ON EUCLID'S ALGORITHM IN CYCLIC FIELDS

H. HEILBRONN

1. Introduction. In two papers I have proved that there are only a finite number of quadratic fields [6] and of cyclic cubic fields [7] in which Euclid's algorithm (E.A.) holds. Davenport has shown by a different method that there are only a finite number of quadratic fields [1, 2], of non-totally real cubic fields [3, 4] and of totally complex quartic fields in which E.A. holds.

The object of this paper is to extend these results to cyclic fields of higher degree. I shall prove

THEOREM 1. *For every $k \geqslant 4$ there are only a finite number of cyclic fields K of degree k whose discriminant Δ is the power of a prime, in which* E.A. *holds.*

The methods employed in this paper could actually furnish a proof of a theorem dealing with a more general type of cyclic field. But the classical theory of abelian fields allows us to name a large number of cyclic fields in which the class-number is greater than 1, and in which therefore E.A. cannot hold. Since these results are difficult to find in the existing literature, they will be quoted and proved in some detail in this paper.

To begin with we recall the two different definitions of the class-number of an algebraic field. H is the number of classes of ideals in an algebraic field if two ideals are considered equivalent provided their quotient is a principal ideal generated by a totally positive number; h is the number of classes of ideals in an algebraic field if two ideals are considered equivalent provided their quotient is any principal ideal. It is clear that $H = h$ for complex abelian fields.

We denote by $w(N)$ the number of distinct rational primes dividing a rational integer $N \neq 0$.

We call a cyclic field K a field of type T_1 if it is the composite field of cyclic fields K_j of degrees k_j and discriminants Δ_j where any two k_j are relatively prime, where any two Δ_j are relatively prime, and where $w(\Delta_j) = 1$.

We call a cyclic field K of degree k a field of type T_2 if it is the composition field of a field K_1 of type T_1 of odd degree, and of a cyclic field K_2 of discriminant Δ_2 of degree 2^l of the following type: $w(\Delta_2) \leqslant k$ and the discriminant of the unique subfield of K_2 of degree 2^{l-1} is a power of a prime, if $l > 1$. (For the purpose of this definition K_1 or K_2 may be the field of rational numbers.) We can now formulate

THEOREM 2. $(k, H) > 1$ *for a cyclic field K not of type T_1.*

THEOREM 3. $h > 1$ *for a cyclic field K not of type T_2.*

Received January 5, 1950.

All results of this paper and of my two previous papers can be summarized as

THEOREM 4. *For each* $k \geqslant 2$ E.A. *holds only in a finite number of cyclic fields* K *of degree* k *and discriminant* Δ, *if only fields of the following types are considered.*

(1) k *a prime.*
(2) $w(k) = 1$, k *odd.*
(3) $w(k) = 1$, K *complex.*
(4) $w(\Delta) = 1$.
(5) $w(\Delta) > w(k)$, k *odd.*
(6) $w(\Delta) > w(k)$, K *complex.*
(7) $w(\Delta) \geqslant k + w(k)$.
(8) $w(\Delta^*) > 1$ *for the discriminant* Δ^* *of every non-rational subfield* K^* *of* K.
(9) k *odd,* K *not of type* T_1.
(10) K *complex and not of type* T_1.
(11) K *not of type* T_2.

Finally I should like to mention two types of cyclic fields for which E.A. may possibly hold in an infinity of cases.

(a) The real quartic field

$$\rho(\sqrt{\tfrac{1}{2}(5 + 5^{\frac{1}{2}})p})$$

of discriminant $125p^2$, where $p \equiv 3 \pmod{20}$ is a prime.

(b) The complex sextic field

$$\rho((e^{2\pi i/9} + e^{-2\pi i/9}),\ (-p)^{\frac{1}{3}})$$

of discriminant -3^8p^3, where $p \equiv 3 \pmod 4$ is a prime.

We establish the following conventions. Small italics except e, i, and o denote positive rational integers, d, p and q denote positive rational primes.

K, K', K_j etc. denote abelian fields of degrees k, k', k_j etc. and discriminants Δ, Δ', Δ_j etc.

Only absolutely abelian fields will be considered in this paper.

2. Dirichlet characters and Abelian fields. Two Dirichlet characters $\chi(n) \pmod m$ and $\chi'(n) \pmod{m'}$ are said to belong to the same train if and only if $\chi(n) = \chi'(n)$ for all n with $(n, mm') = 1$. Then each train contains exactly one primitive character $\chi_0(n) \pmod f$; f is called the conductor of the train, and also the conductor of all characters in the train. The product of two trains is defined in the obvious way, and it is clear that the trains form an infinite abelian group with respect to multiplication.

If $\chi(n)$ is a character mod m and if

$$m = m_1m_2,\ (m_1, m_2) = 1,$$

https://doi.org/10.4153/CJM-1951-029-4 Published online by Cambridge University Press

then $\chi(n)$ can be written in the form

$$\chi(n) = \chi_1(n)\chi_2(n)$$

where $\chi_1(n)$ and $\chi_2(n)$ are uniquely determined characters mod m_1 and m_2 respectively. In particular, if $\chi(n)$ is primitive, then $\chi_1(n)$ and $\chi_2(n)$ are primitive.

The principal results of class-field theory can easily be expressed in the following way.

Between all finite groups $\mathfrak{G}$ of trains and all abelian fields K there is a one-one relation [5, Theorem 1] which satisfies the following conditions:

I. The group $\mathfrak{G}$ is isomorphic to the Galois group of the field K. [5, Theorem 2.]

II. A field K' contains a field K if and only if the corresponding group $\mathfrak{G}'$ contains the corresponding group $\mathfrak{G}$. [5, Theorem 10.]

III. $|\Delta|$ equals the product of the conductors of the trains in $\mathfrak{G}$. [5, Theorem 16.]

IV. $$\zeta_K(s) = \prod_{\chi} L(s, \chi),$$

where $\zeta_K(s)$ denotes the Dedekind ζ-function of K, and where χ runs through the primitive characters of the trains in $\mathfrak{G}$. [5, Theorem 14.]

V. If $\Delta = \pm p^l$, p becomes in K the kth power of a self-conjugate prime ideal of the first order.

VI. If $(\Delta, p) = 1$, p^l is the norm of an integral ideal in K if and only if $\chi(p^l) = 1$ for all primitive characters of the trains in $\mathfrak{G}$.

VII. If $(\Delta, n) = 1$, n is the norm of an integral ideal in K if and only if in the canonical representation

$$n = {p_1}^{l_1} \ldots {p_s}^{l_s}$$

each factor ${p_j}^{l_j}$ is the norm of an integral ideal in K.

VIII. If n is the norm of an integral ideal in K, then $\chi(n) \geqslant 0$ for all characters of the trains in $\mathfrak{G}$.

IX. If K' is an abelian extension of K of relative discriminant 1, then the class-number H of K is divisible by k'/k. More precisely, the class-group of K contains a subgroup whose quotient group is isomorphic to the Galois group of K' over K. [5, Theorems 2 and 16.]

In addition we require two lemmas about discriminants.

LEMMA 1. *If the fields K_1 and K_2 have discriminants Δ_1 and Δ_2 and if $(\Delta_1, \Delta_2) = 1$, then the composition field $K_0 = K_1, K_2$ has discriminant*

$$\Delta_0 = {\Delta_1}^{k_2}{\Delta_2}^{k_1}$$

and degree $k_0 = k_1k_2$. [8, Theorem 88.]

LEMMA 2. *If K' is an abelian extension field over K, then*

$$|\Delta'| = |\Delta|^{k'/k}$$

if and only if K' has relative discriminant 1 over K. [8, Theorem 39.]

3. Proof of Theorem 2. Let $\chi(n)$ be the primitive character in one of the trains which generate the group $\mathfrak{G}$ corresponding to K, so that k is the order of $\chi(n)$. Then we can write

$$\chi(n) = \chi_1(n) \ldots \chi_s(n),$$

where $\chi_1(n), \ldots, \chi_s(n)$ are primitive characters mod $p_1^{l_1}, \ldots, p_s^{l_s}$ respectively, all the p_j being distinct. Let $k_1, \ldots, k_s$ denote the order of $\chi_1(n), \ldots, \chi_s(n)$ respectively; then the smallest common multiple

$$[k_1, \ldots, k_s] = k.$$

Let P_j denote the product of the conductors of the characters

$$\chi_j(n), \chi_j^2(n), \ldots, \chi_j^{k_j-1}(n) \qquad (1 \leqslant j \leqslant s).$$

Then the product of the conductors of the characters

$$\chi(n), \chi^2(n), \ldots, \chi^k(n)$$

equals $\qquad P_1^{k/k_1} \ldots P_s^{k/k_s} = |\Delta|$

by III.

Let us now consider the group $\mathfrak{G}'$ of all trains generated by

$$\chi_1(n), \ldots, \chi_s(n).$$

$\mathfrak{G}'$ contains the train $\chi(n)$, and the order k' of $\mathfrak{G}'$ equals

$$k' = k_1 \ldots k_s.$$

The product of the conductors of all trains in $\mathfrak{G}'$ equals

$$(P_1^{k/k_s} \ldots P_s^{k/k_s})^{k_1 \cdots k_s} = |\Delta^{k'/k}| = |\Delta'|$$

where Δ' is the discriminant of the field K' corresponding to $\mathfrak{G}'$.

It follows by I, II, and Lemma 2 that K' is an extension field of relative discriminant 1 over K. Hence by IX

$$H \equiv 0 \pmod{k'/k}.$$

Hence, if $k' > k$, then $(k, H) > 1$. If $k' = k$, then any two of the numbers $k_1, \ldots, k_s$ are relatively prime, and the field K is of type T_1. This proves Theorem 2.

4. Proof of Theorem 3. We prove first:

LEMMA 3. *If K is complex, then $H = h$. If K is real, then $h > 1$ unless*

https://doi.org/10.4153/CJM-1951-029-4 Published online by Cambridge University Press

the class group of K (in the narrow sense) is the direct product of not more than $k-1$ abelian groups of order 2.

Proof. The first part of the lemma is trivial.

If K is real, then -1 is a non-totally positive unit in K. Therefore the group of all numbers in K, which are products of a unit in K, and of a totally positive number in K, is a subgroup of the group of all numbers ($\neq 0$) in K of index $\leqslant 2^{k-1}$. More precisely, the quotient group is the direct product of at most $k-1$ groups of order 2. Since this quotient group is isomorphic to the quotient group of the two class groups in K, the lemma follows.

Assuming the notation used in the proof of Theorem 2, it suffices by virtue of IX and Lemma 3, to prove that, if the Galois group of K' over K is the direct product of at most $k-1$ groups of order 2, then K is of type T_2.

Let K_0 be the field of largest odd degree k_0 which is contained in K, and let K_e be the field of largest degree $k_e = 2^l$ which is contained in K. Then K_0 and K_e are uniquely determined and we have

$$K = K_0,K_e\ , \quad k = k_0k_e.$$

Let K_ϵ be the unique subfield of K_e of degree $k=\frac{1}{2}k_e$. Then we have to prove

(i) K_0 is of type T_1.

(ii) $w(\Delta_e) \leqslant k$.

(iii) $w(\Delta_\epsilon) = 1$ if $k_\epsilon > 1$.

We construct the extension field K'_0 over K_0 by the same process which gave us the extension field K' over K. If K_0 were not of type T_1, then $k'_0/k_0 > 1$ and odd. Since K'_0 is a subfield of K', we should have

$$(k'/k'_0)\ (k'_0/k_0) = (k'/k)\ (k/k_0),$$

which is a contradiction, because each factor on the right is a power of 2. This proves (i).

Next we construct the extension field K'_e by the same process. Again K'_e is a subfield of K' and we have

$$(k'/k'_e)\ (k'_e/k_e) = (k'/k)\ (k/k_e).$$

Here

$$k/k_e \equiv 1 \pmod 2,\ 2^{k-1} \equiv 0 \pmod{k'/k}.$$

If $w(\Delta_e) > k$, then

$$2^k \equiv 0 \pmod{k'_e/k_e}$$

which gives a contradiction. This proves (ii).

Finally if $k_e \geqslant 4$, $w(\Delta_\epsilon) \geqslant 2$, then the absolute Galois group of K'_e would have a subgroup of type (4, 4) by virtue of I. *A fortiori* the absolute Galois group of K' would have a subgroup of type (4, 4). Since the absolute Galois group of K is cyclic, the Galois group of K' over K would contain an element of order 4, which contradicts our hypothesis. This proves (iii).

https://doi.org/10.4153/CJM-1951-029-4 Published online by Cambridge University Press

5. Conventions and notations. We start by proving

LEMMA 4. *If K is cyclic, $w(\Delta) = 1$, $|\Delta| \geqslant k^{3(k-1)}$, then*

$$|\Delta| = d^{k-1},\ d \equiv 1 \pmod{k}.$$

Proof. Let $\chi(n)$ be the primitive character in one of the trains which generate the group $\mathfrak{G}$ corresponding to K. By I and III $\chi(n)$ is a primitive character mod d^a (say) of order k. Hence

$$k \mid \varphi(d^a) = d^{a-1}(d-1),$$

which means that either $d \mid k$ or $k/d - 1$. In the latter case, if $a > 1$, we should have a number n such that

$$\chi(n) \neq 1,\ n \equiv 1 \pmod{d^{a-1}}.$$

For this value of n

$$n^d \equiv 1 \pmod{d^a},$$
$$1 = \chi(n^d) = \chi^d(n) = \chi(n) \neq 1,$$

which is a contradiction. Hence $\chi(n)$ is a character mod d; $\chi^j(n)$ is *a fortiori* a character mod d for $1 < j < k$, and it follows from III that

$$|\Delta| = d^{k-1}.$$

If d/k, we proceed as follows. We assume that

$$k = d^b m,\ (m, d) = 1.$$

Then, for $d > 2$, the group of all characters mod d^a is cyclic of order $\varphi(d^a)$. Hence the number of characters mod d^a of order k equals $\varphi(k)$ if $k/\varphi(d^a)$ and 0 otherwise. Hence there exists a primitive character mod d^a of order k if and only if

$$\varphi(d^a) \equiv 0 \pmod{k},\ \varphi(d^{a-1}) \not\equiv 0 \pmod{k}.$$

This implies

$$m \mid (d-1),\quad a = b + 1,$$
$$d^a \leqslant dk \leqslant k^2,\ |\Delta| \leqslant k^{2(k-1)}.$$

If $d = 2$, $d \mid k$, the argument is similar. We may assume at once that $a > 3$. Then the group of characters mod d^a is abelian of type $(2, 2^{a-2})$, and the number of characters of order $k = 2^b$ equals 3 if $b = 1$, 2^b if $2 \leqslant b \leqslant a - 2$, 0 if $b > a - 2$.

Hence there exists a primitive character mod 2^a of order k if and only if

$$b = a - 2.$$

This implies

$$d^a = d^2 k \leqslant k^3,\quad |\Delta| \leqslant k^{3(k-1)}.$$

For the rest of the paper excluding the last paragraph we assume $k \geqslant 4$, K cyclic; hence by virtue of Lemma 4

https://doi.org/10.4153/CJM-1951-029-4 Published online by Cambridge University Press

$$d \equiv 1 \pmod{k}, \quad |\Delta| = d^{k-1}.$$

$\chi(n)$ is again the primitive character mod d of order k in a train which generates the group $\mathfrak{G}$ corresponding to K. $\chi(n)$ will now be fixed.

Let A_j denote the class of integers n for which

$$\chi(n) = e^{2\pi ij/k} \qquad (0 \leqslant j \leqslant k-1).$$

Let B denote the subclass of integers b in A_0 for which

$$b = b_1 b_2, \ (b_1, b_2) = 1$$

implies b_1 in A_0. Let C denote the sub-class of integers c in A_0 which can be decomposed in the form

$$c = c_1 c_2, \ (c_1, c_2) = 1, \ \chi(c_1) \neq 1.$$

Clearly every number in A_0 lies either in B or in C. It follows from VI and VII that a number n is norm of an integral ideal in K prime to d if and only if n lies in B.

Also $q_1 < q_2$ are the two smallest primes not in A_0 which do not equal d; and r is the smallest number in C which is prime to q_1 and which satisfies

(1) $$r \equiv -d \pmod{4} \qquad \text{if } q_1 = 2,$$

(2) $$r \equiv -d^2 - 1 \pmod{9} \quad \text{if } q_1 = 3.$$

For $q_1 \geqslant 5$ no additional condition is imposed upon r.

Let ϵ be a positive number which will be fixed later; it may be arbitrarily small. The constants involved in the symbols O and o will depend on k only. Unless the contrary is stated the symbol o will refer to the limit as $d \to \infty$. We put

$$x = [d^{\frac{1}{4}+\epsilon}], \quad y = [d^{\frac{1}{4}+\epsilon}].$$

6. Further lemmas.

LEMMA 5. $\sum_{p \leqslant z} p^{-1} = \log\log z + \gamma + o(1)$ *as* $z \to \infty$, *where* γ *is an absolute constant.* [9, Theorem 7].

LEMMA 6. *For each non-principal character* $\chi(n)$ mod m

$$\sum_{n=1}^{z} \chi(n) = O(m^{\frac{1}{2}} \log m) \qquad [10].$$

LEMMA 7. $q_2 \leqslant y$ *if* d *is sufficiently large.*

Proof. We assume $q_2 > y$. Then all primes $\leqslant y$, with the possible exception of q_1, belong to A_0. Hence, if

$$n \leqslant x, \ (n, q_1) = 1, \ p | n, \ y < p,$$

then $\chi(n) = \chi(p)$ unless n is divisible by the product pp' of two primes in the interval $y < p \leqslant x$, $y < p' \leqslant x$.

Therefore we have for $1 \leqslant j \leqslant k-1$

$$\sum_{\substack{n=1\\(n,\,q_1)=1}}^{x} \chi^j(n) = \sum_{\substack{n=1\\(n,\,q_1)=1}}^{x} 1 + \sum_{\substack{n=1\\(n,\,q_1)=1}}^{x} (\chi^j(n)-1)$$

$$= (1-q_1^{-1})x + O(1) + \sum_{\substack{y<p\leqslant x\\ p\neq q_1}} (\chi^j(p)-1) \sum_{\substack{m\leqslant x/p\\(m,\,q_1)=1}} 1 + \sum_{p>y} \sum_{\substack{p'>y\\ pp'\leqslant x}} O(x/pp')$$

$$= (1-q_1^{-1})x + O(1) + \sum_{y<p\leqslant x} \{(\chi^j(p)-1)(1-q_1^{-1})xp^{-1} + O(1)\}$$

$$+ O(xy^{-1}) + O\Big(x\Big(\sum_{y<p<d^{\frac{1}{4}+2\epsilon}} p^{-1}\Big)^2\Big)$$

$$= (1-q_1^{-1})x\Big\{1 + \sum_{y<p\leqslant x} (\chi^j(p)-1)p^{-1}\Big\} + O(\pi(x))$$

$$+ O\left\{x\left(\log\frac{\frac{1}{4}+2\epsilon}{\frac{1}{4}-2\epsilon} + o(1)\right)^2\right\} \qquad \text{(Lemma 5)}$$

$$= (1-q_1^{-1})x\Big\{1 + \sum_{y<p\leqslant x} (\chi^j(p)-1)p^{-1}\Big\} + O(\epsilon^2 x) + o(x).$$

Applying Lemma 6, this gives, after division by $(1-q_1^{-1})x$,

$$0 = O(\epsilon^2) + o(1) + 1 + \sum_{y<p\leqslant x} (\chi^j(p)-1)p^{-1}.$$

Summing this over $j = 1, \ldots, k-1$ we obtain

$$0 \geqslant O(\epsilon^2) + o(1) + k - 1 - k \sum_{y<p\leqslant x} p^{-1}.$$

Hence

$$\sum_{y<p\leqslant x} p^{-1} \geqslant 1 - k^{-1} + O(\epsilon^2) + o(1).$$

But by Lemma 6

$$\sum_{y\leqslant p\leqslant x} p^{-1} = \log\log x - \log\log y + o(1)$$

$$= \log\frac{\frac{1}{2}+\epsilon}{\frac{1}{4}-\epsilon} + O(1) = \log 2 + O(\epsilon) + o(1).$$

Hence

$$\log 2 \geqslant 1 - k^{-1} + O(\epsilon),$$

which is not true if ϵ is sufficiently small. This proves the lemma.

From now on ϵ is fixed as a function of k.

LEMMA 8. *$q_1 r < d^{1-\epsilon}$, if d is sufficiently large.*

Proof. We assume that d is so large that Lemma 7 applies. If q_2 lies in A_j $(1 \leqslant j \leqslant k-1)$, we choose for u the smallest number in A_{k-j} which satisfies

https://doi.org/10.4153/CJM-1951-029-4 Published online by Cambridge University Press

$$(u, q_1q_2) = 1,$$
$$uq_2 \equiv -d \pmod 4 \text{ if } q_1 = 2,$$
$$uq_2 \equiv -d^2-1 \pmod 9 \text{ if } q_1 = 3.$$

If d is sufficiently large, it is easily deduced from Lemma 6 that

$$u < x.$$

(The detailed argument is explicitly developed in [7].) Since uq_2 lies in C it follows from the definition of r that

$$r \leqslant uq_2 < xq_2,$$

and by Lemma 7 that

$$q_1r < q_1(xq_2) < xq_2^2 \leqslant xy^2 \leqslant d^{1-\epsilon}.$$

LEMMA 9. *If $q_1 \geqslant 5$, $s < q_1$, we can find a prime p_0 such that*

$$(p_0, s) = 1, \ p_0 < q_1, \ p_0 \leqslant \log d$$

provided d is sufficiently large [7, Lemma 4].

LEMMA 10. *For sufficiently large d we can write*

$$d = sr + tq_1,$$

where s in B, $(t, q_1) = 1$.

Proof. We distinguish three cases.

First case. $q_1 = 2$. We have

$$d = r + 2t,$$

and it follows from (1) that t is odd.

Second case. $q_1 = 3$. Then we have with $s = 1$ or $s = 2$

$$d = sr + 3t.$$

Clearly s lies in B, since $q_1 = 3$ is the smallest positive integer not in A_0. If t were divisible by 3, we should have by (2)

$$\begin{aligned} sr &\equiv -s(d^2+1) \equiv d && \pmod 9, \\ (\pm 2s - 1)d &\equiv s(d \pm 1)^2 && \pmod 9, \\ (-4s^2+1)d^2 &\equiv s^2(d^2-1)^2 && \pmod 9, \\ -4s^2 + 1 &\equiv 0 && \pmod 9, \end{aligned}$$

which is not true for $s = 1$ or $s = 2$.

Third case. $q_1 \geqslant 5$. Again, by Lemma 8, we can find s and t such that

$$d = sr + tq_1, \quad s < q_1.$$

Clearly, s lies in B, as it is not divisible by a prime $\geqslant q_1$.

https://doi.org/10.4153/CJM-1951-029-4 Published online by Cambridge University Press

But q_1 may possibly divide t. If $q_1 | t$, we use the prime p_0 of Lemma 9 and denote by n the smallest positive solution of the congruence

$$s + nq_1 \equiv 0 \pmod{p_0}.$$

Then

$$s + nq_1 < q_1 + (p_0 - 1)q_1 = p_0 q_1. \tag{3}$$

We consider the representation

$$d = (s + nq_1)r + (t - nr)q_1.$$

Since $n < q_1$, $t - nr$ is prime to q_1. Since by (3), Lemma 9 and Lemma 8, for sufficiently large d

$$(s + nq_1)r < p_0 q_1 r \leqslant (\log d)d^{1-\epsilon} < d,$$

it follows that

$$t - nr > 0.$$

Finally it follows from (3) and Lemma 9 that no prime $\geqslant q_1$ divides $s + nq_1$. Hence $s + nq_1$ lies in B, and our lemma is proved in all cases.

LEMMA 11. *If d is sufficiently large,*

$$d = c + g,$$

where c lies in C, and g does not lie in B.

Proof. We assume that d is so large that Lemma 10 applies, and put

$$c = sr, \quad g = tq_1.$$

Clearly g does not lie in B, since

$$g = tq_1, \ (t, q_1) = 1, \qquad q_1 \text{ not in } A_0.$$

Since r lies in C, we have a decomposition

$$r = r_1 r_2, \ (r_1, r_2) = 1,$$

where r_1 does not lie in A_0. It follows from the fundamental theorem of arithmetic that we have a decomposition of s such that

$$s = s_1 s_2, \ (s_1, s_2) = 1, \ (r_1, s_2) = (r_2, s_1) = 1.$$

Since s lies in B, s_1 lies in A_0. We have a decomposition

$$c = sr = (s_1 r_1)(s_2 r_2), \ (s_1 r_1, s_2 r_2) = 1,$$

where $s_1 r_1$ does not lie in A_0. Hence c, lying in A_0, lies in C.

7. Proof of Theorem 1. We assume that E.A. holds in K. Then, by condition V, there exists in K a self-conjugate principal prime ideal (δ) of norm d.

We assume that d is so large that Lemma 11 applies. Since c lies in A_0, the congruence

$$n^k \equiv c \pmod{d}$$

has a solution. Since E.A. holds in K, we can find an integer γ in K such that

$$n \equiv \gamma \pmod{\delta}, \quad |N(\gamma)| < |N(\delta)| = d.$$

Since (δ) is self-conjugate, the congruence

$$n \equiv \gamma' \pmod{\delta}$$

holds for each conjugate γ' of γ. Multiplying these k congruences we obtain

$$c \equiv n^k \equiv N(\gamma) \pmod{\delta},$$
$$c \equiv N(\gamma) \pmod{d}.$$

Hence

$$\text{either } N(\gamma) = c \text{ or } N(\gamma) = c - d = -g.$$

This means that the norm of the ideal (γ) equals c or g, which is impossible by Lemma 11 and condition VII.

8. Proof of Theorem 4. We take each individual assertion in Theorem 4, starting from the end.

(11) follows from Theorem 3.

(10) follows from Theorem 2, since $H = h$ if K is complex.

(9) follows from Theorem 3, since for odd k a field of type T_2 is a field of type T_1.

(8) If k is divisible by an odd prime, K_0 is not of type T_1, and therefore K is not of type T_2. If $k = 2^l$, $l \geqslant 2$, the field K_ϵ has discriminant Δ_ϵ with $w(\Delta_\epsilon) > 1$, hence K is not of type T_2. If $k = 2$, the result follows from my first paper [6].

(7) If K were of Type T_2, then

$$w(\Delta_0) \leqslant w(k_0)$$

and

$$w(\Delta_e) \leqslant k \text{ for even } k.$$

Hence

$$w(\Delta) \leqslant w(\Delta_0) + w(\Delta_e) \leqslant \begin{cases} w(k_0) < k + w(k) & \text{for odd } k. \\ w(k_0) + k = k - 1 + w(k) & \text{for even } k. \end{cases}$$

(6) K is not of type T_1, and $h = H > 1$.

(5) Since for odd k a field of type T_2 is a field of Type T_1, K is not of type T_2.

https://doi.org/10.4153/CJM-1951-029-4 Published online by Cambridge University Press

(4) follows from Theorem 1 for $k \geqslant 4$, and from my older results if $k = 2$ or $k = 3$.

(3) follows from (4) and (6).

(2) follows from (4) and (5).

(1) follows from (2) if k is odd, and from my older results if $k = 2$.

References

[1] H. Davenport, *Indefinite binary quadratic forms, and Euclid's Algorithm in real quadratic fields*, Proc. London Math. Soc., in course of publication.

[2] ——— *Indefinite binary quadratic forms*, Quart. J. Math., Oxford Ser. (2), vol. 1 (1950), 54-62.

[3] ——— *Euclid's Algorithm in cubic fields of negative discriminant*, Acta Math., vol. 84 (1950), 159-179.

[4] ——— *Euclid's Algorithm in certain quartic fields*, Trans. Amer. Math. Soc., vol. 68 (1950), 508-532.

[5] H. Hasse, *Bericht über neuere Untersuchungen aus der Theorie der algebraischen Zahlkörper*, Jber. Deutsch. Math. Verein., vol. 35 (1926), 1-55.

[6] H. Heilbronn, *On Euclid's Algorithm in real quadratic fields*, Proc. Cambridge Phil. Soc., vol. 34 (1938), 521-526.

[7] ——— *On Euclid's Algorithm in self-conjugate cubic fields*, Proc. Cambridge Phil. Soc., vol. 46 (1950), 377-382.

[8] D. Hilbert, *Bericht über die Theorie der algebraischen Zahlkörper*, Jber. Deutsch. Math. Verein., vol. 4 (1897), 175-546.

[9] A. E. Ingham, *The distribution of prime numbers* (Cambridge, 1932).

[10] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Nachr. Akad. Wiss. Göttingen, Math. Phys. Kl. 1918, 21-29.

The Royal Fort, Bristol 8