ON THE COMMON INDEX DIVISORS OF AN ALGEBRAIC FIELD*

BY

H. T. ENGSTROM

I. INTRODUCTION

Let d be the discriminant of an algebraic field K generated by a root θ of an irreducible equation

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0 \tag{1}$$

whose coefficients are rational integers. We shall call (1) the characteristic equation for θ. If d_θ is the discriminant of θ then $d_\theta = k_\theta^2 \cdot d$ where k_θ is a rational integer, the index of θ. A divisor common to the indices of every integer of the field has been called by Kronecker a "gemeinsamer ausserwesentlicher Discriminantenteiler" of the field. We shall use the term "common index divisor."†

The existence of common index divisors was first established in 1871 by Dedekind‡ who exhibited examples in fields of third and fourth degrees. Dedekind§ further showed that a rational prime p can be a common index divisor of a field K if and only if at least one of the inequalities $r(f) > g(f)$ holds, where $r(f)$ is the number of prime ideal divisors of p of degree f, and $g(f)$ is the number of different prime functions (mod p) of fth degree. Using Kronecker's theory of algebraic numbers, Hensel‖ has given a necessary and sufficient condition on the so-called "index form" for p to be a common index divisor. In 1907, Bauer¶ showed that if $p < n$ there exists a field of nth degree in which p is a common index divisor. Von Zylinsky** has

* Presented to the Society, December 27, 1928, and March 30, 1929; received by the editors in June, 1929.

† This terminology corresponds to that of Fricke (*Algebra*, vol. 3, Leipzig, 1928) who uses the term "ständiger Indexteiler."

‡ R. Dedekind, Göttinger Gelehrte Anzeigen, 1871, pp. 1481–1494.

§ R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höhere Kongruenzen*, Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen, vol. 23 (1878), pp. 1–23.

‖ K. Hensel, *Arithmetische Untersuchungen über die gemeinsamer ausserwesentlicher Discriminantenteiler einer Gattung*, Journal für Mathematik, vol. 113 (1894), pp. 128–160.

¶ M. Bauer, *Über den ausserwesentlicher Discriminantenteiler algebraischer Körper*, Mathematische Annalen, vol. 64 (1907), p. 573.

** E. von Zylinsky, *Zur Theorie der ausserwesentlicher Discriminantenteiler algebraischer Körper*, Mathematische Annalen, vol. 73 (1913), pp. 273–274.

established the necessity of this condition, i.e., p can be a common index divisor of a field of nth degree only if $p<n$.

This paper is concerned with the problem of determining the greatest power, p^χ, of p which is a common index divisor in a given field and, in particular, how χ is connected with the prime ideal decompositon of p. In a recent paper Professor Ore* makes the conjecture that χ is not in general determined by the prime ideal decomposition of p. The author verifies this conjecture by showing that for degrees eight or higher certain types of prime ideal decomposition may occur in fields for which χ is different. For fields of degree less than eight we show that χ is determined by the prime ideal decomposition of p. Theorems are developed giving this value of χ for all types of prime ideal decomposition which may occur in such fields. Some types of ideal decomposition determine χ even in the field of nth degree. For some of such cases, including the case where all the ideals are of first degree and first order, χ is given by the theorems of this paper.

II. The determination of χ in some general cases

1. Let $f(x)=0$ be the characteristic equation of an integer θ of the field K and suppose $d_\theta = p^\delta \cdot q$ where $(p, q)=1$. If

$$f(x) \equiv f_1(x)\cdot f_2(x)\cdots f_r(x) \pmod{p^\alpha}$$

where $\alpha>\delta+1$, and $f_i(x)$, $i=1, 2, 3, 4$, is irreducible (mod p^α) and of degree n_i, then, by the first theorem of Ore,†

$$[p] = \mathfrak{p}_1^{e_1}\cdot\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r} \tag{2}$$

where $N\mathfrak{p}_i^{e_i}=p^{n_i}$. The field generated by a root $\Theta^{(i)}$ of $f_i(x)=0$ is called the Abbildungskörper of $\mathfrak{p}_i$ and shall be denoted by $K^{(i)}$. Let p^{κ_i} denote the highest power of p contained in the index of $\Theta^{(i)}$ in $K^{(i)}$, and furthermore let $p^{\rho_{ij}}$ be the highest power dividing the resultant $R(f_i(x), f_j(x))$. Then the index of θ is divisible by exactly p^{κ_θ}, where

$$\kappa_\theta = \sum_{i>j}\rho_{ij} + \sum_i \kappa_i. \ddagger \tag{3}$$

In order to find χ for the field K from the prime ideal decomposition (2) it is necessary to determine the values of ρ_{ij} and κ_i for an integer θ of the field

* O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Mathematische Annalen, vol. 99 (1928).

† O. Ore, *Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körper*, Mathematische Annalen, vol. 96 (1926).

‡ O. Ore, loc cit., p. 345.

for which κ_θ takes on the least value. We shall first examine the problem for the simplest case.

2. Consider a field K of nth degree in which

$$[p] = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_n, \tag{4}$$

where $N\mathfrak{p}_i = p$, $i = 1, 2, \cdots, n$. If $f(x) = 0$ is the characteristic equation of an arbitrary integer θ in K, then

$$f(x) \equiv (x + a_1)(x + a_2) \cdots (x + a_n) \pmod{p^\alpha} \tag{5}$$

for α sufficiently great. It is seen that $\kappa_i = 0$, $i = 1, 2, \cdots, n$. Furthermore $R(f_i(x), f_j(x)) = a_i - a_j$. Hence k_θ is divisible by the same power of p as

$$\prod_{i>j}(a_i - a_j). \tag{6}$$

To determine χ for the field K we seek a set of rational integers $a_1, a_2, \cdots, a_n$ which correspond to an integer of the field by (5) and such that (6) contains the least possible power of p. We shall make use of the following theorem:

THEOREM 1. *Let $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_s$ be any distinct prime ideal divisors of p in K and let $\phi_1(x), \phi_2(x), \cdots, \phi_s(x)$ be a set of prime functions, not necessarily distinct, of degrees $m_1, m_2, \cdots, m_s$ where m_i divides the degree f_i of $\mathfrak{p}_i$. Then there exists a primitive integer θ in K such that $\phi_i(\theta)$ contains exactly $\mathfrak{p}_i^{h_i}$, $i = 1, 2, \cdots, s$, where $h_1, h_2, \cdots, h_s$ is an arbitrary set of positive rational integers.*

For an arbitrary prime ideal $\mathfrak{p}$ of degree f dividing p, every integer ω of K satisfies the congruence

$$\omega^{p^f} - \omega \equiv 0 \pmod{\mathfrak{p}}$$

which has, therefore, as many roots as its degree p^f. On the other hand, the polynomial $x^{p^f} - x$ is congruent (mod p) to the product of all prime functions (mod p) whose degrees are divisors of f. It follows that

$$\phi_1(x) \equiv (x - \omega_1)(x - \omega_2) \cdots (x - \omega_{m_1}) \pmod{\mathfrak{p}_1}$$

where $\omega_1, \omega_2, \cdots, \omega_{m_1}$ are integers in K. By a generalization of a theorem of Schönemann* we have

$$\phi_1(x) \equiv (x - \mu_1)(x - \mu_2) \cdots (x - \mu_{m_1}) \pmod{\mathfrak{p}_1^{h_1}}$$

where $\mu_1, \mu_2, \cdots, \mu_{m_1}$ are also integers in K. Hence there exists an integer

* Th. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, Journal für Mathematik, vol. 32 (1846), pp. 93–95.

θ_1 in K such that $\phi_1(\theta_1) \equiv 0 \pmod{\mathfrak{p}_1^{h_1}}$. We may suppose θ_1 chosen so that $\phi_1(\theta_1)$ is divisible by exactly $\mathfrak{p}_1^{h_1}$, for suppose $\phi_1(\theta_1)$ were divisible by $\mathfrak{p}_1^{\beta}$, $\beta > h_1$. Then if π is an integer in K containing exactly $\mathfrak{p}_1^1$ and we set $\theta_1' = \theta_1 + \pi^{h_1}$, we have

$$\phi_1(\theta_1') = \phi_1(\theta_1 + \pi^{h_1}) = \phi_1(\theta_1) + \pi^{h_1} \cdot \phi_1'(\theta_1) + \cdots + \frac{\pi^{mh_1}}{m!}\phi_1^{(m)}(\theta_1).$$

Since $\phi_1'(\theta_1) \not\equiv 0 \pmod{\mathfrak{p}_1}$, it follows that $\phi_1(\theta_1')$ is divisible by exactly $\mathfrak{p}_1^{h_1}$.

Similarly we may determine integers $\theta_2, \theta_3, \cdots, \theta_s$ so that $\phi_i(\theta_i)$ is divisible by exactly $\mathfrak{p}_i^{h_i}$, $i = 1, 2, \cdots, s$, and hence if θ is chosen so that

$$\theta \equiv \theta_i \pmod{\mathfrak{p}_i^{h_i+1}} \qquad (i = 1, 2, \cdots, s),$$

it follows that $\phi_i(\theta)$ is divisible by exactly $\mathfrak{p}_i^{h_i}$, $i = 1, 2, \cdots, s$. Furthermore θ may be supposed primitive, for if it were not primitive let

$$\theta' = \theta + p^{h+1} \cdot r \cdot \Theta \qquad (h > h_i, i = 1, 2, \cdots, s),$$

where Θ is a primitive integer and r is a rational integer. It is seen that r can be chosen so that θ' is primitive while $\phi_i(\theta')$ contains exactly $\mathfrak{p}_i^{h_i}$, $i = 1, 2, \cdots, s$. Hence Theorem 1 is proved. From Theorem 1 we have the following Theorem:

THEOREM 2. *If $a_1, a_2, \cdots, a_n$ is an arbitrary set of n rational integers, then there exists an integer θ in K for which $f(x)$ has the decomposition* (5) *for some α.*

For by Theorem 1 we may choose θ so that $\theta + a_i \equiv 0 \pmod{\mathfrak{p}_i^{\beta}}$, $i = 1, 2, \cdots, n$. Suppose

$$f(x) \equiv (x + b_1)(x + b_2) \cdots (x + b_n) \pmod{p^{\alpha}}.$$

Then $\theta + b_i \equiv 0 \pmod{\mathfrak{p}_i^{\alpha - \rho'}}$ where α may be chosen so large that $\alpha - \rho' > \beta$. Hence $\theta + a_i \equiv \theta + b_i \pmod{\mathfrak{p}_i^{\beta}}$ and $a_i \equiv b_i \pmod{p^{\beta}}$ and Theorem 2 follows. If the a's are all distinct and β is chosen so that they are distinct (mod p^{β}) then

$$f(x) \equiv (x + a_1)(x + a_2) \cdots (x + a_n) \pmod{p^{\beta}}$$

where $\beta > \delta$.

To determine θ so that (6) contains the least power of p we make use of the following theorem due to Hensel.*

The discriminant $\prod_{i \neq k} (a_i - a_k)$ of n arbitrary rational integers is divisible by the discriminant $D_n = \prod_{i \neq j} (i - j)$ of the first n positive rational integers.

Hence, for a field in which p has the decomposition (4), D_n contains exactly p^{χ}. The following theorem is obtained by simple calculation.

* K. Hensel, *Über den grössten gemeinsamen Teiler aller Zahlen welche durch ein ganze Funktion von n Veränderlichen darstellbar sind*, Journal für Mathematik, vol. 116 (1896), p. 352.

THEOREM 3. *If K is an algebraic field of nth degree in which*

$$[p] = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_n, \quad N\mathfrak{p}_i = p,$$

then

$$\chi = \sum_{i=1} s_i \left\{ n - p^i \left(\frac{s_i + 1}{2} \right) \right\}, \quad s_i = \left[\frac{n}{p^i} \right].$$

3. We shall extend this result to a more general type of prime ideal decomposition. Suppose $\mathfrak{p}_i$ is a prime ideal of order e_i and degree f_i dividing p, and $\phi(x)$ is a prime function (mod p) of degree f_i. We may determine a primitive integer θ in K such that $\phi(\theta)$ is divisible by exactly $\mathfrak{p}_i^1$. If $f_i(x)$ is the factor (mod p^α) corresponding to $\mathfrak{p}_i$ of the characteristic equation for θ, then the Newton polygon $(p, \phi(x))$ of $f_i(x)$ is a straight line with slope $1/e_i$.* Since $f_i(x)$ must be of degree $e_i f_i$ we have

$$f_i(x) = \phi(x)^{e_i} + p \cdot M(x), \tag{7}$$

where $M(x) \not\equiv 0$ (modd $p, \phi(x)$). After Ore, we call the form (7) the "normal form." It follows by the theorem of Dedekind that if the factor corresponding to an ideal $\mathfrak{p}_i$ is normal then $\kappa_i = 0$. If the prime ideal decomposition of p is such that $g(f_i) < r(f_i)$ for $f_i \neq 1$, it follows that we may choose θ so that $\kappa_i = 0$ for $f_i \neq 1$. Furthermore, if $f_i \neq 1$, $R(f_i(x), f_j(x)) \not\equiv 0$ (mod p), i.e. $\rho_{ij} = 0$. Hence we have the following theorem:

THEOREM 4. *Let K be an algebraic field of nth degree in which*

$$[p] = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_s^{e_s}, \quad N\mathfrak{p}_i = p^{f_i}.$$

If $g(f_i) < r(f_i)$ for $f_i \neq 1$, and $e_i = 1$ for $f_i = 1$, then

$$\chi = \sum_i s_i \left\{ r - p^i \left(\frac{s_i + 1}{2} \right) \right\}, \quad s_i = \left[\frac{r}{p^i} \right],$$

where r is the number of first degree prime ideals dividing p.

4. If the degree of the field is less than eight, Theorem 4 can be extended to the case where some of the first degree ideals are of higher order. We shall say that a prime ideal $\mathfrak{p}$ of fth degree dividing p is associated with a prime function $\phi(x)$ (mod p), whose degree is a divisor of f, for the integer θ if $\mathfrak{p}$ divides $\phi(\theta)$. It follows from Theorem 1 that an integer θ can be found in any field with any given association of the prime ideal divisors of p. We shall

* O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Mathematische Annalen, vol. 99 (1928), p. 100.

use the notation $\mathfrak{p}^a \mid \phi(\theta)$ to indicate that $\phi(\theta)$ is divisible by exactly the ath power of $\mathfrak{p}$. Let

$$\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_t \tag{8}$$

be the prime ideals dividing p for which $f_i = 1$ and $e_i > 1$, and let

$$\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_r \tag{9}$$

be those of first order and first degree. Suppose further that $g(f_i) \geqq r(f_i)$ for $f_i \neq 1$. If the ideals (8) are each associated with a distinct prime function of first degree for an integer θ whose index contains exactly p^χ, then χ may be determined from the prime ideal decomposition. We shall show that this association can be assumed for θ in a field of degree less than eight if $t \leqq p$.

Suppose that $t \leqq p$ and that at least two of the ideals (8), say $\mathfrak{p}_1$ and $\mathfrak{p}_2$, must necessarily be associated with a single prime function, say x, for an integer θ whose index is divisible by exactly p^χ. Then there must exist at least $p-t+1$ prime functions, say

$$x + 1, x + 2, \cdots, x + p - t + 1,$$

with which none of the ideals (8) are associated for θ. Suppose that n_i of the ideals (9) divide $\theta + i$, $i = 1, 2, \cdots, p+t-1$. If $f_i(x)$ is the factor (mod p^α) of $f(x)$ corresponding to $\mathfrak{p}_i$, we have, from the Newton polygon,

$$f_i(x) = x^{e_i} + pM_i(x), \quad i = 1, 2.$$

Hence $\rho_{12} \geqq 2$.

Consider the value of κ for another integer θ_1 in K for which $\mathfrak{p}_1^1 \mid \theta_1 + 1$ while the other associations remain the same as for θ. Let $f_1^{(1)}(x)$ be the factor (mod p^α) of the characteristic equation of θ_1 which corresponds to $\mathfrak{p}_1$. Then

$$f_1^{(1)}(x) = (x + 1)^{e_1} + p \cdot B, \quad B \not\equiv 0 \pmod{p}.$$

Hence for θ_1 we have $\kappa_1 + \sum \rho_{1j} = n_1$. It follows from our assumption that the value of κ for θ_1 must exceed χ, i.e.

$$n_1 > 2. \tag{10}$$

Similarly, $n_i > 2$ for $i = 1, 2, \cdots, p-t+1$. Hence if n is the degree of the field, we have

$$n \geqq 3(p - t + 1) + 2t. \tag{11}$$

It follows that $n \geqq 7$, i.e., if $t \leqq p$ and $n \leqq 7$ the index of some integer θ for which the ideals (8) are associated with distinct prime functions is divisible by exactly p^χ.

This result is true for $n=7$. To establish this suppose first that $t\geqq 3$. It follows from (11) that $n\geqq 9$. In the second place if $t=2$ and $p>2$ from (11) we have $n\geqq 10$. We have yet to consider the case where $t=2$ and $p=2$. In the field of seventh degree this becomes the case where

$$[2] = \mathfrak{p}_1^2\cdot\mathfrak{p}_2^2\cdot\mathfrak{p}_3\cdot\mathfrak{p}_4\cdot\mathfrak{p}_5, \quad N\mathfrak{p}_i = 2. \tag{12}$$

Let us assume as above that χ must necessarily occur for an integer θ in K for which both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are associated with a single prime function, say x. From (10) it follows that the other ideals $\mathfrak{p}_3$, $\mathfrak{p}_4$, $\mathfrak{p}_5$ must be associated with $x+1$ for θ. Suppose $\mathfrak{p}_1^a\cdot\mathfrak{p}_2^b \mid \theta$. Then

$$f(x) \equiv f_1(x)f_2(x)\cdots f_5(x) \pmod{2^\alpha},$$

where

$$\begin{aligned} f_1(x) &= x^2 + 2k_1x + 2^a m_1, & (m_1,2) &= 1, \\ f_2(x) &= x^2 + 2k_2x + 2^b m_2, & (m_2,2) &= 1. \end{aligned} \tag{13}$$

We shall make use of the following lemma:

LEMMA 1. *If $f_1(x)$ and $f_2(x)$ have the form* (13), *then* $\min(\kappa_1+\kappa_2+\rho_{12})=3$.

For we have

$$R(f_1(x),\ f_2(x)) = -(2^a m_1 - 2^b m_2)^2 + 2(k_2-k_1)(k_1 2^b m_2 - k_2 2^a m_1). \tag{14}$$

If $a\geqq 2$ and $b\geqq 2$, it follows that $\rho_{12}\geqq 3$. If $a=1$ and $b>1$ we have from (14) that $\rho_{12}=2$. Furthermore $\Theta^{(2)}/2$ is an integer in the Abbildungskörper $K^{(2)}$ since it satisfies the equation

$$x^2 + k_2x + 2^{b-2}m_2 = 0.$$

Hence $\kappa_2\geqq 1$, i.e., $\kappa_1+\kappa_2+\rho_{12}\geqq 3$. The similar result follows if $a>1$, $b=1$. If $a=1$ and $b=1$ we have from (14) that $\rho_{12}\geqq 3$. We have thus shown that $\min(\kappa_1+\kappa_2+\rho_{12})\geqq 3$.

It remains to show that there exists an integer θ in the field for which $\kappa_1+\kappa_2+\rho_{12}=3$. By choosing $a=1$ and $b=3$ we have $\rho_{12}=2$ and furthermore $\kappa_1=0$ since $f_1(x)$ is in the normal form. It is also seen that $\Theta^{(2)}/2$ satisfies an equation which has the normal form and hence $\kappa_2=1$. For this choice of θ, $\kappa_1+\kappa_2+\rho_{12}=3$ and the lemma follows.

Returning to our argument we shall show that the assumption that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in (12) must be associated with the same prime function for the θ whose index contains exactly 2^χ leads to a contradiction. For if an integer θ_1 is chosen so that $\mathfrak{p}_2^1 \mid \theta_1+1$ while the other associations are the same as for θ, we would have

$$\kappa_2 + \sum_i \rho_{2i} = 3,$$

the other terms in (3) remaining the same as for θ. We have thus shown that in a field of degree less than eight, $t \leqq p$, the index of some integer for which each of the ideals (8) is associated with a distinct prime function contains exactly p^x.

It follows that the required integer is such that the ideals (9) are associated with prime functions as in Theorem 4 while each of the ideals (8) is associated with a distinct prime function, first exhausting the prime functions with which the smaller number of ideals (9) is associated. The following theorem is obtained by simple calculation.

THEOREM 5. *If K is an algebraic field of degree $n<8$ in which*

$$[p] = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_s^{e_s}, \quad N\mathfrak{p}_i = p^{f_i},$$

where $g(f_i) > r(f_i)$ for $f_i \neq 1$, and $e_i = 1$ for $f_i = 1$ except for t ideals, $t \leqq p$, then

$$\chi = t(s_1 + 1) - \min(t, p - r + ps_1) + \sum_i s_i \left\{ r - p^i \left(\frac{s_i + 1}{2} \right) \right\}, \quad s_i = \left[\frac{r}{p^i} \right],$$

where r is the number of first degree, first order prime ideals dividing p.

If $t=1$ it follows immediately that the above result is valid for a field of nth degree and we have the following corollary:

COROLLARY. *If K is a field of nth degree in which $t=1$ and the other conditions of Theorem 5 are satisfied, then*

$$\chi = s_1 + \sum_i s_i \left\{ r - p \left(\frac{s_i + 1}{2} \right) \right\}. \tag{15}$$

5. We shall now consider certain types of ideal decomposition of the prime 2 for which χ may be determined. Let K be a field of nth degree in which

$$[2] = \mathfrak{p}_1^a \cdot \mathfrak{p}_2^b \cdot \mathfrak{p}_3^2, \quad N\mathfrak{p}_i = 2,$$

and $a \geqq b \geqq 2$. Choose an integer θ so that $\mathfrak{p}_1^1 \mathfrak{p}_3^c \mid \theta$ and $\mathfrak{p}_2 \mid \theta + 1$. Then the characteristic equation of θ has the decomposition

$$f(x) \equiv f_1(x) f_2(x) f_3(x) \pmod{2^a},$$

where

$$f_1(x) = x^a + 2k_1 x^{a-1} + \cdots + 2m_1, \quad (m_1, 2) = 1,$$
$$f_2(x) = (x+1)^b + 2l_1(x+1)^{b-1} + \cdots + 2m_2, \quad (m_2, 2) = 1,$$
$$f_3(x) = x^2 + 2n_1 x + 2^c m_3, \quad (m_3, 2) = 1.$$

If $a=2$, it follows from Lemma 1 that min $(\rho_{13}+\kappa_1+\kappa_3)=3$ for integers of K for which $\mathfrak{p}_1$ and $\mathfrak{p}_3$ are associated with x. For the θ chosen above we have $\kappa_1=\kappa_2=\rho_{12}=0$, and furthermore, as in Lemma 1, if we choose $c=3$ it follows that $\kappa_3=1$ and $\rho_{13}=2$. Hence, if $a=2$, we have $\chi=3$.

Consider the case where $a>2$. Since $R_{ij}=N^{(i)}(f_j(\Theta^{(i)}))$, where $N^{(i)}$ indicates the norm taken in the Abbildungskörper $K^{(i)}$, it follows that $\rho_{ij}\geqq 2$ for the two ideals $\mathfrak{p}_i$ and $\mathfrak{p}_j$ which are associated with the same prime function. Hence we have min $(\rho_{13}+\kappa_1+\kappa_3)\geqq 2$. But if $c=1$, we have

$$R_{13} = N^{(3)}(\Theta^{(3)a} + 2k_1\Theta^{(3)a-1} + \cdots + 2m_1) \tag{16}$$

where

$$\Theta^{(3)2} + 2n_1\Theta^{(3)} + 2m_3 = 0. \tag{17}$$

From (17) it follows that $\mathfrak{p}_3^1 \mid \Theta^{(3)}$. Hence from (16) we have $\mathfrak{p}_3^4 \mid R_{13}$, i.e. $\rho_{13}=2$. Furthermore $\kappa_1=\kappa_2=\kappa_3=\rho_{12}=\rho_{23}=0$. Hence for this choice of θ we have $\kappa=2$ and we conclude that $\chi=2$ for $a>2$.

This result may be extended to the ideal decomposition

$$[2] = \mathfrak{p}_1^a \cdot \mathfrak{p}_2^b \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4, \quad N\mathfrak{p}_i = 2, \quad a \geqq b \geqq 2.$$

If θ is chosen so that $\mathfrak{p}_1^1\mathfrak{p}_3^3 \mid \theta$ and $\mathfrak{p}_2^1\mathfrak{p}_4^1 \mid \theta+1$ it is seen as above that $2^\chi \mid k\theta$, i.e., $\chi=3$ or 4 according as $a>2$ or $a=2$. Similarly for the field in which

$$[2] = \mathfrak{p}_1^a \cdot \mathfrak{p}_2^b \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4 \cdot \mathfrak{p}_5, \quad N\mathfrak{p}_i = 2, \quad a \geqq b \geqq 2,$$

we choose θ so that $\mathfrak{p}_1^1\mathfrak{p}_3^3 \mid \theta$ and $\mathfrak{p}_2^1 \cdot \mathfrak{p}_4^1 \cdot \mathfrak{p}_5^2 \mid \theta+1$ and obtain $\chi=5$ or 6 according as $a>2$ or $a=2$. These results may be combined in the following theorem:

THEOREM 6. *If K is a field of nth degree in which*

$$[2] = \mathfrak{p}_1^a \cdot \mathfrak{p}_2^b \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4^c \cdot \mathfrak{p}_5^d, \quad N\mathfrak{p}_i = 2,$$

where $a\geqq b\geqq 2>c\geqq d$, then $\chi=2+c+2d$ or $3+c+2d$ according as $a>2$ or $a=2$.

This theorem is also true in fields in which [2] contains prime ideals of degree greater than one, provided that $r(f)\leqq g(f)$ for $f\neq 1$.

6. Consider a field in which

$$[2] = \mathfrak{p}_1^{(2)a} \cdot \mathfrak{p}_2^{(2)} \cdot \mathfrak{p}_3^b \cdot \mathfrak{p}_4 \cdot \mathfrak{p}_5 \cdots \mathfrak{p}_s$$

where $N\mathfrak{p}_1^{(2)} = N\mathfrak{p}_2^{(2)} = 2^2$; $N\mathfrak{p}_i = 2$ for $i > 2$. It is easily shown that $\phi(x) = x^2 + x + 1$ is the only prime function (mod 2) of second degree. Suppose an integer θ is chosen so that $\mathfrak{p}_1^{(2)^1} \cdot \mathfrak{p}_2^{(2)^2} \mid \phi(\theta)$. Then if $f_1(x)$ and $f_2(x)$ are the factors (mod 2^α) of the characteristic equation of θ which correspond to $\mathfrak{p}_1^{(2)}$ and $\mathfrak{p}_2^{(2)}$, we have

$$f_1(x) = \phi(x)^a + Q_1(x)2^{\beta_1}\phi(x)^{a-1} + \cdots + 2Q_a(x),$$
$$f_2(x) = \phi(x) + 2^2 R(x),$$

where $Q_i(x) \not\equiv 0$ (modd 2, $\phi(x)$) and $R(x) \not\equiv 0$ (modd 2, $\phi(x)$). It follows that $\kappa_1 = \kappa_2 = 0$ and $\rho_{12} = 2$. If $\mathfrak{p}_1^{(2)}$ and $\mathfrak{p}_2^{(2)}$ are not associated with first degree prime functions it follows from the corollary to Theorem 5 that κ is least for the integer θ for which the ideals $\mathfrak{p}_4, \mathfrak{p}_5, \cdots, \mathfrak{p}_s$ are associated as in that theorem. Hence the least value of κ for an integer so chosen is $2+T$ where T is the expression (15). If, on the other hand, θ is chosen so that one of the ideals $\mathfrak{p}_1^{(2)}$, $\mathfrak{p}_2^{(2)}$, say $\mathfrak{p}_1^{(2)}$, is associated with a first degree prime function, say x, then

$$f_1(x) = x^{2a} + 2q_1 x^{2a-1} + \cdots + 2^2 q_{2a},$$

which is not in the normal form and hence $\kappa_1 \geqq 1$. But if $s \geqq 4$ the association of Theorem 5 has at least one of the ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_s$ associated with x and hence $\sum_j \rho_{ij} \geqq 2$. Furthermore, any significant change of association of the ideals $\mathfrak{p}_3, \mathfrak{p}_4, \cdots, \mathfrak{p}_s$ would increase κ by at least one and, since $\kappa_1 \geqq 1$, we would have $\kappa \geqq 2+T$. It follows that if $s \geqq 4$, $\chi = 2+T$ where T is the expression (15).

If $s < 4$, let us determine θ so that $\mathfrak{p}_1^{1} \mid \theta^2+\theta+1$, $\mathfrak{p}_2^{1} \mid \theta$, and $\mathfrak{p}_3^{1} \mid \theta+1$. Then

$$f_1(x) = \phi(x)^a + 2^{\beta_1}Q_1(x)\phi(x)^{a-1} + \cdots + 2Q_a(x),\ Q_i(x) \not\equiv 0 \ (\text{modd } 2, \phi(x));$$
$$(18)\quad f_2(x) = x^2 + 2kx + 4m, \quad (m,2) = 1;$$
$$f_3(x) = (x+1)^b + 2M(x), \quad M(x) \not\equiv 0 \qquad (\text{modd } 2, x+1).$$

We may further suppose that θ satisfies the congruence*

$$(19)\qquad \theta \equiv 2\omega \qquad (\text{mod } \mathfrak{p}_2^{(2)^\alpha})$$

where

$$(20)\qquad \omega^2 + \omega + 1 \equiv 0 \qquad (\text{mod } \mathfrak{p}_2^{(2)^\alpha}).$$

* O. Ore, *Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern*, Mathematische Annalen, vol. 97 (1927), p. 576.

From (19) and (20) we have $\theta^2+2\theta+4\equiv 0 \pmod{\mathfrak{p}_2^{\alpha}}$. But from (18) $\theta^2+2k\theta+4m\equiv 0 \pmod{\mathfrak{p}_2^{(2)\alpha-\rho}}$ where we may assume $\alpha-\rho>2$. It follows that $2(k-1)\theta\equiv 4(1-m) \pmod{\mathfrak{p}_2^{\alpha-\rho}}$, and hence k must be odd. The integer $\Theta^{(2)}/2$ in the Abbildungskörper $K^{(2)}$ satisfies the equation $x^2+kx+m=0$, which, since k is odd, has the normal form $x^2+x+1+2M(x)=0$. Hence $\kappa_2=1$ and, since $\kappa_1=\kappa_3=\rho_{1j}=0$, $\chi=1$. We thus have the following theorem:

THEOREM 7. *In a field of nth degree in which*

$$[2] = \mathfrak{p}_1^{(2)^a}\cdot\mathfrak{p}_2^{(2)}\cdot\mathfrak{p}_3^{b}\cdot\mathfrak{p}_4\cdots\mathfrak{p}_s,$$

$$N\mathfrak{p}_1 = N\mathfrak{p}_2 = 2^2; \quad N\mathfrak{p}_i = 2,\ i>2,$$

we have

$$\chi = 2 + s_1 + \sum_{i=1} s_1\left\{r - 2^i\left(\frac{s_i+1}{2}\right)\right\} \text{ or } \chi = 1$$

according as $s\geqq 4$ *or* $2\leqq s<4$.

7. As a last case consider a field in which

$$[2] = \mathfrak{p}_1^{(2)}\cdot\mathfrak{p}_2^{(2)}\cdot\mathfrak{p}_3^{(2)}\cdot\mathfrak{p}_4^{a},$$

$$N\mathfrak{p}_i = 2^2,\ i = 1,2,3;\ N\mathfrak{p}_4 = 2.$$

If $a=0$ choose θ so that $\mathfrak{p}_1^{(2)^1}|\theta^2+\theta+1$, $\mathfrak{p}_2^{(2)^1}|\theta$ and $\mathfrak{p}_3^{(2)^1}|\theta+1$. As above, $\rho_{ij}=0$ and $\kappa_2=\kappa_3=1$. It is seen that the index of θ contains exactly 2^x since any other association leads to a larger κ, i.e. $\chi=2$. Similarly, if $a\neq 0$, by choosing θ so that $\mathfrak{p}_1\cdot\mathfrak{p}_2^2|\theta^2+\theta+1$, $\mathfrak{p}_3|\theta$ and $\mathfrak{p}_4|\theta+1$, we see that $\chi=3$. Hence we have the following theorem:

THEOREM 8. *If K is a field of nth degree in which*

$$[2] = \mathfrak{p}_1^{(2)}\cdot\mathfrak{p}_2^{(2)}\cdot\mathfrak{p}_3^{(2)}\cdot\mathfrak{p}_4^{a},$$

$$N\mathfrak{p}_i = 2^2,\ i = 1,2,3;\ N\mathfrak{p}_4 = 2;$$

then $\chi=2$ *or* 3 *according as* $a=0$ *or* $a\neq 0$.

8. The theorem of von Zylinsky and the criterion of Dedekind are sufficient for determining which rational primes are common index divisors in a field from the prime ideal decompositions. The theorems of this paper are sufficient for calculating the powers of these primes contained in the greatest common index divisor of any field of degree less than eight. The following table gives the results of these calculations.

POWERS OF RATIONAL PRIMES CONTAINED IN THE GREATEST COMMON INDEX DIVISOR OF AN ALGEBRAIC FIELD

$[p] = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$, $N\mathfrak{p}_i = p^{f_i}$

Degree of Field	Prime Ideal Decomposition $[f_1, f_2, f_3, \cdots]$	$[e_1, e_2, e_3, \cdots]$	Prime 2	3	5
			x	x	x
3	[1 1 1]	[1 1 1]	1		
4	[1 1 1 1]	[1 1 1 1]	2	1	
	[1 1 1]	[2 1 1]	1		
	[2 2]	[1 1]	1		
5	[1 1 1 1 1]	[1 1 1 1 1]	5	2	
	[1 1 1 1]	[2 1 1 1]	2	1	
	[1 1 1]	[2 2 1]	1		
	[1 1 1]	[3 1 1]	1		
	[2 1 1 1]	[1 1 1 1]	1		
	[2 2 1]	[1 1 1]	1		
6	[1 1 1 1 1 1]	[1 1 1 1 1 1]	8	3	1
	[1 1 1 1 1]	[2 1 1 1 1]	4	2	
	[1 1 1]	[2 2 2]	3		
	[1 1 1 1]	[2 2 1 1]	2	1	
	[1 1 1 1]	[3 1 1 1]	2	1	
	[2 1 1 1 1]	[1 1 1 1 1]	2	1	
	[2 2 1 1]	[1 1 1 1]	2		
	[2 2 2]	[1 1 1]	2		
	[1 1 1]	[3 2 1]	1		
	[2 1 1 1]	[1 2 1 1]	1		
	[2 2 1]	[1 1 2]	1		
	[2 2]	[2 1]	1		
	[3 1 1 1]	[1 1 1 1]	1		

Degree of Field	Prime Ideal Decomposition $[f_1, f_2, f_3, \cdots]$	$[e_1, e_2, e_3, \cdots]$	Prime 2 χ	3 χ	5 χ
7	[1 1 1 1 1 1 1]	[1 1 1 1 1 1 1]	12	4	2
	[1 1 1 1 1 1]	[2 1 1 1 1 1]	7	3	1
	[2 1 1 1 1 1]	[1 1 1 1 1 1]	5	2	
	[1 1 1 1 1]	[2 2 1 1 1]	4	2	
	[1 1 1 1 1]	[3 1 1 1 1]	4	2	
	[1 1 1 1]	[2 2 2 1]	4	1	
	[2 2 1 1 1]	[1 1 1 1 1]	3		
	[2 2 2 1]	[1 1 1 1]	3		
	[1 1 1 1]	[3 2 1 1]	2	1	
	[1 1 1]	[3 2 2]	2		
	[1 1 1 1]	[4 1 1 1]	2	1	
	[2 1 1 1 1]	[1 2 1 1 1]	2	1	
	[2 2 1 1]	[1 1 2 1]	2		
	[3 1 1 1 1]	[1 1 1 1 1]	2	1	
	[1 1 1]	[3 3 1]	1		
	[1 1 1]	[4 2 1]	1		
	[2 1 1 1]	[1 2 2 1]	1		
	[2 1 1 1]	[1 3 1 1]	1		
	[2 1 1 1]	[2 1 1 1]	1		
	[2 2 1]	[1 2 1]	1		
	[2 2 1]	[1 1 3]	1		
	[3 1 1 1]	[1 2 1 1]	1		
	[3 2 2]	[1 1 1]	1		
	[4 1 1 1]	[1 1 1 1]	1		

III. An example showing that χ is not determined by the prime ideal decomposition in the general case

Consider a field K of eighth degree in which

$$[3] = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4^2, \quad N\mathfrak{p}_i = 3. \tag{21}$$

Let θ be an integer in K chosen so that

$$\mathfrak{p}_1^1 \mathfrak{p}_2^1 \mid \theta, \quad \mathfrak{p}_3^1 \mid \theta + 1, \quad \mathfrak{p}_4^1 \mid \theta + 2. \tag{22}$$

If $f(x) = 0$ is the characteristic equation for θ, then

$$f(x) \equiv f_1(x) f_2(x) f_3(x) f_4(x) \pmod{3^a},$$

where, from the Newton polygons,

$$
\begin{aligned}
f_1(x) &= x^2 + 3k_1x + 3m_1, \\
f_2(x) &= x^2 + 3k_2x + 3m_2, \\
f_3(x) &= (x+1)^2 + 3k_3(x+1) + 3m_3, \\
f_4(x) &= (x+2)^2 + 3k_4(x+1) + 3m_4,
\end{aligned} \tag{23}
$$

and $(m_i, 3)=1$. Then $\rho_{i3}=\rho_{i4}=\kappa_i=0$, $i=1, 2, 3, 4$. To calculate κ_θ we need only calculate ρ_{12}. We have

$$R(f_1(x), f_2(x)) \equiv -9(m_2-m_1)^2 \pmod{3^3}, \tag{24}$$

and therefore $\rho_{12}=2$ or $\rho_{12}>2$ according as $m_1 \not\equiv m_2 \pmod 3$ or $m_1 \equiv m_2 \pmod 3$.

We shall show that $m_1 \pmod 3$ is independent of the choice of θ satisfying (22). Since θ is a prime with respect to $\mathfrak{p}_1$, any integer θ' of K satisfies a congruence

$$\theta' \equiv a + b\theta \pmod{\mathfrak{p}_1^{3^a}} \tag{25}$$

where a and b are rational integers. If θ' satisfies (22) we must have $a\equiv 0 \pmod{\mathfrak{p}_1}$ and $b\not\equiv 0 \pmod{\mathfrak{p}_1}$, i.e., $a\equiv 0 \pmod 3$ and $b\not\equiv 0 \pmod 3$. Let $f_1^{(1)}(x)$ be the factor corresponding to $\mathfrak{p}_1$ in the decomposition (mod 3) of the characteristic equation of θ'. Then $f_1^{(1)}(x)=x^2+3k_1'x+3m_1'$. Hence

$$\theta'^2 + 3k_1'\theta' + 3m_1' \equiv 0 \pmod{\mathfrak{p}_1^{\alpha}}. \tag{26}$$

Substituting (25) in (26) and using the relations $a\equiv 0 \pmod 3$ and $\theta^2+3k_1\theta+3m_1\equiv 0 \pmod{\mathfrak{p}_1^{\alpha-\rho}}$, we have

$$3m_1b^2 - 3m_1' \equiv 0 \pmod{\mathfrak{p}_1^3}. \tag{27}$$

Since $b\equiv 0 \pmod 3$ we have $b^2\equiv 1 \pmod 3$ or $b^2\equiv 1 \pmod{\mathfrak{p}_1}$. Hence it follows from (27) that $m_1\equiv m_1' \pmod{\mathfrak{p}_1}$, i.e., $m_1\equiv m_1' \pmod 3$. We have thus shown that in a given field m_1 in (23) is fixed (mod 3) for any integer θ satisfying (22).

On the other hand, if m_1, m_2, m_3, m_4 are four arbitrary rational integers not divisible by 3 there exists a field K containing an integer θ satisfying (22) such that the given m's occur in (23). For let

$$f_i(x) = \phi_i^{(1)}(x) + 3(k_1\phi_i^{(1)}(x) + m_i)$$

where m_i takes on the given values and $\phi_i^{(1)}(x)$, $i=1, 2, 3, 4$, are the corresponding prime functions in (23). We may choose k_i so that

$$k_i\phi_i^{(1)}(x) + m_i \not\equiv k_j\phi_j^{(1)}(x) + m_j$$

for $i\neq j$. Then the discriminant of the polynomial $\Pi(x)=\Pi_{i=1}^4 f_i(x)$ is not

zero. Suppose it is divisible by exactly 3^δ. Then an equation of the form

$$f(x) = \Pi(x) + 3^{\delta+1}M(x) = 0$$

will determine the required field if $f(x)$ is irreducible. But we can obviously make $f(x)$ irreducible by choosing $M(x)$ so that $f(x)$ satisfies the Eisenstein irreducibility criterion with respect to a prime other than 3.

It follows from (24) that fields for which $m_1 \not\equiv m_2 \pmod 3$ have $\chi = 2$. On the other hand, if $m_1 \equiv m_2 \pmod 3$ and we choose θ so that $\mathfrak{p}_1^1 \cdot \mathfrak{p}_2^3 \mid \theta$, $\mathfrak{p}_3^1 \mid \theta+1$, and $\mathfrak{p}_4^1 \mid \theta+2$ it follows as in Theorem 5 that $\chi = 3$. We have thus proved the following theorem:

THEOREM 9. *There exist two types of fields of eighth degree in which*

$$[3] = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4^2, \quad N\mathfrak{p}_i = 3.$$

For fields of one type $\chi = 2$, *for the other* $\chi = 3$.

It follows readily that

$$[3] = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4^2 \cdot \mathfrak{p}_5, \quad N\mathfrak{p}_i = 3, i = 1,2,3,4, \quad N\mathfrak{p}_5 = 3^{n-8},$$

is an example of a type of ideal decomposition in the field of nth degree for which χ is not uniquely determined, i.e.,

THEOREM 10. *For fields of nth degree,* $n < 8$, χ *is not in general determined by the prime ideal decomposition.*

IV. CONCLUSION

The complete solution of the problem of determining the possible values of χ for a given prime ideal decomposition is based on the solution of the problem of normalizing the factors (mod p^α) of the characteristic equation. The latter problem is a fundamental problem in the theory of algebraic numbers. In the theory of Kronecker a common index divisor must divide the index form, a homogeneous form in n variables of degree $\frac{1}{2}n(n-1)$, for all integral rational values of the variables. By using known theorems on the greatest common divisor of integers represented by forms it can be shown that the greatest common index divisor of a field of nth degree is not greater than $(\frac{1}{2}n(n-1))!$. The results of this paper seem to indicate that the expression for χ in Theorem 3 is the best maximum for χ for a field of nth degree, but a proof seems to revert to the more fundamental problem mentioned above.

YALE UNIVERSITY,
NEW HAVEN, CONN.