any exceptional unit belonging to $\pm E_K^2$. Theorem 4.1.1. is then a consequence of the following proposition (the group G is defined in 2.2 ; the orbit under G of an exceptional unit x is the set

$$\{x, 1-x, 1/x, 1/(1-x), (x-1)/x, x/(x-1)\}) :$$

4.1.2. - PROPOSITION. - *Let* K *be a number field of unit rank at most* 2 , *which contains an exceptional sequence* $0, 1, u, v$ *of length* 4 . *Then, some unit belonging to the orbit (under the action of* G *) of one of the exceptional units* u, v, v/u, $(1-v)/(1-u)$ *or* $(1-1/v)/(1-1/u)$ *is the square or the opposite of a square, except possibly if* $[K:\mathbb{Q}] = 6$ *and* $\zeta_4 \in K$.

Proof of 4.1.2. - Fields of degree ≤ 4 containing ζ_4 are easily dealt with ([10], § 3). Assume that $\zeta_4 \notin K$, and let $E = E_K / \pm E_K^2$. As a vector space over $\mathbb{F}_2$, it has dimension ≤ 2, and this dimension is indeed 2 unless some exceptional unit of K belongs to $\pm E_K^2$, for the images of u, 1-u, (u-1)/u are not distinct if $\dim E \leq 1$. If none of the units u, v, v/u belongs to $\pm E_K^2$, then the images of u, v are a basis of E; if 1-u and $\frac{u-1}{u} \notin \pm E_K^2$, one has $v = \pm\lambda^2(1-u)$ or $v = \pm\lambda^2(u-1)/u$ for some $\lambda \in E_K$. Replacing if necessary 0, 1, u, v by 0, 1, u, u/v, we may assume that the equality $v = \pm\lambda^2(1-u)$ holds. Now, if none of the exceptional units 1-v and (1-v)/(1-u) is in $\pm E_K^2$, one has $1-v = \pm\mu^2 u$ or $1-v = \pm\mu^2(u-1)/u$ for some $\mu \in E_K$. If $(1-v)/u = \pm\mu^2$, then $(1-1/v)/(1-1/u) \in \pm E_K^2$. Thus, we may assume that the equality $1-v = \pm\mu^2(u-1)/u$ holds. Consider now the unit 1-u/v; if it does not belong to $\pm E_K^2$, it satisfies one of the equalities $1-u/v = \pm\nu^2 u$, $1-u/v = \pm\nu^2(1-u)$, $1-u/v = \pm\nu^2(u-1)/u$ for some $\nu \in E_K$. If $1-u/v = \pm\nu^2 u$, then $(1-u/v)/(1-1/v) = 1-(1-u)/(1-v) \in \pm E_K^2$; if $1-u/v = \pm\nu^2(1-u)$, then $(1-u/v)/(1-u) = 1-(1-1/v)/(1-1/u) \in \pm E_K^2$; if $1-u/v = \pm\nu^2(u-1)/u$, then $(u/v-1)/(u/v) \in \pm E_K^2$, q.e.d.

4.2. - Cubic polynomials and exceptional units. - Let K be a cubic field which possesses an exceptional unit x, with trace a. With the notation of 2.2, x is a root of one of the following four polynomials :

$$\begin{aligned} P_1(X) &= X^3 - aX^2 + (a-3)X + 1 \\ P_2(X) &= X^3 - aX^2 + (a+1)X - 1 \\ P_3(X) &= X^3 - aX^2 + (a-1)X - 1 \\ P_4(X) &= X^3 - aX^2 + (a-1)X + 1 . \end{aligned}$$

The discriminants of these polynomials are ([16])

$$d_{P_1}(a) = (a^2-3a+9)^2 , \quad d_{P_2}(a) = (a^2-3a-1)^2 - 32 , \quad d_{P_3}(a) = d_{P_2}(a-1)$$

and $\quad d_{P_4}(a) = d_{P_2}(2-a)$.

These polynomials were used by Nagell ([16]) to show that infinitely many abelian and non abelian cubic fields contain exceptional units, so that Theorem 4.1.1. is the best possible. The discriminant of P_2 is negative for $-1 \leq a \leq 4$, and then $d_K = -23$ or -31, and positive otherwise ; moreover, one easily sees that d_{P_2} is a square if and only if $a = -2$ or $+5$, and then $d_K = +49$ (i.e. $K = \mathbb{Q}(\eta)$).

If $P_1(x) = 0$, then $K = \mathbb{Q}(x)$ is an abelian cubic field, and conversely, all exceptional units of abelian cubic fields are zeros of some polynomial P_1 except for 18 units of $\mathbb{Q}(\eta)$. Polynomials P_1 were considered by M.-N. Gras ([7]) in connection with integral power bases in abelian cubic fields. She proved the inequality $M(K) \leq 3$ for K abelian other than $\mathbb{Q}(\eta)$ by the following argument : if $0, 1, u, v$ is an exceptional sequence in K, then at least one of the units $u, v, u/v$ has norm $+1$; thus, K contains a unit of the second kind, and hence $K = \mathbb{Q}(\eta)$. Note that all abelian cubic fields with $M \geq 3$ do have units of the first kind ; hence, for such a field, the ratio h_K^+/h_K is odd.

4.3. - *Totally real non abelian cubic fields*. - Let K be a cubic field, and let x be an exceptional unit of K. We suppose that K is not abelian. Hence (see 2.2) exactly 2 units of the orbit of x are defined by a polynomial P_2. If u is one of them, the other is $1-u$; so exactly one unit of the orbit of x is a zero of a polynomial P_2 and is of positive trace. We denote by T this trace ; it is an invariant of the orbit of x, and we shall assume now that x is precisely this unit ; one has $T \geq 6$ by 4.2.

4.3.1. - THEOREM.- *Let* K *be a totally real non abelian cubic field* ; *let* x *be an exceptional unit of* K, *with trace* $T \geq 6$ *and which is a zero of a polynomial* $P_2 : x^3 - Tx^2 + (T+1)x - 1 = 0$. *Then, the following properties hold for* K *and* T :

(i) *The discriminant* d_K *of* K *is congruent to* 1 *modulo* 8.

(ii) *Every prime divisor* p *of* d_K *has a prime factor of degree* 1 *in the quartic field of discriminant* -448 ; *in particular, such a* p *is congruent to* $+1$ *or* -1 *modulo* 8.

(iii) $h_K^+/h_K = 2$.

(iv) *If* $T \not\equiv 1$ *modulo* 4, *then the exact sequence*

$$0 \longrightarrow (\pm 1) \longrightarrow Cl_K^+ \longrightarrow Cl_K \longrightarrow 1$$

splits ; *if* $T \equiv 1$ *modulo* 4, *then* h_K *is even*.

(v) *Let* k *be the quadratic field contained in the Galois closure* N *of* $K/\mathbb{Q}$. *Then, either* $d_K = d_k$, *or* $d_K = 7^2 d_k$ *and* $T \equiv -2$ *modulo* 7.

Proof. - (i) One has $d_{P_2} = (T^2 - 3T - 1)^2 - 32 = d_K m^2$ for some $m \in \mathbb{Z}$. Since d_{P_2} takes only values $\equiv 1$ mod. 8, so does d_K. The root of the equations

$d_{P_2}(a) = 0$ are $\frac{3 \pm (3+\varepsilon\sqrt{2})\sqrt{-1+2\varepsilon\sqrt{2}}}{2}$ ($\varepsilon = -1$ or $+1$). This shows that the field with minimal polynomial d_{P_2} is the quartic field of discriminant $-448 = -2^6 . 7$, which prooves (ii).

(iii) The polynomial P_2 takes for $X = 0, 1, 2$ the values $-1, +1, 9-2T<0$; thus, x is totally positive ; since it is not a square (§ 4.1), h_K^+/h_K is even. Since $\pm(1-x)$ are not totally positive, $h_K^+/h_K = 2$.

(iv) To prove (iv), we construct extensions which are unramified at finite places. Let y be a zero of the polynomial $X^3 - aX^2 + (a+1)X - 1$; then, $z = 1/y$ is a zero of $X^3 - (a+1)X^2 + aX - 1 = X(X-1)(X-a) - 1$. Now, for $a \equiv 1 \bmod 4$, the polynomial $Z^2 - (z-(a+1)/2)Z + [(a-1)/4]^2$ has coefficients in $\mathbb{Z}_K$ and discriminant $(z-a)(z-1) = 1/z = y$, a unit. Taking $y = x$ if $T \equiv 1 \bmod 4$ (resp. $y = 1-x$ if $T \equiv 2 \bmod 4$), we see that the extension $K(\sqrt{x})/K$ (resp. $K(\sqrt{(1-x)}/K)$ is unramified (resp. ramifies exactly at two infinite places). This proves (iv) if $T \equiv 1$ or $T \equiv 2 \bmod 4$. Similarily, for $a \equiv 0 \bmod 4$, we consider the polynomial $Z^2 - (z-a/2)Z + (a/4)^2$; its discriminant is $z(z-a) = 1/(z-1) = y/(1-y)$. We now take $y = x$ if $T \equiv 0 \bmod 4$ and $y = 1-x$ if $T \equiv -1 \bmod 4$; the extension $K(\sqrt{x(1-x)})/K$ ramifies exactly at two infinite places, q. e. d.

(v) Write $d_K = d_k f^2$, so that f is the relative discriminant of N/k. Then, f divides the discriminant Δ of $x, \sigma x, \sigma^2 x$, where σ generates $\mathrm{Gal}(N/k)$; an easy calculation shows that $\Delta = T^2(T^2 - 3T - 3)^2$. Let p be a prime divisor of f. Then p is totally ramified in $K/\mathbb{Q}$, and p divides T or $T^2 - 3T - 3$. If p divides T, then p divides $(T^2 - 3T - 1)^2 - 32 \equiv -31 \bmod p$; hence, $p = 31$; but one has $P_2(X) \equiv X^3 + X - 1 \bmod p$; since $X^3 + X - 1$ has 2 distinct roots mod 31, p cannot be totally ramified in $K/\mathbb{Q}$. Hence, p divides $T^2 - 3T - 3$; then, $(T^2 - 3T - 1)^2 - 32 \equiv -28 \bmod p$, thus p divides 28, and $p = 7$ since d_K is odd by (i) ; the congruence $T \equiv -2 \bmod 7$ is then obvious, and theorem 4. 3. 1 is now completely proved.

4. 3. 2. - Remark. - To non abelian cubic fields with h_K even (resp. with h_K odd and h_K^+/h_K even), there correspond by class field theory quartic fields of type S_4 with the same discriminant which are totally real (resp. totally complex). By [4], the first 2 discriminants of totally real S_4 fields are $1957 \equiv -3 \bmod 8$ and 2 777, which corresponds to $T = 9$. Hence, the smallest

discriminant of a totally real non abelian cubic field with even class number and $M = 3$ is 2 777. By [5], there are only 2 discriminants of totally complex quartic fields which are less than 761 and congruent to ± 1 mod 8, namely 257 and $697 = 17.41$; they correspond to $T = 6$ and $T = 7$ respectively ; hence, the smallest two discriminants of non abelian cubic fields, totally real, with $M = 3$, are 257 and 697.

4.3.3. - Remark. - For $T = 9$, 13 and 17, we have verified that the sequence

$$0 \longrightarrow (\pm 1) \longrightarrow Cl_K^+ \longrightarrow Cl_K \longrightarrow 0$$

does not split.

4.4. - The field with discriminant $d = 257$. - As we saw in the proof of theorem 4.3.1, the unramified extension K' of the cubic field K with discriminant $d_K = 257$ is generated over K by a root x of the polynomial $f(T) = T^2 - \gamma_1 T + 1$ where γ_1 is a zero of the polynomial $X^3 + X^2 - 4X - 3$; the norm of $f(T)$ is the reciprocal polynomial $g(T) = T^6 + T^5 - T^4 - T^3 - T^2 + T + 1$, with discriminant $+257^2$. One has $M(K') \geq 7$ by the sequence $0, 1, x, x+1, x^2, 1/x, x/(x+1)$ which is exceptional under the conditions $0, \pm 1, \pm\theta, \zeta_3 \in U(g)$; this proves that K' is Euclidean ; it has $L = 8$; the exact value of M (7 or 8) is not known.

5. - Quartic and quintic fields

We prove in this section upper bounds of M for fields with $n = 4$, $r \leq 2$ and $n = 5$, $r = 1$, using proposition 2.4.1, (iii). We also discuss the value of M for the other fields with $n = 4$ or 5.

5.1. - Non totally real quartic fields

5.1.1. - THEOREM. - Let K be a non totally real quartic field. Then, $M(K) \leq 5$ except if K is one of the fields $\mathbb{Q}(\beta)$, $\mathbb{Q}(\rho)$ or $\mathbb{Q}(\delta)$ of table 1, § 3, with respective discriminants +117, -275 and -283.

Proof. - The result for totally complex fields is stated in [10] (§ 3.11), and can be proved directly by making use of remark 5.1.2. below together with proposition 4.1.2. For fields with $r = 2$, we apply proposition 2.4.1 (iii), and determine all the exceptional sequences $0, 1, u, v$ for which u is a square, say $u = x^2$.

Suppose first that $K = \mathbb{Q}(x)$. Then x is a zero of a polynomial f with $0, \pm 1 \in U(f)$. Taking into account the action of the group

$$H = \{x \mapsto x ,\ x \longmapsto 1/x ,\ x \longmapsto -x ,\ x \longmapsto -1/x\} ,$$

we are reduced to study five families of polynomials depending linearly on an integral parameter $a \geq 0$. We give the polynomials and their discriminants :

$$\begin{aligned}
P_a(X) &= X^4 - aX^3 - X^2 + aX + 1 & d_{P_a} &= (a^2-4)^2 (4a^2+9)\\
Q_a(X) &= X^4 - aX^3 - 2X^2 + (a-1)X + 1 & d_{Q_a} &= 4(a^2-a)^3 + 16(a^2-a)^2 - 72(a^2-a) - 283\\
R_a(X) &= X^4 - aX^3 - 3X^2 + aX + 1 & d_{R_a} &= (a^2+4)^2 (4a^2+25)\\
S_a(X) &= X^4 - aX^3 + X^2 + aX - 1 & d_{S_a} &= 4a^6 - 47a^4 + 112a^2 - 400\\
T_a(X) &= X^4 - aX^3 + (a+1)X - 1 & d_{T_a} &= 4(a^2+a)^3 - 48(a^2+a)^2 + 84(a^2+a) - 283 .
\end{aligned}$$

These discriminants are non zero, except d_{P_a} for $a = 2$ or -2. An easy verification shows that these five polynomials have 4 reals roots to within the following 12 exceptions : P_o ($d_K = +144$), P_1 ($d_K = +117$), Q_o, Q_1 ($d_K = -283$), Q_2 ($d_K = -331$), S_o ($d_K = -400$), S_1 ($d_K = -331$), S_2 ($d_K = -448$), S_3 ($d_K = 283$), T_o ($d_K = -283$), T_1 ($d_K = -275$) and T_2 ($d_K = -643$).

Suppose now that $[\mathbb{Q}(x) : \mathbb{Q}] < 4$. Then, $x \in \mathbb{Q}(\theta)$ ($\theta^2 - \theta - 1 = 0$) ; replacing the sequence $0, 1, u, v$ by an equivalent one, we see that there is in K an exceptional sequence $0, 1, \theta, v$. If $M(K) \geq 5$, there exists such a sequence with $v \notin \mathbb{Q}(\theta)$, for $\mathbb{Q}(\theta)$ has $M = 4$. Let $g(X) = X^2 + aX + b$ be the minimal polynomial of v over $\mathbb{Q}(\theta)$; then, $g(0)$, $g(1)$, $g(\theta)$ are units of $\mathbb{Q}(\theta)$. We are thus lead to the following diophantine system, in which $p', q', r' \in \mathbb{Z}$ and $k, \ell, m \in \{-1, +1\}$:

$$\text{(i)}\quad b = k\,\theta^{p'} \ ; \qquad \text{(ii)}\quad 1 + a + b = \ell\,\theta^{q'} \ ; \qquad \text{(iii)}\quad \theta^2 + a\theta + b = m\,\theta^{r'} .$$

By making use of the linear combination θ^{-1}(i) $- \theta$ (ii) $+$ (iii), we obtain an equation which takes one of the following forms :

(a) $\theta^p + \theta^q + \theta^r = 1$;

(b) $\theta^p + \theta^q = \theta^r + 1$, with $p, q, r \in \mathbb{Z}$

It is easy to prove that the solutions of equation (a) are, up to a permutation of (p, q, r), the triplets $(-2, -2, -3)$ and $(-1, -3, -4)$; equation (b) has infinitly many solutions (put $p=0$, $q=r$ or $p=r$, $q=0$), and, besides these solutions, only the solutions $(2, 2, 3)$, $(1, -2, 0)$, $(-2, 1, 0)$ and $(-1, -1, -3)$; one verifies that the two infinite families of solutions of equation (b) yield only finitely many fields which are not totally real. The proof, though somewhat tedious, is not difficult, and we leave it to the reader. The result is that an exceptional sequence $0, 1, \theta, v$, $v \notin \mathbb{Q}(\theta)$, occurs if and only if v belongs to one of the four fields whose discriminants are $+125$, -275, -400 and -475 .

Using now proposition 2.4.1 for $r=2$ and proposition 4.4.2 (or [10]) for $r=0$, one obtains immediately the inequality $M(K) \leq 5$ except possibly when d_K belongs to the following list : $+117$, $+125$, $+144$, -275, -283, -331, -400, -448, -475, -643. Tables of [6] show that to each of the 10 discriminants above, there corresponds, up to isomorphism, only one field, and that, moreover, the L constants of these fields are ≤ 5 except if $d_K = +117$, -275 or -283, q.e.d.

5.1.2. - Remark. - The field with discriminant -643 has $L = 5$, and the exact value of M (4 or 5) is not known. The other 14 fields K with $n = 4$, $r = 2$ and $|d_K| \leq 900$ are easily seen to have $M = L \in \{2, 3, 4, 5, 7, 9\}$. Proposition 4.1.2 can be used to prove that a field K with $n=4$, $r = 2$ and $|d_K| > 643$ cannot have an exceptional sequence $0, 1, u, v$ with $\mathbb{Q}(u, v) = K$ unless it satisfies the condition $h_K^+/h_K = 2$. This proves the inequality $M \leq 3$ for a lot of fields. For instance, there is one such field with $900 < |d_K| < 1\,000$; it is generated by a root of the polynomial $f(X) = X^4 - 2X^3 + 3X^2 - 1$, and has discriminant $d_K = -976 = -2^4 . 61$. Since $f(0) = -1$, $h_K^+ = h_K$, hence $M(K) \leq 3$, and thus $M(K) = 3$ since $f(1) = 1$, whereas $L(K) = 4$.

5.2. - Quintic fields with one real place

5.2.1. - THEOREM. - Let K be a field of degree five with one real place. Then $M(K) \leq 5$ except if K is one of the fields with discriminant 1 609, 1 649 or 1 777 and possibly the field with discriminant 9137 (see below for a definition of these fields).

Proof. - We apply proposition 2.4.1, (iii). Thus we have to list the fields which possess a unit x such that x, $x-1$, $x+1$ are units (i.e. x^2 is an exceptional unit). Let f be the minimal polynomial of x. Then, f is a monic polynomial of degree five such that $f(0)$, $f(-1)$, $f(+1) \in \{-1, +1\}$. Moreover, since f has only one real zero, one has $f(-1) \leq f(0) \leq f(+1)$. Among the units x, $-x$, $1/x$, $-1/x$, exactly one satisfies the conditions $f(-1) = f(0) = f(1) = -1$. Finally, exactly 23 polynomials arise (one finds a short list of polynomials by using the conditions $f(y) < 0$ for $y = \pm 1/2$ or -2). We give now the list of the fields we found, their discriminant, the number of polynomials f with $f(-1) = f(0) = f(1) = -1$ defining them and one of these polynomials for each field (let f_i be the polynomial corresponding to K_i).

K_1	1 609, prime	3	$X^5 - 3X^3 + 2X - 1$
K_2	1 649 = 17.97	3	$X^5 - X^4 + X^2 - X - 1$
K_3	1 777, prime	3	$X^5 + X^4 - 2X^3 - X^2 + X - 1$
K_4	2 209 = 47^2	2	$X^5 + X^4 + X^3 - X^2 - 2X - 1$
K_5	2 297, prime	2	$X^5 - X^4 - 3X^3 + X^2 + 2X - 1$
K_6	2 617, prime	1	$X^5 - X^4 - 2X^3 + X^2 + X - 1$
K_7	2 665 = 5.13.41	1	$X^5 + X^3 - 2X - 1$
K_8	2 869 = 19.151	2	$X^5 - X - 1$
K_9	3 017 = 7.431	1	$X^5 - X^3 - 1$
K_{10}	4 549, prime	1	$X^5 - 2X^4 - 2X^3 + 2X^2 + X - 1$
K_{11}	4 897 = 59.83	1	$X^5 + X^4 - X^3 - X^2 - 1$
K_{12}	5 501, prime	1	$X^5 + 2X^4 - 2X^2 - X - 1$
K_{13}	5 653, prime	1	$X^5 + 2X^4 + 2X^3 - 2X^2 - 3X - 1$
K_{14}	9 137, prime	1	$X^5 + 3X^4 + 2X^3 - 3X^2 - 3X - 1$.

One verifies easily that these fields have $L \leq 5$ except the fields K_1, K_2, K_3, K_{14}. For K_{14}, $L = 7$; the exact value of $M(4, 5, 6$ or $7)$ is not known ;

probably, $M = 4$. For the fields K_1, K_2, K_3, one has $M > 5$: the field K_1 has $L = 11$, and sequence **C** applied to the polynomial $-f_1(-X)$ shows the inequality $M \geq 9$; the field K_2 has $L = 9$, and sequence B_2 applied to the polynomial $X^5 - 3X^3 - X^2 + 3X + 1$ shows the inequality $M \geq 8$; finally, the field K_3 has $M = L = 7$ (apply B, $x^2/(x^2-1)$ to the polynomial $-f_3(-X)$; conditions are $0, \pm 1, \theta, \alpha, \sqrt{2} \in U(f)$).

5.2.2. - Remark. - Exactly 2 fields with $n = 5$ and $r = 1$ which do not belong to the list above can be defined by a polynomial f with $0, 1, \zeta_6 \in U(f)$; they are the fields K_{15} and K_{16} with respective discrimiants 3 889 and 4 417 of [10], table 3. For both of them, $M = 5$. This shows that the inequality $M \leq 1+2^{r+s-1}$ of proposition 2.4.1, (iii) cannot be improved for $(r, s) = (1, 2)$.

5.3. - Quintic fields with $r \geq 3$. - Whereas only finitely many fields with $n = 5$, $r = 1$ are known to have $M > 3$, it is easy to construct infinitely many fields with $n = 5$ and $r = 3$ (resp. $r = 5$) and $M \geq 5$ by using polynomials f (resp. g) with $0, 1, \zeta_6 \in U(f)$ (resp. $0, \pm 1, \theta \in U(g)$). Only finitely many quintic fields are known to have $M \geq 6$. Here as some examples :

- The field with discriminant - 4 511 generated by a zero x of the polynomial $f(X) = X^5 + X^4 - 3X^3 - 2X^2 + X + 1$ has $L = 13$; the sequence C, $(x^3 - x)/(x^3 - x - 1)$, $-1/(x^3 - x^2 - x)$ shows the inequality $M \geq 11$.

- The field with discriminant -4 903 generated by a zero x of the polynomial $f(X) = X^5 - X^4 - 3X^3 + X^2 + 2X + 1$ has $M = L = 9$ (use the sequence A_1, $-x/(x^2 - x - 1)$).

- The field with discriminant -5 519 generated by a zero x of the polynomial $f(X) = X^5 - 2X^4 - X^3 + X^2 + X + 1$ has $M = L = 7$ (apply the sequence A).

- Finally, the field $\mathbb{Q}(2 \cos 2\pi/11)$ has $M = L = 11$; this is proved by applying the sequence A_2, $(x+1)/x$, $-x/(x^2-x-1)$ to the polynomial $X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1$; conditions are $0, \pm 1, \pm\theta, 2, \pm\eta\ -\eta^{-1}, \alpha, \sqrt{2}, \delta^{-2} \in U(f)$ and moreover "$x^5 - x^4 - 3x^3 + 2x^2 + x - 1$ is a unit". The polynomial above has the zero $-(\zeta_{11} + \zeta_{11}^{-1})$.

5.4. - Euclidean quadratic extensions. - Let K_o be a number field. The abelian extensions of K_o which can be proved to be Euclidean by the inequality $M(K) \geq M(K_o)$ are easily described by class field theory. All the fields which can be dealt with by this method for $[K_o : \mathbb{Q}] \leq 4$ can be found in [10] except 4 of them (for K_o, see table 1, § 3).

5.4.1. - The field K_o with $n = 4$, $r = 2$ and $d_{K_o} = -275$ has $M = 9$; 3 quadratic extensions can be handled, whose relative discriminants have respective norms 25, 29 and 59. The first one appears in [10], table 9 ; the other two fields whose respective discriminants are $5^4.11^2.29 = 2\ 193\ 125$ and $-5^4.11^2.59 =$ $= -4\ 461\ 875$ are new Euclidean fields.

5.4.2. - The field K_o with $n = 4$, $r = 2$ and $d_{K_o} = -283$ has $M = 7$; 2 quadratic extensions can be handled, whose relative discriminants have respective norms 17 and 37 ; the first one appears in [10], table 9 ; the second one, with discriminant $37.283^2 = 2\ 963\ 293$ is a new Euclidean field.

5.4.3. - The field K_o with $n = r = 4$ and $d_{K_o} = 725$ has $M = 10$ or 11 ; the inequality $M \geq 10$ is enough to handle the quadratic extension of K_o whose relative discriminant has norm 11 ; we find a new Euclidean field, with discriminant $-5^4.11.29^2 = -5\ 781\ 875$; no new Euclidean field would be found by the inequality $M(K_o) \geq 11$.

5.4.4. - The known lower bounds of $M(K_o)$ for fields K_o of degree 5 are not sharp enough to handle extensions of K_o by the inequality $M(K) \geq M(K_o)$. However, two fields could eventually be dealt with by an improvement of the previous results. For the first one, we take as field K_o the field K_1 considered in § 5.2 whose discriminant is 1 609 ; it has $L = 11$, and is defined by the polynomial $f(X) = X^5 - 3X^3 + 2X - 1$; let x be a root of f ; then, by class field theory, K_o possesses a quadratic extension K with relative discriminant $(107, x-36)$; the field K has discriminant $d_K = -277\ 010\ 267$, and could be proved Euclidean via the inequality $M(K_o) \geq 11$; it can be defined by the polynomial $Y^2 + (1/x-1)Y+1$. For the second one, let K_o be the field with discriminant $-4\ 511$ of § 5.3, defined by a zero x of the polynomial $f(X) = X^5 + X^4 - 3X^3 - 2X^2 + X + 1$; the quadratic extension K of K_o defined by the polynomial $Y^2 - xY + 1$ has discriminant $-13^2.19.347^2 = -386\ 633\ 299$; it could be proved Euclidean via the inequality $M(K_o) \geq 12$, but we only know the inequality $M \geq 11$ (see § 5.3).

6. - Sextic fields

6.1. - Fields with unit rank 2 . - We obtain upper bounds of M for fields with $n = 6$, $r = 0$ by making use of proposition 2.4.1 (i).

6.1.1. - THEOREM. - Let K be a totally complex sextic field of degree 6 . Then $M(K) \leq 9$ with at most two exceptions : the field K_1 , which is the ray class field over $\mathbb{Q}(\zeta_3)$ with conductor a prime lying above 19 , and the field K_2, which is the ray class field over $\mathbb{Q}(\alpha)$ with conductor a prime above 19 .

Proof. - We first study the existence of exceptional sequences $0, 1, x^2, u$ with x primitive in K . Then, x is a root of a polynomial
$f(X) = X^6 - aX^5 + bX^4 - cX^3 - (b+1)X^2 + (a+c)X + 1 \in \mathbb{Z}[X]$, since $0, \pm 1 \in U(f)$. Replacing if necessary x by $-x$, $1/x$ or $-1/x$, we may assume that a and b are ≥ 0 , and also that c is ≥ 0 if $a = 0$. Bounds for a, b, c are obtained from the inequalities $f(t) > 0$ for $t = \pm 1/2$ and $t = \pm 2$. An explicit computation shows that exactly 19 polynomials occur, which define (up to isomorphism) 17 fields ; 12 of them can be found in [10], table 5 : they are the fields with discriminants -9 747 , -10 051 , -10 571, -10 816 , -11 691 , -14 731, -16 551 , -23 031 , -24 003 , -27 971 and -33 856 (the two fields $\mathbb{Q}(\sqrt{-\alpha})$ and $\mathbb{Q}(\zeta_4, \alpha)$). The remaining 5 fields are the field $\mathbb{Q}(\zeta_4, \gamma)$, and the following 4 fields defined by one of the polynomials

$$X^6 - X^3 - X^2 + X + 1 \qquad (d = -32\ 911),$$

$$X^6 - 3X^5 + X^4 + 5X^3 - 2X^2 - 2X + 1 \quad (d = -41\ 823),$$

$$X^6 - X^5 + X^4 + 2X^3 - 2X^2 - X + 1 \qquad (d = -54\ 691)$$

and $$X^6 - 2X^5 + 4X^3 - X^2 - 2X + 1 \qquad (d = -60\ 992) .$$

The inequality $L < 9$ holds for all these fields except for the first two which are K_1 and K_2 .

We must now look at the sequences $0, 1, x^2, u$ with $[\mathbb{Q}(x):\mathbb{Q}] < 6$; then $\mathbb{Q}(x) = \mathbb{Q}(\eta)$ or $\mathbb{Q}(\alpha)$ by theorem 4.1.1. The case when K contains $k = \mathbb{Q}(\eta)$ is easily dealt with : K is a C. M. field, and, since $h_k^+ = 1$, the "Hasse index" $[E_K : \mu_K E_k]$ is equal to 1 ; we leave to the reader the proof of the equality $M(K) = M(k) (= 7)$. If $K = \mathbb{Q}(\alpha, w)$ is totally imaginary of degree 2 over $\mathbb{Q}(\alpha)$ and if $0, 1, \alpha^2, w$ is exceptional, then w is a zero of

$$f(X) = X^2 - (u+1-v)\, X + u$$

where $u, v, f(\alpha^2) \in \alpha^{\mathbb{Z}}$. Now, the Diophantine equation in non negative integers p, q, r

$$\alpha^p + 1 = \alpha^q + \alpha^r$$

has the solutions $p = q$ arbitrary, $r = 0$ and (provided $q \geq r$) only four extra solutions :

$$(p\ q\ r) = (4\ 3\ 2),\ (6\ 5\ 3),\ (7\ 5\ 5),\ (9\ 8\ 5).$$

Together with the inequality $(u+1-v)^2 - 4u < 0$, one finds exactly nine fields, with relative discriminants of norm 19, 23, 27, 35, 43, 55, 59, 64, 64. All of them appear in table 5 of [10] , and, except for 19, their L constant is less than 9 .

Theorem 6.1.1. is now an easy consequence of proposition 2.4, (i).

6.1.2. - The field K_1 has $L = 13$; the inequality $M \geq 9$ is a consequence of B'_3 applied to the polynomial $X^6 - X^5 - 2X^4 + X^3 + X^2 + 1$.

6.1.3. - The field K_2 has $L = 11$. The equality $M = 11$ is proved by applying A_2 , $(x^3 - x^2 - x)/(x-1)$, $(x^3 - x^2 - 2x+1)/(x^2-2x)$ to the polynomial $X^6 - 3X^5 + 5X^3 - X^2 - 2X + 1$; hence, K_2 is an exception to theorem 6.1.1.

6.1.4. - Totally complex quadratic extensions K of totally real cubic fields k can be studied by the method used to prove theorem 6.1.1. for extensions of $\mathbb{Q}(\eta)$; one finds that either $M(K) = M(k)$, or $K = k(\zeta_3)$, $M(K) = 3$ and $M(k) = 2$.

6.1.5. - One can apply proposition 2.4.1, (ii) for cubic extension K of $\mathbb{Q}(\zeta_4)$ after having classified the finitely many extensions K which contain an exceptional unit which is a square or the opposite of a square. One then proves the inequality

$M(K) \leq 5$ for these fields, except if K is one of the fields $\mathbb{Q}(\zeta_4, \eta)$, $\mathbb{Q}(\zeta_4, \alpha)$, the ray class field K' over $\mathbb{Q}(\zeta_4)$ whose conductor is a prime above 13 ($d_{K'} = -10\ 816$) and possibly the field $\mathbb{Q}(\zeta_4, \gamma)$. The field K' has $L = 8$, and one shows the equality $M = 8$ by applying the sequence B, $(x+1)/x^2$, $(x^2+x+1)/(x+1)$ to the polynomial $X^6 - X^4 - 2X^3 + 2X + 1$.

6.1.6. - Let k an imaginary quadratic field with $d_k < -4$, and let K be a cubic cyclic extension of k. The method of M.-N. Gras (see § 4.1) can be used to show the inequality $M(K) \leq 3$ for the fields K which do not possess exceptional units of the second kind. One sees that the inequality $M \leq 3$ holds for K except if $K = k(\eta)$ or if K is the Galois closure of one of the three cubic fields of discriminant -23, -31 or -44.

6.1.7. - CONJECTURE. - Let K be a field with unit rank at most 2. Then, up to finitely many exceptions, one has $M(K) = 7$ if $K \supset \mathbb{Q}(\eta)$, $M(K) = 5$ if $K \supset \mathbb{Q}(\alpha)$, $M(K) = 4$ if $K \supset \mathbb{Q}(\theta)$ and $M(K) \leq 3$ otherwise.

We saw in § 4, that the conjecture above is true for fields of degree $n \leq 3$. For fields of degree $n = 4$ (and hence $r \leq 2$), the only exceptions are probably the 9 fields considered in § 5.1, whose discriminants are +144, +125, +117, -275, -283, -331, -448, -475, -643 ; similarly it is possible that for $n = 5$ (and hence $r = 1$), the only exceptions are the 16 fields which occur in § . 5.2. Many exceptions can be found for $n = 6$, $r = 0$, and it would be difficult to state a precise conjecture.

6.2. - <u>Non totally complex sextic fields</u>. - We establish in this subsection some lower bounds of M for the three smallest known discriminants in each of the situations $r = 2$, $r = 4$ and $r = 6$.

6.2.1. - The field with $r = 2$ and $d = 28\ 037 = 23^2.53$ (a quadratic extension of $\mathbb{Q}(\alpha)$), defined by the polynomial $X^6 - 3X^5 + X^4 + 4X^3 - 3X^2 - 2X + 1$, has $L = 17$ and $M \geq 10$ by the sequence A_2, $(x^3-x)/(x^2-x-1)$.

6.2.2. - The field with $r = 2$ and $d = 29\ 077$ (a prime) defined by the polynomial $X^6 - X^5 - X^4 - X^2 + 2X + 1$ has $L = 13$ and $M \geq 9$ by the sequence B_3.

6.2.3. - The field with $r = 2$ and $d = 29\,189 = 17^2.101$, defined by the polynomial $X^6 - 3X^4 + X^2 + X + 1$ has $L = 13$ and $M \geq 10$ by the sequence C, $(x^2 - x - 1)/(x^2 - 2)$.

6.2.4. - The field with $r = 4$ and $d = -92\,779$ (a prime), defined by the polynomial $X^6 - X^5 - 4X^4 + 2X^3 + 4X^2 - 1$, has $L = 17$ and $M \geq 12$ by the sequence A_2 , $(x+1)/x$, $-x/(x^2-x-1)$, x^2+x .

6.2.5. - The field with $r = 4$ and $d = -94\,363 = -197.479$ of table 3 has also $L = 17$ and $M \geq 12$ by the sequence above.

6.2.6. - The field with $r = 4$ and $d = -103\,243 = -7^4 . 43$ (a quadratic extension of $\mathbb{Q}(\eta)$), defined by the polynomial $X^6 + X^5 - 3X^4 - 4X^3 + X^2 + 4X + 1$ has $L = 13$, and $M \geq 10$ by the sequence C^* .

6.2.7. - The field $\mathbb{Q}(\theta, \eta)$, with $r = 6$ and $d = 300\,125 = 5^3 . 7^4$ has $L = 29$ and $M \geq 18$ ([15], § 1).

6.2.8. - The field $\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$ with $r = 6$ and $d = 371\,293 = 13^5$ has $L = 13$ and $M \geq 11$ ([10], § 3.3).

6.2.9. - The field with $r = 6$ and $d = 434\,581 = 7^4.181$, a quadratic extension of $\mathbb{Q}(\eta)$, has $L = 13$ and $M \geq 11$ by the sequence C, $(x^2-x-1)/(x^2-2)$, $(x^3+x^2)/(x^3-x^2+1)$ applied to the polynomial $X^6 - 2X^5 - 4X^4 + 5X^3 + 4X^2 - 2X - 1$, the norm of $X^2 + \eta^{-1} X - 1$; it is a new Euclidean field.

7. - Special fields

In this section, we discuss fields which are of particular interest, and prove some lower bounds of M for fields of table 3 which need a special treatment.

We make no particular comments for fields with $n \leq 6$, since these cases are discussed in § 4, 5, 6.

Some discriminants appeared many times with various polynomials. We have not tried to prove that the different polynomials define the same fields (which is probably true), and have written only once each discriminant.

7.1. - Fields with $n = 7$, $r = 1$, $s = 3$. - The smallest three known discriminants are -184 607, -193 327 , -193 607 appearing for the polynomials $X^7 - X^6 - X^5 + X^3 + X^2 - X - 1$, $X^7 - 2X^4 - 3X^3 + X^2 + 3X + 1$, $X^7 + X^6 - 4X^5 - 4X^4 + 5X^3 + 4X^2 - X - 1$ respectively (Euclidean fields with these discriminants can be found in [10] , table 8) ; the inequality $M \geq 10$; $M \geq 8$; $M \geq 9$, resp. is proved by the sequence B'_2 , $x^3 - x^2 + 1$, x^3 ; B_1 , $(x+1)/x^2$; C respectively.

The field K with discriminant $-357\,911 = -71^3$ is a subfield of the Hilbert class field H of the field $k = \mathbb{Q}(\sqrt{-71})$; actually, the polynomial $f(X) = X^7 - X^6 - X^5 + X^4 - X^3 - X^2 + 2X + 1$ has the factorisation $f(X) \equiv (X-6)^2(X+22)^2\,(X-24)^2\,(X+15)$ mod 71 , which shows that Kk is an unramified extension of k ; if K were not a subfield of H , k would have an extension k' of absolute degree 98 with $|d_{k'}|^{1/98} = |d_k|^{1/2}$, in contradiction with the known lower bounds of discriminants ([3] , [17]). Another polynomial with discriminant -71^3 is $g(X) = X^7 - 2X^6 + 4X^5 - 4X^4 + 5X^3 - 4X^2 + 2X - 1$, and the method above shows that g again defines subfields of H . Sequence D shows the inequality $M \geq 6$ with g . Note that $L(K) = 7$, and $M(K) = 7$ by B_1 applied to f.

7.2. - Fields with $n = 7$, $r = 3$, $s = 2$. - The first three known discriminants, namely 612 233, 612 569 and 640 681 are quoted in table 3 ; one has $M \geq 11$ (resp. 10, 11) by the sequence C, $(x^3-x)/(x^3-x-1)$, $(x^4+x^3-2x^2-x)/(x^3-x-1)$ (resp. A_1 , $x^2/(x^2-1)$, $-1/(x^2-x-1)$; B_5).

The field with discriminant 674 057 of table 3 has $M \geq 9$ by the sequence A , $(x^2-x)/(x^2-x-1)$, $1/(2x-x^2)$, which is invariant under s .

7.3. - Fields with $n = 7$, $r = 5$, $s = 1$. - Two fields appear in table 3. The second one, with discriminant -2 369 207, has $M \geq 12$ by the sequence B_5 , $(x^2-x-1)/(x^3-2x)$. The first one, with discriminant -2 306 599 , has $M \geq 12$ by the sequence C , $-1/(x^2-x-1)$, $(x^2-x-1)/(x^2-2)$, x^3 .

The field with discriminant -2 616 839 = -61.42 899 , defined by the polynomial $X^7 - 4X^6 + 2X^5 + 4X^4 - X^3 - 2X - 1$ has $L = 13$, and $M \geq 11$ by the sequence B_5 . The inequality $M \geq 13$ is needed to prove that this field is Euclidean.

7.4. - Fields with $n = 8$, $r = 0$, $s = 4$. - The field with the smallest known discriminant ($1\ 257\ 728 = 2^8 . 17^3$, cf. [10], table 9) can be defined by the polynomial $X^4 - (2+\zeta_4)X^3 + (1+\zeta_4)X^2 - (1+\zeta_4)X + \zeta_4$. It has $L = 16$, and the sequence D shows $M \geq 6$; the better inequality $M \geq 8$ is proved in [15].

The cyclotomic field $\mathbb{Q}(\zeta_{15})$ can be defined by the polynomial $X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$; the sequence

$$0 , 1 , x , (x-1)/x , 1/(1-x) , x^2 , -1/x^2 , (x^2-1)/x^2 , 1/(1-x^2)$$

shows the inequality $M \geq 9$; conditions are $0 , \pm 1 , \zeta_4 , \zeta_6 , -\alpha , -\frac{1}{\alpha} , \zeta_8 , \zeta_{12} \in U(f)$; the sequence is invariant under the transformation $\omega \mapsto 1/\omega(1/x)$.

Table 3 contains 17 new Euclidean fields with $n = 8$, $r = 0$; among them, 7 contain a non trivial subfield.

7.5. - Fields with $n = 8$, $r = 2$, $s = 3$. - Table 3 contains 30 fields ; 29 of them are new Euclidean fields, and one of them was found by Mestre. Among these 30 fields, only 3 contain a non trivial subfield, and these can be obtained by a tower of quadratic extensions of $\mathbb{Q}(\theta)$. For two of them, the required inequality for M already holds for a quartic subfield. The third one is the field $\mathbb{Q}(\sqrt{5-4\sqrt{\theta}})$, with discriminant $4\ 960\ 000 = 2^8 . 5^4 . 31$; the inequality $M \geq 9$ is proved by the sequence A , $(x^2-1)/(x^2-x-1)$, $(x^3-x^2-x)/(x-1)$.

7.6. - Fields with $n = 8$, $r = 4$, $s = 2$. - The smallest known discriminant corresponds to the field $K_{8,4}$ of § 8 ; it is the ray class field modulo a prime above 29 in $\mathbb{Q}(\theta)$. As a quadratic extension of $\mathbb{Q}(\sigma)$, $K_{8,4}$ is defined by the polynomial $X^2 - (1+\theta^2\sigma)X + (1+\theta^2\sigma)$, whose norm is $X^8 - 5X^7 + 6X^6 + 3X^5 - 15X^4 + 19X^3 - 11X^2 + 4X - 1$, of discriminant $5^4 . 29^3 . 7^4 = 7^4 d_{K_{8,4}}$ ($K_{8,4}$ has discriminant 15 243 125). The best known inequality for M is $M \geq 10$, a consequence of the same inequality for $\mathbb{Q}(\sigma)$. The second discriminant we found is $15\ 297\ 613 = 37 . 643^2$; the corresponding field is defined by the polynomial

$$X^8 - 2X^7 - 3X^6 + 6X^5 + 2X^4 - 5X^3 + X^2 + 2X - 1 =$$

$$= (X^2 - (1+\delta_2^{-1})X + \delta_2)(X^6 - (1-\delta_2^{-1})X^5 + (2\delta_2 - 5\delta_2^2 - 2\delta_2^3)X^4 +$$

$$+ (7-2\delta_2-7\delta_2^2-2\delta_2^3)X^3 + (-5-5\delta_2+10\delta_2^2+4\delta_2^3)X^2 + (-3+2\delta_2+\delta_2^2)X - \delta_2^{-1}),$$

where $\delta_2^4 + 3\delta_2^3 - 2\delta_2 - 1 = 0$. The inequality $M \geq 14$ is proved by the sequence A_2 , x^2+x, $(x^2+x-1)/x$, $(x^3-x+1)/x$, $(x^3+x^2-x)/(x^2-1)$, x^3-x+1 . The inequality $M \geq 16$ would suffice to prove that this field is Euclidean. Other fields appeared for which the inequality $M \geq 16$ would suffice ; one of them is defined by the polynomial $X^8 - X^7 - 4X^6 + X^5 + 6X^4 + 2X^3 - 4X^2 - X + 1$ with discriminant 15 908 237 = 43.369 959 ; the inequality $M \geq 12$ is shown by the sequence A_2 , x^2+x , $(x^2+x-1)/x$, $(x+1)/x$.

7.7. - Fields of degree 9 . - Euclidean fields are known only for $r = 1$; 10 fields can be found in table 3 ; they do not contain cubic fields. The field with discriminant 33 626 161 is defined by the polynomial $X^9 - X^8 - 3X^7 + 2X^6 + 2X^5 + 2X^3 - X^2 - 2X - 1$; the inequality $M \geq 10$ comes using the sequence B , $x^2/(x^2-1)$, $(x^3-x)/(x^3-x-1)$, $1/(x^2-x)$, $(x^3-x-1)/(x-1)$. The field with discriminant 36 155 633 is defined by the simple polynomial $X^9 + X^7 + X^6 - X^3 - X^2 - X - 1$; the inequality $M \geq 10$ is proved via the sequence III , $-1/x$, $-1/x^2$, x^2+1 , $-(x+1)/x^2$, x^3+x+1 .

For $n = 9$, $r \geq 3$, one probably needs the difficult inequality $M \geq 17$ to find Euclidean fields by Lenstra's method. This is the inequality one needs to handle the field with $n = 9$, $r = 3$ and discriminant -110 852 311 = $-31^3.61^2$, which is the ray class field over $\mathbb{Q}(\gamma)$ modulo the prime ideal of degree 1 above 61 . This field was discovered as the field defined by a root of the polynomial $X^9 + 2X^8 - 2X^7 - 7X^6 - 3X^5 + 8X^4 + 9X^3 - 3X^2 - 5X - 1$, which is the norm of the polynomial $X^3 - \gamma^2 X^2 - X - \gamma^4$; one has $M \geq 10$ by C^* . Here are two more examples with $n = 9$, $r = 3$: the field with prime discriminant -112 992 391 , defined by the polynomial $X^9 - 4X^7 + X^6 + 5X^5 - 2X^4 - 3X^3 + 2X + 1$, has $M \geq 11$ by the sequence C , $(x^3+x^2)/(x^2+x-1)$, $-x^3+2x+1$, and the field with discriminant -113 511 599 = -193. 727. 809 , defined by the polynomial $X^9 + X^8 - 4X^7 - 3X^6 + 5X^5 + 3X^4 - 2X^3 - 2X^2 + X + 1$ has $M \geq 11$ by C^* , $(x^2+x-1)/x$.

7.8. - Fields of degree 10 . - Three fields appear in table 3 ; one of them (a cyclic extension of $\mathbb{Q}(\zeta_3)$) was found by Mestre. The other two, which do not contain any non trivial subfields since their discriminants are prime numbers, are new Euclidean fields. The last one was found by the sequence C^* . The first one has $M \geq 10$ by the sequence
B , $x^2/(x^2-1)$, $(x^3-x)/(x^3-x-1)$, $(x^3-x-1)/(x-1)$, $-x^5+2x^3+x^2$; conditions are $0, 1, -1, \theta, \alpha, \sqrt{2}, 1/\gamma, \delta^2 \in U(f)$ and, moreover, that the five following elements should be units : $x^4+x^3-2x^2-2x-1$, $x^6-3x^4-x^3+2x^2+x+1$, $x^5-2x^3-x^2+1$, $x^6-x^5-2x^4+2x^2+2x-1$, $x^6-x^5-2x^4+2x^3+x^2-x-1$.

8. - Small discriminants

It is an experimental fact that, for low degrees, the fields whose root discriminants are very small when compared with Odlyzko's lower bounds under GRH have a rather large M constant. We cannot state any precise conjecture ; large means at least greater than the degree of the field. This phenomenon appears clearly in § 4 to 6 , where explicit upper bounds of M are given. Examples of large values of M for fields of degree ≥ 7 can be found in § 7.

This remark can be used in the other direction to find fields with small discriminants : one constructs polynomials which satisfy some of the conditions given in § 3, and choose among these polynomials those with not too large coefficients. It was in this way that the field with $n = 7$, $r = 5$ and discriminant -2 306 599 (cf. table 4) was discovered and quoted in [14] before it was proved Euclidean. Fields with small discriminants were found when testing exceptional sequences. We give a brief account of the results, and list in table 4 for pairs (n, r) with $n \leq 8$, $n \leq 9$ and $r < 9$ and $n = 10$, $r \leq 6$ the smallest value we found for the root discriminant $|d_K|^{1/n}$ of a field with the corresponding values for n and r . We denote by $K_{n,r}$ such a field (warning : the notation is not that of [14]). For $n = 7$ and for $n = 8$, $r \neq 2$, these fields are those of [14], § 4. For $n \leq 6$ and $n = r = 7$, they are known to be those with the smallest value of $|d_K|$ ([19] , [20]). For $n \leq 6$ and for $(n, r) = (7, 1)$ and $(8, 0)$, they are quoted in [10] ; they are Euclidean, and so are the fields $K_{n,r}$ for $(n, r) = (7, 3)$, $(7, 5)$, $(8, 2)$, $(9, 1)$ and $(10, 0)$ (see table 3).

The field $K_{8,0}$ is the ray class field over $\mathbb{Q}(\zeta_4)$ with conductor $\mathfrak{P}_{17}$ (we keep the notation of [13] : $\mathfrak{P}_p$ denotes a prime ideal of degree 1 above the prime number p) ; its discriminant is minimal among the fields which contain a quartic subfield. The same result holds for the field of conductor $\mathfrak{P}_{59}$ over $K_{4,2}$, which was used in [14] ; but 7 fields with a smaller value of $|d_K|$ were discovered after [14] was written ; so, we take for $K_{8,2}$ the field with discriminant $-4\ 296\ 311 = -199.21\ 589$ of table 3 . The field $K_{8,4}$ is the ray class field of conductor $\mathfrak{P}_{29}$ over $\mathbb{Q}(\theta)$. The field $K_{8,6}$ is the ray class field of conductor $\mathfrak{P}_{131}$ over $K_{4,4}$ and the field $K_{8,8}$ is the ray class field of conductor $\mathfrak{P}_{41}$ over $\mathbb{Q}(\sqrt{2})$.

We now discuss examples of degree 9 . The field $K_{9,1}$ is the field with discriminant $30\ 451\ 401 = 31.982\ 271$ of table 3 . The field $K_{9,3}$ is the ray class field of conductor $\mathfrak{P}_{61}$ over $\mathbb{Q}(\gamma)$ (see § 7.7) . The field $K_{9,5}$ is defined by the polynomial $X^9 + 2X^8 - 6X^7 - 7X^6 + 9X^5 + 9X^4 - 3X^3 - 5X^2 + 1$; its discriminant is $485\ 533\ 729 = 4\ 283.113\ 363$. Another interesting example with $n = 9$, $r = 5$ is provided by the polynomial $X^9 - X^8 - 4X^7 + 4X^6 + 4X^5 - 4X^4 - 2X^3 + 2X^2 + 2X - 1$ with discriminant $489\ 385\ 129$, a prime. The field $K_{9,7}$ is defined by the polynomial $X^9 + X^8 - 4X^7 - 5X^6 + 3X^5 + 9X^4 + 2X^3 - 6X^2 - X + 1$; its discriminant is $-2\ 385\ 869\ 687 = -7\ 121.335\ 047$.

We finish the list of the fields $K_{n,r}$ by taking for $K_{10,0}$ the field with discriminant $-215\ 067\ 767$ of table 2 , for $K_{10,2}$ the field with discriminant $817\ 298\ 432 = 2^{10}.798\ 143$ defined by the polynomial $X^{10} - 4X^8 - 2X^7 + 5X^6 + 6X^5 - X^4 - 6X^3 - X^2 + 2X + 1$, for $K_{10,4}$ the field with discriminant $-3\ 617\ 508\ 259 = -127.28\ 484\ 317$ defined by the polynomial $X^{10} - 3X^8 - 3X^7 + 2X^6 + 6X^5 + 3X^4 - 2X^3 - 3X^2 - X + 1$, and for $K_{10,6}$ the field with discriminant $19\ 936\ 537\ 141$, defined by the polynomial $X^{10} - X^8 - X^7 - 8X^6 + 4X^5 + 15X^4 - 4X^3 - 7X^2 + X + 1$.

The fields $K_{n,r}$ listed above are not claimed to be those with minimal discriminant in absolute value for the given values of n and r . Actually, we did not make great efforts to find fields with $n = 8$, $r \geq 4$ or $n = 9$, $r \geq 3$, or $n = 10$, $r \geq 2$, since the lower bounds for M which are required to prove that these fields are Euclidean are somewhat too large. However, it is well possible that some of the fields we considered in § 7 with $n = 8$, $r = 4$ or $n = 9$, $r = 3$ have big enough M constant to be proved Euclidean by Lenstra's method. A near miss is provided for $n=12$, $r=0$ by the ray class field of conductor $\mathfrak{P}_{37}$ over $\mathbb{Q}(\zeta_3)$, for which one needs the inequality $M \geq 20$, whereas Mestre ([15], § 1) has proved the inequality $M \geq 18$.

For signature (n, r) with $r < 7$, $n = 8$, $r = 0$ or 2 and $n = 9$, $r = 1$, a more intensive research was made. For this reason, we finish this section by the

CONJECTURE. - For $(n,r) = (7,1)$, $(7,3)$, $(7,5)$, $(8,0)$, $(8,2)$ and $(9,1)$, the fields $K_{n,r}$ are the fields with the minimal value of $|d_K|$.

9. - Tables

Table 1 can be found in section 3. It is similar to table 10 of Lenstra, [10].

Table 2 contains the discriminants d_K of all norm Euclidean fields of degree 2, 3, 4 with a sufficiently large Lenstra constant and of norm Euclidean extensions of degree 6 and 8 with likewise sufficiently large Lenstra constant M. Inclusions are indicated and, in some cases a field generator is added ; d_K is underlined whenever, for a proper subfield K_o, the inequality $M(K) \geq M(K_o)$ already proves K to be Euclidean ; 18 of the given fields are new. The fields in degree 2 and 3 of course, and the totally real and totally complex quartic fields with one exception ($d_K = 229$) where known to be Euclidean before Lenstra's paper [10], likewise the two cyclotomic fields $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{15})$.

Table 3 contains a list of all Euclidean number fields obtained by lower bounds for M after [10] appeared. It includes the four fields found by Mestre. This table is divided into ten parts according to the different values n, r, s of the involved field K. We give the discriminant $d_K = d$ and its prime factorization. Unless $n = 7$, the second column contains either 0 -and then the field does not have any proper subfield- or one of those symbols listed in table 1 which generates a proper subfield K_o of maximal degree. In the first case $K_o = \mathbb{Q}$. Next columns contain the coefficients of a monic, irreducible polynomial $f \in K_o[X]$ generating the field in question, a lower bound for M needed to prove K to be Euclidean via the estimates of Lenstra. The last column gives the sequence in terms of a zero x of f, which allows to conclude the validity of the lower bound for M. In some cases, a reference is given to previous sections. Some of the polynomials of table 3 were computed by Lenstra. As we were looking only for polynomials with reasonably low discriminants, fields without a power basis for the integers will have escaped even if their discriminant is low and at the same time their Lenstra constant is large enough. For example, the field $\mathbb{Q}(\zeta_3, \theta)$ would not have been detected by this method. $U(f)$ clearly is defined for all monic $f \in \mathbb{Z}[X]$, and for a monic factor $g \in \mathbb{Z}[X]$ one has $U(g) \supset U(f)$. Therefore, irreducibility is easily handled with.

Table 4 is an improvement of [14], table II. It gives for given (n, r) the lower bound $\mathrm{Odl}_{n,r}$ of $|d_K|^{1/n}$, obtained by Odlyzko under GRH, for fields K of degree n with r real places, and the number $(|d_{K_{n,r}}|^{1/n}/\mathrm{Odl}_{n,r})-1$, written as a percentage.

Table 5 is an update of Lenstra's table 11 of [10].

-:-:-:-

Added in proof (october, 1982)

One of us (A. Leutbecher) has found 34 new euclidean fields by convenient enlargements of sequence D (3 with $n=7$, $r=1$, 9 with $n=8$, $r=2$ and 22 with $n=9$, $r=1$). One of these fields, defined by the polynomial $X^9-X^8+X^7-3X^6+5X^5-8X^4+8X^3-6X^2+3X-1$, has discriminant $101.292\,181 = 29\,510\,281$ and can be taken as a new field $K_{9,1}$ (§ 8). The total amount of known euclidean fields is now 466, and, in table 5, the new numbers for $(n, r+s) = (7,4)$, $(8,5)$ and $(9,5)$ are 39, 39 and 32 instead of 36, 30 and 10 respectively. In table 4, one can put 0,92 % instead of 1,27 % for $n=9$, $r+s=5$, and the conjecture which ends section 8 must be subsequently modified. Some lower bounds of M can be improved (e.g. $M \geq 11$ for $K_{8,0}$, $M \geq 12$ for $\mathbb{Q}(\zeta_{15})$), and a field with $n=9$, $r=3$ and discriminant $-367.299\,401 = -109\,880\,167$ appeared, which can be used as a new $K_{9,3}$ (in table 4, one has then 1,02 % instead of 1,12 %).

These results will appear somewhere else.

Table 2

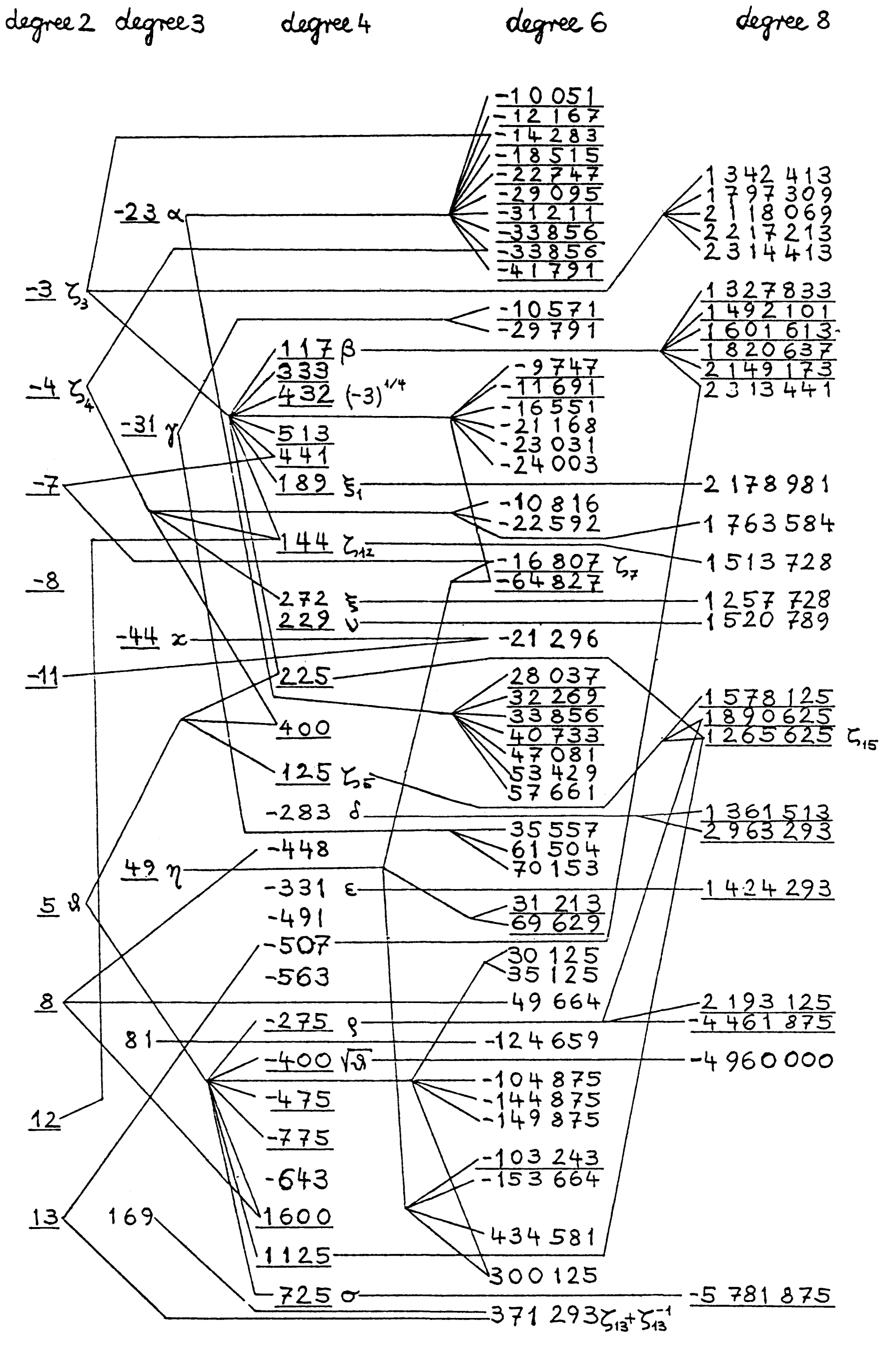
degree 2
degree 3
degree 4
degree 6
degree 8
-3 ζ_3
-4 ζ_4
-7
-8
-11
5 ϑ
8
12
13
-23 α
-31 γ
-44 x
49 η
81
169
117 β
333
432 $(-3)^{1/4}$
513
441
189 ξ_1
144 ζ_{12}
272 ξ
229 ν
225
400
125 ζ_5
-283 δ
-448
-331 ε
-491
-507
-563
-275 ϱ
-400 $\sqrt{\vartheta}$
-475
-775
-643
1600
1125
725 σ
-10 051
-12 167
-14 283
-18 515
-22 747
-29 095
-31 211
-33 856
-33 856
-41 791
-10 571
-29 791
-9 747
-11 691
-16 551
-21 168
-23 031
-24 003
-10 816
-22 592
-16 807 ζ_7
-64 827
-21 296
28 037
32 269
33 856
40 733
47 081
53 429
57 661
35 557
61 504
70 153
31 213
69 629
30 125
35 125
49 664
-124 659
-104 875
-144 875
-149 875
-103 243
-153 664
434 581
300 125
371 293 $\zeta_{13}+\zeta_{13}^{-1}$
1 342 413
1 797 309
2 118 069
2 217 213
2 314 413
1 327 833
1 492 101
1 601 613
1 820 637
2 149 173
2 313 441
2 178 981
1 763 584
1 513 728
1 257 728
1 520 789
1 578 125
1 890 625
1 265 625 ζ_{15}
1 361 513
2 963 293
1 424 293
2 193 125
-4 461 875
-4 960 000
-5 781 875

Table 3

$n = 6$, $r = 2$, $s = 2$

d	K_o	a_o , a_1 , ...	$M \geq$	sequence
47 149 prime	0	1 , -1 , 2 , 2 , -3 , -1 , 1	6	B
50 173 = 131.383	0	1 , 2 , 0 , -4 , -2 , 1 , 1	6	B
51 757 = 73.709	0	1 , 1 , -2 , -2 , 0 , 0 , 1	6	B
57 152 = 2^6.19.47	0	1 , 2 , 2 , -2 , -3 , 0 , 1	6	B
57 661 = 23^2.109	α	$-\alpha^3$, -1 , 1	6	A, [15]
62 437 = 29.2 153	0	-1 , -1 , -3 , 4 , 3 , -4 , 1	7	A
66 049 = 257^2	γ_1	1 , $1+\gamma_1$, 1 $(\gamma_1^3 + 2\gamma_1^2 - 3\gamma_1 - 1 = 0)$	7	§ 4.4
70 153 = 31^2.73	γ	-1 , $-\gamma^{-1}$, 1	7	A

$n = 6$, $r = 4$, $s = 1$

$-d$	K_o	a_o , a_1 , ...	$M \geq$	sequence
94 363 = 197.479	0	-1 , -1 , 5 , 2 , -4 , -1 , 1	7	A
104 483 = 163.641	0	1 , -1 , -4 , 6 , 2 , -4 , 1	7	A
104 875 = 5^3.839	θ	$-\theta$, -1 , -1 , 1	7	A
118 987 = 11.29.373	0	1 , 1 , -5 , 4 , 3 , -4 , 1	7	A
124 659 = 3^8.19	η_1	$-\eta_1$, $1-\eta_1^2$, $1 (\eta_1^3 - 3\eta_1 + 1 = 0)$	7	A
144 875 = 5^3.19.61	θ	1 , 2θ , $-2-\theta$, 1	8	A , θ^2
149 875 = 5^3.11.109	θ	-1 , $-\theta^2$, 0 , 1	8	B_2
153 664 = $2^6.7^4$	η	η , 0 , 1	8	B , x^2+x , $\frac{x^2+x-1}{x}$
161 939 = 67.2 417	0	-1 , -1 , 4 , 3 , -3 , -2 , 1	8	B , x^2+x , $\frac{2x+1}{x}$

$n = 6$, $r = 6$, $s = 0$

d	K_o	a_o , a_1 , ...	$M \geq$	sequence
434 581 = 7^4.181	η	-1 , η^{-1} , 1	11	§ 6.2.9

Table 3 (continued)

n = 7 , r = 1 , s = 3

- d	$a_o, a_1, \dots$	$M \geq$	sequence
261 871 = 307. 853	1, 0, -1, 3, 1, -4, 0, 1	6	B
283 223 = 61. 4 643	1, 0, 0, 0, 1, 0, -2, 1	6	B
286 711 prime	1, 0, -1, 2, 1, -2, -1, 1	6	B
289 831 = 109. 2 659	-1, -4, -2, 8, 3, -5, -1, 1	6	A
289 987 prime	-1, -2, -3, 4, 5, -3, -2, 1	6	A
311 071 = 277. 1 123	-1, 1, -3, 3, -4, 4, -2, 1	6	D, [15]
334 727 prime	-1, -1, 1, 4, 1, -3, -1, 1	6	B
338 191 = 7. 48 313	1, 2, 0, -2, -1, 0, 0, 1	6	B
357 911 = 71^3	1, 2, -1, -1, 1, -1, -1, 1	6	B
380 831 = 11. 89. 389	1, 2, 0, -1, -1, -1, 0, 1	7	B , $(x+1)/x^2$
396 259 prime	-1, 1, 0, -1, 1, 0, 0, 1	7	V^*
424 831 = 11^2. 3 511	-1, -2, 2, 4, -3, -3, 1, 1	7	B_1
433 391 = 7. 101. 613	-1, -2, -2, 3, 4, -2, -2, 1	7	B_1

n = 7 , r = 3 , s = 2

d	$a_o, a_1, \dots$	$M \geq$	sequence
612 233 = 71. 8 623	-1, -3, 1, 5, 0, -4, 0, 1	8	C
612 569 = 593. 1 033	-1, -4, 2, 2, 1, 1, -3, 1	8	A_1
640 681 = 59. 10 859	1, 2, -2, 0, 2, -2, -1, 1	8	B_2
649 177 = 59. 11 003	1, 1, 0, 1, 0, -3, 0, 1	8	B_2
661 033 = 173. 3 821	-1, -2, 3, 5, -1, -4, 0 1	9	C
674 057 prime	-1, 0, 0, 0, 4, 0, -3, 1	9	§ 7.2

Table 3 (continued)

$n = 7$, $r = 3$, $s = 2$

d	$a_o, a_1, \ldots$	$M \geq$	sequence
689 033 prime	1, 3, 2, -2, -3, -2, 1, 1	9	C
696 401 = 109.6 389	1, 4, 4, -3, -7, -1, 2, 1	9	B_2, $(x^3+x^2-x-1)/x$
724 873 = 31.67.349	-1, -1, -1, 3, 5, -3, -2, 1	9	A_2
726 721 = 79.9 199	-1, 0, 2, 3, 0, -4, 0, 1	9	C
746 633 = 127.5 879	-1, 1, 0, -2, 5, 0, -3, 1	9	A_2
753 209 = 37.20 357	1, -2, -3, 6, 4, -5, -1, 1	9	A_2
763 993 = 113.6 761	1, 2, 0, -2, 1, -1, -1, 1	9	B_3
765 529 = 19.43.937	1, 3, 1, -3, -1, -1, 0, 1	9	B_3
780 401 prime	1, -2, -5, 5, 7, -4, -2, 1	9	A_2
788 857 = 31.25 447	-1, -5, -1, 8, 3, -5, -1, 1	9	A_1, $-x/(x^2-x-1)$
789 289 = 79.97.103	-1, 0, 2, 4, -1, -4, 0, 1	9	C
792 873 = 3^2.37.2 381	1, 1, 1, 2, -3, -3, 1, 1	9	B_3
794 233 = 11.103.701	1, -1, 0, 4, 0, -4, 0, 1	9	C
796 753 = 41.19 433	-1, -2, 4, 8, -5, -6, 2, 1	9	C
819 713 = 41.19 993	-1, -3, 0, 5, 2, -4, -1, 1	9	A_1, $-x/(x^2-x-1)$
830 801 prime	1, 0, -4, 0, 5, -2, -2, 1	9	A_2
877 193 = 739.1 187	-1, 1, 5, 0, -4, -1, 0, 1	10	B_3, $x/(x^2-1)$
909 673 = 23.39 551	-1, -3, -3, 5, 6, -4, -2, 1	10	B_3, $x/(x^2-1)$

$n = 7$, $r = 5$, $s = 1$

- d	$a_o, a_1, \ldots$	$M \geq$	sequence
2 306 599 = 107.21 557	-1, 1, 3, 1, -1, -3, 0, 1	12	§ 7.3
2 369 207 = 23.239.431	1, 0, -1, 5, -1, -5, 1, 1	12	§ 7.3

Table 3 (continued)

$n = 8$, $r = 0$, $s = 4$

d	K_o	a_o , a_1 , . . .	M ≥	sequence
1 717 853 prime	0	1, 1, -2, -2, 4, 2, -3, -1, 1	6	B
1 740 113 prime	0	1, 3, 1, -5, -2, 4, 0, -2, 1	6	B
1 763 584 = $2^8.83^2$	ζ_4	ζ_4, ζ_4 , $-1-\zeta_4$, $-1-\zeta_4$, 1	6	B
1 901 413 prime	0	1, 0, -3, 1, 6, -1, -4, 0, 1	6	B
1 925 093 = 1 063.1 811	0	1, 3, 1, -4, -2, 2, 0, -1, 1	6	B
2 020 553 = 113.17 881	0	1, 1, -3, -3, 4, 4, -2, -2, 1	6	B
2 105 893 = 29. 72 617	0	1, -1, 2, -1, 1, -1, 1, -2, 1	6	D
2 118 069 = $3^4.79.331$	ζ_3	-1, ζ_6 , $-\zeta_6$, ζ_6-1, 1	6	D
2 178 981 = $3^6.7^2.61$	ξ_1	ζ_6, $-\xi_1$, 1 $(\xi_1^2-\xi_1-\zeta_6=0)$	6	D
2 193 125 = $5^4.11^2.29$	ρ	1, ρ , 1	6	§ 5.4
2 217 213 = $3^4.31.883$	ζ_3	ζ_6, $-1-\zeta_6$, $1+2\zeta_6$, $-1-\zeta_6$, 1	6	D
2 217 749 prime	0	1, 1, -3, -4, 3, 6, -1, -3, 1	6	B
2 314 413 = $3^4.28\,573$	ζ_3	ζ_3, ζ_3, ζ_3^{-1} , 0 , 1	7	B, $(x+1)/x^2$
2 338 213 prime	0	1, 2, -3, -7, 6, 7, -4, -2, 1	7	A
2 542 753 = 409. 6 217	0	1, 3, 2, -3, -4, 1, 1, -1, 1	7	B , $(x+1)/x^2$

Table 3 (continued)

$n = 8$, $r = 0$, $s = 4$

d	K_o	$a_o, a_1, \ldots$	$M \geq$	sequence
2 590 093 = 11.41.5 743	0	1, 2, 1, -5, -4, 7, 2, -4, 1	7	A
2 606 473 prime	0	1, -2, 6, -9, 11, -10, 6, -3, 1	7	D, $(x^3-2x^2+x-1)/(x^3-x^2+x-1)$
2 963 293 = 37.283^2	δ	$1+\delta$, δ^2-1, 1	7	§ 5.4

$n = 8$, $r = 2$, $s = 3$

- d	K_o	$a_o, a_1, \ldots$	$M \geq$	sequence
4 296 211 = 199.21 589	0	-1, -3, -4, 4, 8, -1, -5, 0, 1	9	C
4 297 507 = 2 011.2 137	0	-1, 1, 4, -6, -2, 8, -1, -3, 1	9	A_2
4 364 587 = 29.150 503	0	-1, -4, -2, 7, 4, -3, -3, 0, 1	9	B_3
4 386 467 = 41.83.1 289	0	1, 1, 1, -3, -1, 4, -1, -2, 1	9	B'_3
4 421 387 = 1 321.3 347	0	1, -1, -1, 2, 2, 0, -2, -1, 1	9	B'_3
4 423 907 prime	0	-1, -4, -4, 7, 9, -5, -5, 1, 1	9	B_3
4 456 891 prime	0	-1, 3, 3, -8, -1, 8, -1, -3, 1	9	A_2
4 461 875 = $5^4.11^2.59$	ρ	1, $1-\rho^{-1}$, 1	9	§ 5.4

Table 3 (continued)

$n = 8$, $r = 2$, $s = 3$

$-d$	K_o	$a_o, a_1, \ldots$	$M \geq$	sequence
4 505 651 prime	0	-1, -3, 0, 5, 4, -4, -4, 1, 1	9	C
4 570 723 prime	0	-1, -2, -1, 3, 5, -3, -4, 1, 1	9	C
4 584 491 = 19.101.2 389	0	-1, -3, 0, 8, 4, -5, -4, 1, 1	9	C
4 596 992 = 2^8.17 957	0	-1, 0, 3, 2, -3, 0, 1, -2, 1	9	B'_3
4 603 987 prime	0	-1, -1, 0, 0, 2, 1, -2, -1, 1	9	B'_3
4 614 499 prime	0	-1, 3, 1, -9, 0, 8, -1, -3, 1	9	A_2
4 623 371 = 18.31^2.283	0	1, 1, -4, 0, 8, -1, -6, 1, 1	9	B_3
4 648 192 = 2^8.67.271	0	1, 2, -3, -2, 6, 0, -4, 0, 1	9	B_3
4 663 051 = 31.359.419	0	1, -1, -3, 5, 5, -4, -4, 1, 1	9	C
4 690 927 = 443.10 589	0	-1, -2, 0, 0, 3, 2, -3, -1, 1	9	B_3
4 775 363 = 1 931.2 473	0	1, 0, -6, -2, 9, 1, -5, 0, 1	9	C
4 785 667 = 29.59.2 797	0	-1, -3, -1, 1, 5, 2, -4, -1, 1	9	B_2, $(x^4-2x^2)/(x^3-x-1)$
4 809 907 = 19.253 153	0	-1, -2, 1, 5, 4, -4, -4, 1, 1	9	C
4 858 379 = 17^2.16 811	0	1, -1, -4, 4, 8, -4, -5, 1, 1	9	C , [15]

Table 3 (continued)

$n = 8$, $r = 2$, $s = 3$

$-d$	K_o	$a_o, a_1, \dots$	$M \geq$	sequence
4 960 000 = $2^8.5^4.31$	$\sqrt{\theta}$	$\sqrt{\theta}-1$, -1, 1	9	§ 7.5
5 040 467 prime	0	1, -1, -3, 1, 7, 0, -5, 0, 1	9	C
5 040 547 = 37.59.2 309	0	1, 2, -2, -1, 1, 1, 0, -2, 1	9	B'_2, $(x^2+x+1)/(x+1)$
5 103 467 prime	0	-1, 0, 3, 2, 1, -3, -3, 1, 1	9	C
5 165 819 = 641.8059	0	-1, -3, -1, 3, 5, -1, -4, 0, 1	9	B_2 , $(x^3-x)/(x^3-x-1)$
5 286 727 prime	0	1, 1, -3, 0, 5, 0, -4, 0, 1	10	C , $(x^2+x-1)/x$
5 781 875 = $5^4.11.29^2$	σ	1, $-\sigma$, 1	10	§ 5.4
6 011 107 = 149.40 343	0	1, 0, -3, 3, 6, -4, -4, 1, 1	10	B_3 , $x/(x^2-1)$

Table 3 (continued)

$n = 9$, $r = 1$, $s = 4$

d	K_o	$a_o , a_1 , \dots$	M ≥	sequence
30 450 401 = 31.982 271	0	1, 1, -2, -4, 3, 7, -2, -4, 0, 1	9	B'_3
30 626 693 prime	0	-1, -3, -2, 2, 3, 4, -1 -4, 0, 1	9	B_2 , $(x^3-x^2-x)/(x^3-x-1)$
31 638 601 prime	0	1, -2, -3, 8, 1, -10, 6, 3, -4, 1	9	A_2
32 652 713 prime	0	-1, -1, 1, 1, 2, 3, -2, -3, 0, 1	9	B'_3
32 923 873 = 809.40 697	0	-1, 0, 0, 0, -2, -1, 5, 0, -3, 1	9	A_1 , $x^2/(x^2-1)$
33 626 161 = 23.67.21 821	0	-1, -2, -1, 2, 0, 2, 2, -3, -1, 1	10	§ 7.7
34 405 373 prime	0	1, 1, 0, -2, -2, 4, 2, -3, -1, 1	10	B'_3 , $-1/(x^3-x^2-x)$
35 051 893 = 109.321 577	0	1, 1, -3, -4, 5, 8, -4, -5, 1, 1	10	C , $(x^3+x^2-x-1)/x$
36 155 633 prime	0	-1, -1, -1, -1, 0, 0, 1, 1, 0, 1	10	§ 7.7
38 159 713 = 17.2 244 689	0	-1, -2, -4, -1, 8, 7, -5, -5, 1, 1	10	C^*

Table 3 (end)

$n = 10$, $r = 0$, $s = 5$

- d	K_o	a_o , a_1 , ...	M ≥	sequence
215 067 767 prime	0	1, 2, 3, -4, -7, 1, 7, 2, -4, -1, 1	10	§ 7.8
224 415 603 = $3^5 . 31^4$	ζ_3	-1, $2\zeta_3$-1, $2\zeta_3$+1, ζ_3 , $2\zeta_3$+1, 1	10	[15]
236 438 047 prime	0	1, 2, -2, -5, 1, 6, 4, -4, -4, 1, 1	10	C^*

Table 4

Small discriminants

r+s \ n	2	3	4	5	6	7	8	9	10
1	1.721 0.64%								
2	2.225 0.50%	2.820 0.85%	3.263 0.79%						
3		3.639 0.56%	4.036 0.90%	4.345 0.77%	4.592 0.65%				
4			5.124 1.27%	5.322 1.11%	5.484 0.51%	5.619 0.61%	5.734 0.92%		
5				6.640 2.55%	6.638 1.36%	6.653 0.85%	6.675 1.08%	6.699 1.27%	6.726 1.27%
6					8.143 0.48%	7.960 1.88%	7.834 0.90%	7.745 1.12%	7.680 1.36%
7						9.611 14.99%	9.266 3.00%	9.012 2.40%	8.818 2.44%
8							11.036 3.16%	10.547 4.43%	10.177 5.28%

Table 5

The number of known Euclidean fields

r+s	n										Total
	1	2	3	4	5	6	7	8	9	10	
1	1	5									6
2		16	52	34							102
3			57	11	12	28					108
4				9	10	33	36	43			131
5					1	11	24	30	10	4	80
6						3	2	0	0	0	5
Total	1	21	109	54	23	75	62	73	10	4	432

REFERENCES

[1] I.O. ANGELL, A Table of Totally Real Cubic Fields, Math. Comp. 30, 184-187 (1976).

[2] W. G. CIOFFARI, The Euclidean condition in püre cubic and complex quartic fields, Math. Comp. 33, 389-398 (1979).

[3] F. DIAZ Y DIAZ, Tables minorant la racine n-ième du discriminant d'un corps de degré n, Publ. Math. Orsay, 80.06 (1980).

[4] H. J. GODWIN, Real quartic fields with small discriminants, J. London Math. Soc. 31, 478-485 (1956).

[5] H. J. GODWIN, On totally complex quartic fields with small discriminants, Proc. Cambridge Phil. Soc. 53, 1-4 (1957).

[6] H. J. GODWIN, On quartic fields of signature one with small discriminant, Quart. J. Math. Oxford 8, 214-222 (1957).

[7] M.-N. GRAS, Lien entre le groupe des unités et la monogénéité des corps cubiques cycliques, Publ. Math. Fac. Sc. Besançon, année 1975-76, fasc. 1, 19p.

[8] A. HURWITZ, Zur Theorie der algebraischen Zahlen, Nachr. der k. Ges. d. Wiss. Göttingen, Math. Phys. Klasse, 324-331 (1895) ; Werke, Bd 2, 236-243.

[9] A. HURWITZ, Der Euklidische Divisionssatz in einem endlischen algebraischen Zahlkörper, Math. Z. 3, 123-126 (1919); Werke, Bd 2, 471-474.

[10] H. W. LENSTRA, Jr., Euclidean Number Fields of Large Degree, Invent. Math. 38, 237-254 (1977).

[11] H. W. LENSTRA, Jr., Quelques exemples d'anneaux euclidiens, C.R.Acad. Sc. Paris, 286, A, 683-685 (1978).

[12] H. W. LENSTRA, Jr., Euclidean Number Fields 1, 2, 3, Math. Intelligencer 2, 6-15, 73-77, 99-103 (1979-80).

[13] J. MARTINET, Petits discriminants, Ann. Inst. Fourier, XXIX, 159-170 (1979).

[14] J. MARTINET, Petits discriminants des corps de nombres, Lectures Notes of the London Math. Soc. (to appear).

[15] J.-F. MESTRE, Corps euclidiens, unités exceptionnelles et courbes elliptiques, J. Number Theory 13, 123-137 (1981).

[16] T. NAGELL, Sur un type particulier d'unités algébriques, Ark. Math. 8, 18, 163-184 (1969).

[17] A. M. ODLYZKO, Discriminant Bounds, Mimeographed, 1976.

[18] O. T. O'MEARA, On the finite generation of linear groups over Hasse domains, J. reine angew. Math. 217, 79-108 (1965).

[19] M. POHST, The minimum Discriminant of Seventh Degree Totally Real Algebraic Number Fields, Number Theory and Algebra, H. Zassenhaus ed., 235-240, Academic Press, New York, 1977.

[20] M. POHST, On the Computation of Number Fields of Small Discriminants Including the Minimum Discriminants of Sixth Degree Fields, J. Number Theory 14, 99-117 (1982).

[21] H. WEBER, Lehrbuch der Algebra, 2 nd ed., Bd. 3, 1908.

-:-:-:-

Armin LEUTBECHER
Mathematisches Institut der
Technischen Universität
D - 8000 MÜNCHEN 2
Postfach 20 24 20

Jacques MARTINET
L. A. au C.N.R.S. n° 226
U.E.R. de Mathématiques
et d'Informatique
Université de Bordeaux I
F 33405 TALENCE CEDEX