TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 289, Number 1, May 1985

ON THE INDEX OF A NUMBER FIELD

BY

ENRIC NART

ABSTRACT. Arithmetic invariants are found which determine the index $i(K)$ of a number field K. They are used to obtain an explicit formula under certain restrictions on K. They provide also a complete explanation of a phenomenon conjectured by Ore [8] and showed by Engstrom in a particular case [2].

Introduction. The index of a finite number field K is defined as

$$i(K) = \text{g.c.d.}\{i(\theta)/\theta \in K \text{ integer}, K = \mathbf{Q}(\theta)\},$$

where $i(\theta)$ denotes the index of θ. The existence or not of fields with $i(K) > 1$ was a crucial problem in the construction of the ideal theory in the rings of numbers. In 1878 Dedekind [1] characterized when a prime $p \in \mathbf{Z}$ divides $i(K)$ in terms of the decomposition of p into a product of prime ideals of K and found the first example of a cubic field with $i(K) = 2$. Let $i_p(K)$ denote the greatest exponent s such that p^s divides $i(K)$. In 1928 Ore [8] conjectured that, in spite of the fact that $i_p(K) = 0$ or > 0 depends only on the decomposition type of p in K, this is not true for the value of $i_p(K)$. In 1930 Engstrom [2] showed that for the number fields of degree $[K:\mathbf{Q}] \leqslant 7$, $i_p(K)$ depends only on the decomposition type of p in K and for these fields computed $i_p(K)$ in all cases. He then settled Ore's conjecture showing that for the number fields of degree 8 in which $3 = (\mathrm{P}_1 \cdot \mathrm{P}_2 \cdot \mathrm{P}_3 \cdot \mathrm{P}_4)^2$, $i_3(K) = 2$ or 3, both possibilities accessible. In the same paper he found an explicit formula for $i_p(K)$ when p is totally decomposed in K. In 1955 Sukallo [10] claimed to have found a formula for $i_p(K)$ when all the prime ideals of K lying over p have degree one, but these results are incorrect as Engstrom's example shows (see also our Corollary 3.3). In a recent paper [9] Śliwa proves that, when p is nonramified in K, $i_p(K)$ is determined by the decomposition type of p in K. There are no more contributions in the literature to the problem of determining and computing $i_p(K)$; thus, we can find it as one of the unsolved problems in the list of Narkiewicz's book [6]. In this paper we find which arithmetic invariants of K determine the value of $i_p(K)$ (§1) and we use them to obtain an extensive generalization of Engstrom's formula (§2). These results allow us to give a complete explanation of Ore's conjecture and to show in which more general situations this phenomenon will occur (§3).

Throughout this paper p will denote a fixed prime number, $\mathbf{F}_p$ the finite field with p elements, $\mathbf{Z}_p$ the ring of p-adic integers, $\mathbf{Q}_p$ the p-adic field and Ω a fixed algebraic

Received by the editors January 10, 1983 and, in revised form, February 22, 1984.
1980 *Mathematics Subject Classification*. Primary 12A99; Secondary 12B05, 12B10.
Key words and phrases. Index of a number field, Ore's conjecture.

0002-9947/85 $1.00 + $.25 per page

closure of $\mathbf{Q}_p$. For any $m \in \mathbf{Z}_p$ we shall denote by $v_p(m)$ the greatest exponent s such that p^s divides m. For any integer $\alpha \in \Omega$ we shall denote $v_p(\alpha) = v_p(N_{L/\mathbf{Q}_p}(\alpha))/[L:\mathbf{Q}_p]$, where $L = \mathbf{Q}_p(\alpha)$.

1. Characterization of $i_p(K)$. Let S be the set of all monic irreducible polynomials of $\mathbf{Z}_p[X]$. Let E be the set of all finite extensions L of $\mathbf{Q}_p$, $\mathbf{Q}_p \subset L \subset \Omega$, classified up to isomorphism, that is, identifying any two isomorphic extensions. We have a natural mapping $S \xrightarrow{\pi} \mathrm{E}$ which assigns to any polynomial $f(X) \in S$ the class of $\mathbf{Q}_p(\alpha)$, where $\alpha \in \Omega$ is any root of $f(X)$. Let us denote $S_L = \pi^{-1}(L)$ for any $L \in \mathrm{E}$. Let $\mathscr{E}$ be the free abelian monoid generated by E, that is, the set of all the elements of the type

$$\Gamma = L_1 + \cdots + L_r, \qquad L_i \in \mathrm{E}, \tag{1}$$

with the L_i not necessarily different. Given $\Gamma \in \mathscr{E}$ expressed as in (1), any family $f_1(X),\ldots,f_r(X)$ of polynomials such that $f_i(X) \in S_{L_i}$ for all i will be called a Γ-family. We can define

$$I_p(\Gamma) = \min_{\Gamma\text{-families}} \left\{ \sum_{1 \leqslant i < j \leqslant r} R_p(f_i, f_j) + \sum_{i=1}^{r} i_p(f_i) \right\}, \tag{2}$$

where, in general, $R(g, h)$ denotes the resultant of two polynomials $g(X), h(X) \in \mathbf{Z}_p[X]$, $R_p(g, h) = v_p(R(g, h))$ and $i_p(f) = v_p(i(\alpha))$ for any root α of a polynomial $f(X) \in S$.

Let K be a finite number field. Let S_K be the set of the minimal polynomials of all the integers $\theta \in K$ such that $K = \mathbf{Q}(\theta)$. Let $\mathrm{P}_1,\ldots,\mathrm{P}_r$ be the prime ideals of K lying over p. Every completion K_{P_i} of K according to the P_i-adic topology can be mapped onto a subfield of Ω, unique up to isomorphism. Though the K_{P_i} are all different as topological fields, their images in E can coincide; for instance, if $K/\mathbf{Q}$ is Galois, the K_{P_i} are all equal to $L = \mathbf{Q}_p(\alpha_1,\ldots,\alpha_n)$, where $\alpha_1,\ldots,\alpha_n$ are the roots in Ω of any $F(X) \in S_K$. Thus, K_{P_i} determines a unique element of E which we shall continue denoting by K_{P_i} and K has intrinsically associated an element of $\mathscr{E}$:

$$e_p(K) = K_{\mathrm{P}_1} + \cdots + K_{\mathrm{P}_r}.$$

Given any $\Gamma = L_1 + \cdots + L_r \in \mathscr{E}$ it is easy to construct fields K such that $e_p(K) = \Gamma$; we consider arbitrary polynomials $f_i(X) \in S_{L_i} \cap \mathbf{Z}[X]$ and take $F(X) = f_1(X) \cdots f_r(X) + p^s G(X)$, with s large enough and $G(X)$ appropriate in order to make $F(X)$ irreducible over $\mathbf{Q}$. The aim of this section is to prove that this element $e_p(K) \in \mathscr{E}$ determines the value of $i_p(K)$. More precisely we shall prove

THEOREM 1.1. *For every number field K, $i_p(K) = I_p(e_p(K))$.*

If $F(X) = f_1(X) \cdots f_r(X)$ is the factorization of any $F(X) \in S_K$ into irreducible factors in $\mathbf{Q}_p[X]$, it is well known that $f_i(X) \in S_{K_{\mathrm{P}_i}}$ and that

$$i_p(\theta) = \sum_{1 \leqslant i < j \leqslant r} R_p(f_i, f_j) + \sum_{i=1}^{r} i_p(f_i),$$

where θ is any root of $F(X)$ in K and $i_p(\theta) = v_p(i(\theta))$ [3, p. 453]. Therefore it is clear that

$$i_p(K) = \min\{i_p(\theta)/\theta \in K \text{ integer}, K = \mathbf{Q}(\theta)\} \geqslant I_p(e_p(K)).$$

Obviously, an arbitrary $e_p(K)$-family is not constituted in general by the irreducible factors of a polynomial of S_K; nevertheless, the proof of Theorem 1.1 will already be complete when we prove the following theorem, which can be considered as the suitable generalization of [2, Theorem 2]:

THEOREM 1.2. *Let K be a number field, let $\mathrm{P}_1,\ldots,\mathrm{P}_r$ be the prime ideals of K lying over p and let $f_1(X),\ldots,f_r(X)$ be an arbitrary $e_p(K)$-family. For every positive integer s there exists a polynomial $F(X) \in S_K$ such that $F(X) \equiv f_1(X)\cdots f_r(X) \pmod{p^s}$.*

The proof of Theorem 1.2 is based on the fact that if two integers of Ω are "close" according to the ultrametric distance of Ω, their minimal polynomials are congruent (mod p^s) for s "large". Let us prove this in detail. Let $|\ |$ be the only extension to Ω of the p-adic absolute value $|x| = p^{-v_p(x)}$. For any positive integer e let S_e be the set of the polynomials of S of degree e. Let us consider the following ultrametric distances in S_e:

$$d(f,g) = \max_{1\leqslant i\leqslant e}\{|a_i - b_i|\},$$

$$\Delta(f,g) = \min_{1\leqslant i,j\leqslant e}\{|\alpha_i - \beta_j|\} \quad \text{(cf. [5])},$$

$$d_e(f,g) = |R(f,g)|^{1/e} = |f(\beta_j)| = |g(\alpha_i)| \quad \text{(cf. [5])},$$

where $f(X) = \sum_{i=0}^{e} a_i X^{e-i}$, $g(X) = \sum_{i=0}^{e} b_i X^{e-i} \in S_e$ have respective roots $\alpha_1,\ldots,\alpha_e$; $\beta_1,\ldots,\beta_e \in \Omega$. We need to prove that $\Delta \geqslant d$ topologically. For the sake of completeness we shall prove

PROPOSITION 1.3. *The three distances d, Δ and d_e are equivalent.*

PROOF. Let $f(X)$, $g(X) \in S_e$ have respective roots $\alpha = \alpha_1,\ldots,\alpha_e$; $\beta = \beta_1,\ldots,\beta_e \in \Omega$. For every positive integer s it is clear that

$$f(X) \equiv g(X) \pmod{p^s} \Rightarrow v_p(g(\alpha)) = v_p\left(\prod_{i=1}^{e}(\alpha - \beta_i)\right) \geqslant s,$$

hence, $\max_{1\leqslant i\leqslant e}\{v_p(\alpha - \beta_i)\} \geqslant s/e$. This proves $d \geqslant d_e \geqslant \Delta$. Let R be the ring of integers of $\mathbf{Q}_p(\alpha)$ and let φ_s be the canonical homomorphism $R \xrightarrow{\varphi_s} R/p^sR$. Let $t = i_p(\alpha)$; we know that $p^tR \subset \mathbf{Z}_p[\alpha]$, hence, for $s \geqslant t$ we have

$$\ker(\varphi_{s|\mathbf{Z}_p[\alpha]}) = \ker(\varphi_s) \cap \mathbf{Z}_p[\alpha] = p^sR \cap \mathbf{Z}_p[\alpha] \subset p^{s-t}\mathbf{Z}_p[\alpha].$$

Therefore, if we denote by ϕ_s the composition of the canonical homomorphisms

$$\mathbf{Z}_p[X] \to \mathbf{Z}_p[X]/f(X) \xrightarrow{\sim} \mathbf{Z}_p[\alpha] \hookrightarrow R \xrightarrow{\varphi_s} R/p^sR,$$

we have $\ker(\phi_s) \subset (p^{s-t}, f(X))$. Hence, if $v_p(\alpha - \beta) \geqslant s$, $\phi_s(g(X)) = 0$ and this leads to $g(X) \in (p^{s-t}, f(X))$. Since $f(X)$ and $g(X)$ are two monic polynomials

with the same degree we conclude that $f(X) \equiv g(X) \pmod{p^{s-t}}$. Therefore $\Delta \geqslant d$ and the proposition is proved. □

PROOF OF THEOREM 1.2. Let $\alpha_i \in \Omega$ be any root of $f_i(X)$ and let $t_i = i_p(f_i)$ for all $1 \leqslant i \leqslant r$. Let $\theta \in K$ be any integer satisfying

$$\theta \equiv \alpha_i \pmod{\mathrm{P}_i^{m_i}}, \qquad 1 \leqslant i \leqslant r, \tag{3}$$

where $m_i \geqslant e(\mathrm{P}_i/p) \cdot (s + t_i)$. We can assume that $\mathbf{Q}(\theta) = K$, since, if it were not the case, we take $\theta' = \theta + p^t\omega$, where $\omega \in K$ is any integer such that $K = \mathbf{Q}(\omega)$; for any embedding $K \xrightarrow{\sigma} \mathbf{C}$, $\theta' = \sigma(\theta')$ is equivalent to

$$\theta - \sigma(\theta) + p^t(\omega - \sigma(\omega)) = 0, \tag{4}$$

hence, taking t large enough we can assure simultaneously that θ' satisfies (3) and that (4) is not possible. Let $F(X) \in S_K$ be the minimal polynomial of θ and let $F(X) = g_1(X) \cdots g_r(X)$ be the factorization of $F(X)$ into irreducible factors in $\mathbf{Q}_p[X]$. For each i, the homomorphism $K \to K_{\mathrm{P}_i}$ sends θ to one of the roots of $g_i(X)$ in Ω, hence, (3) and the last part of the proof of Proposition 1.3 show that $g_i(X) \equiv f_i(X) \pmod{p^s}$. □

REMARK. All the results of this paragraph are extendible, in an obvious way, to the relative case.

2. Computation of $I_p(\Gamma)$ in the totally-ramified case. Let $\mathrm{E}_e^{\mathrm{ram}}$ be the subset of E of the totally-ramified extensions of degree e, $S_e^{\mathrm{ram}} = \pi^{-1}(\mathrm{E}_e^{\mathrm{ram}})$, $\mathrm{E}^{\mathrm{ram}} = \bigcup_{e \geqslant 1} \mathrm{E}_e^{\mathrm{ram}}$ and $S^{\mathrm{ram}} = \bigcup_{e \geqslant 1} S_e^{\mathrm{ram}}$. Let $\mathscr{E}^{\mathrm{ram}}$ be the subset of $\mathscr{E}$ of the $\Gamma = L_1 + \cdots + L_r$ such that $L_i \in \mathrm{E}^{\mathrm{ram}}$ for all i. We have shown in the preceding paragraph that the problem of the computation of $i_p(K)$ for every number field K is equivalent to that of the computation of $I_p(\Gamma)$ for every $\Gamma \in \mathscr{E}$. We deal now with this problem in the case that $\Gamma \in \mathscr{E}^{\mathrm{ram}}$.

If e is a positive integer not divisible by p, there is a well-known bijection $\mathrm{E}_e^{\mathrm{ram}} \xrightarrow{\tilde{N}} \mathbf{F}_p^*/\mathbf{F}_p^{*e}$ [3, Chapter 16]. If $e = p^t e_0$, $p \nmid e_0$, we can define a (not bijective in general) mapping,

$$\mathrm{E}_e^{\mathrm{ram}} \xrightarrow{\tilde{N}} \mathbf{F}_p^*/\mathbf{F}_p^{*e_0},$$

taking $\tilde{N}(L) = \tilde{N}(L_0)$, where L_0 is the only tamely-ramified extension, $\mathbf{Q}_p \subset L_0 \subset L$, of degree e_0.

For any two positive integers m, q we shall denote $\chi(m, q) = \frac{1}{2}a(m - q + b)$, where $m = aq + b$, $0 \leqslant b < q$. The main theorem in this section is the following:

THEOREM 2.1. *Let $\Gamma = n_1\mathbf{Q}_p + n_2L_2 + \cdots + n_rL_r \in \mathscr{E}^{\mathrm{ram}}$ with the L_i all different and such that $e_1 \leqslant e_2 \leqslant \cdots \leqslant e_r$, where $e_i = [L_i : \mathbf{Q}_p]$. Suppose that $n_2, \ldots, n_r$ are bounded by*

$$n_i \leqslant p(p-1)/(e_i, p-1) \quad \text{if } p \nmid e_i,$$

$$\sum_{\substack{e_j = e_i \\ \tilde{N}(L_j) = \tilde{N}(L_i)}} n_j \leqslant p(p-1)/((e_i)_0, p-1) \quad \text{if } e_i = p^t(e_i)_0,\ p \nmid (e_i)_0.$$

Then, if we denote $m_i = \sum_{j \geqslant i} n_j$, $1 \leqslant i \leqslant r$, *and* $e_0 = 0$, *we have*

$$I_p(\Gamma) = \sum_{s \geqslant 2} \chi(n_1, p^s) + \sum_{i=1}^{r} \chi(m_i, p)(e_i - e_{i-1}). \tag{5}$$

The bounds on the n_i's, $i \geqslant 2$, will allow us to prove that the minimum value (2) is attained by a Γ-family with all the polynomials satisfying $i_p(f) = 0$. The first steps deal with general properties of the polynomials S^{ram} and with the computation of $R_p(f, g)$ for two such polynomials.

LEMMA 2.2. *Let* $f(X) \in S_e^{\text{ram}}$.

(i) *There exists* $j \in \{0, 1, \ldots, p-1\}$ *such that* $f(X) \equiv (X - j)^e \pmod{p}$.

(ii) *Newton's polygon of* $f(X + j)$ *has only one side with slope* $v_p(a_e)/e$, *where* $f(X + j) = X^e + a_1 X^{e-1} + \cdots + a_e$.

(iii) $i_p(f) = 0$ *iff* $\deg(f(X)) = 1$ *or* $f(X + j)$ *is Eisenstein.*

(iv) *If* $g(X) \in S_{e'}^{\text{ram}}$, $R_p(f, g) > 0$ *iff* $g(X) \equiv (X - j)^{e'} \pmod{p}$.

PROOF. (i) Since $f(X)$ is irreducible, by Hensel's lemma, $f(X) \equiv \varphi(X)^m \pmod{p}$, where $\varphi(X)$ is an irreducible polynomial of $\mathbf{F}_p[X]$. Let $\alpha \in \Omega$ be any root of $f(X)$ and let $L = \mathbf{Q}_p(\alpha)$. We have $\mathbf{F}_p \subset \mathbf{F}_p(\bar{\alpha}) \subset \bar{L}$, and clearly $\varphi(X)$ is the minimal polynomial of $\bar{\alpha}$ over $\mathbf{F}_p$. Hence, the degree of $\varphi(X)$ is a divisor of the residual degree of $L/\mathbf{Q}_p$, which is equal to one in our case.

(ii), (iii) and (iv) are easy to prove after (i). □

Since a linear change of the variable preserves the value of $R_p(f, g)$, by (i), (ii) and (iv) of this lemma, in the computation of $R_p(f, g)$ we can restrict ourselves to the following case:

LEMMA 2.3. *Let* $f(X), g(X) \in \mathbf{Z}_p[X]$ *be two monic polynomials such that* $f(X) \equiv X^e$, $g(X) \equiv X^{e'} \pmod{p}$ *and with Newton's polygons having only one side with respective slopes* $\lambda = m/e, \lambda' = m'/e'$. *Then* $R_p(f, g) \geqslant \min\{m'e, me'\}$ *and if* $\lambda \neq \lambda'$ *the equality holds.*

PROOF. Let $\alpha_1, \ldots, \alpha_e$; $\beta_1, \ldots, \beta_{e'} \in \Omega$ be the respective roots of $f(X)$ and $g(X)$. $R(f, g) = \prod_{i,j}(\alpha_i - \beta_j)$ and it is well known that $v_p(\alpha_i) = \lambda$ and $v_p(\beta_j) = \lambda'$ for all i, j. □

By (iii) of Lemma 2.2 we are specially interested in the case that both polynomials are Eisenstein. Let S_e^E denote the subset of S^{ram} of Eisenstein polynomials of degree e. By Lemma 2.3, if $f(X) \in S_e^E$, $g(X) \in S_{e'}^E$ and $e \neq e'$, we have $R_p(f, g) = \min\{e, e'\}$. If $e = e'$ we can compute $R_p(f, g)$ by a formula of Krasner:

LEMMA 2.4 (KRASNER [5, p. 156]). *Let* $f(X) = X^e + a_1 X^{e-1} + \cdots + a_e$, $g(X) = X^e + b_1 X^{e-1} + \cdots + b_e \in S_e^E$. *Then*

$$R_p(f, g) = \min_{1 \leqslant i \leqslant e} \{ e \cdot v_p(a_i - b_i) + (e - i) \}.$$

In particular, $R_p(f, g) = e$ *iff* $a_e \not\equiv b_e \pmod{p^2}$.

It is suggested by (i) and (iv) of Lemma 2.2 that, for any $\Gamma \in \mathscr{E}^{\text{ram}}$, the way that the polynomials $f_1(X), \ldots, f_r(X)$ of a Γ-family are distributed among the $X - j$,

$0 \leqslant j < p$, can give a rough idea of the value of $\Sigma_{1 \leqslant i < j \leqslant r} R_p(f_i, f_j)$. It is natural to ask if there exists a standard way of distributing these polynomials such that for any $\Gamma \in \mathscr{E}^{\mathrm{ram}}$ the minimum value of (2) is always attained by a Γ-family with the standard distribution. By (iv) of Lemma 2.2, it is natural to think that the best candidate for a standard distribution is that of maximum equilibrium.

DEFINITION. Let $\Gamma = n_1 L_1 + \cdots + n_r L_r \in \mathscr{E}^{\mathrm{ram}}$ with the L_i all different and such that $[L_1 : \mathbf{Q}_p] \leqslant \cdots \leqslant [L_r : \mathbf{Q}_p]$. We define a Γ-*distribution* to be any decomposition of $n_1, \ldots, n_r$ into a sum of p terms

$$n_i = n_{i,0} + \cdots + n_{i,p-1}, \quad n_{i,j} \geqslant 0; \qquad 1 \leqslant i \leqslant r.$$

A Γ-distribution will be called *standard* if it satisfies

$$\max_{0 \leqslant j < k < p} \left\{ |m_{i,j} - m_{i,k}| \right\} \leqslant 1 \quad \text{for all } 1 \leqslant i \leqslant r,$$

where $m_{i,j} = \Sigma_{t=i}^{r} n_{t,j}$, for all $1 \leqslant i \leqslant r$, $0 \leqslant j < p$.

We can associate to any Γ-family a Γ-distribution taking $n_{i,j}$ to be the number of polynomials of the family that belong to S_{L_i} and are congruent (mod p) to a power of $X - j$. It is obvious that for any Γ-distribution there exist Γ-families with this distribution associated. In the ideal case that all the polynomials in the Γ-family (those with the same degree included) satisfy $i_p(f) = 0$ and $R_p(f, g) = \min\{\deg(f(X)), \deg(g(X))\}$ or $R_p(f, g) = 0$, the minimum value of (2) is always attained when the associated distribution is standard. In the course of the proof of this fact, which is purely combinatorial, we shall obtain also an explicit formula for the value of $\Sigma_{1 \leqslant i < j \leqslant r} R_p(f_i, f_j)$ in that ideal case.

Let us think, in full generality, that instead of polynomials belonging to different S_{L_i}, $1 \leqslant i \leqslant r$, we have "objects" inside r different "boxes"which we label $1, 2, \ldots, r$. The objects inside each box are divided into q classes and we assign to any two objects from the same class, bleonging to the boxes i and j, the weight $\min\{e_i, e_j\}$, where $0 \leqslant e_1 \leqslant \cdots \leqslant e_r \in \mathbf{R}$ depend only on the box. The problem is to determine for which distribution of the objects the total sum of these weights is minimum and to compute this number. Let us begin with the case of one single box. Assume that the weight of the box is $e = 1$ so that, in fact, we are counting the total number of pairs of objects from the same class.

PROPOSITION 2.5. *Let m and q be positive integers. Then $\chi(m, q)$ is the minimum total number of (unordered) pairs of objects from the same class when m objects are divided into q classes. That is*

$$\chi(m, q) = \min\left\{ \sum_{j=1}^{q} \binom{m_j}{2} \right\},$$

where

$$\binom{m_j}{2}$$

is the binomial coefficient and the minimum is taken over all sequences of nonnegative integers $m_1, \ldots, m_q$ with $\Sigma_{j=1}^{q} m_j = m$. The minimum is attained if and only if $|m_j - m_k| \leqslant 1$ for all j, k, that is, when $m_j = a$ or $a + 1$ for all j, where $m = aq + b$, $0 \leqslant b < q$.

PROOF. Suppose a set of m objects is divided into q classes of $m_1,\dots,m_q$ elements respectively. If $m_j - m_k \geqslant 2$ for some $j \neq k$, then removing an object from the jth class and placing it in the kth class decreases the sum

$$\sum_{j=1}^{q} \binom{m_j}{2}$$

by exactly $m_j - m_k - 1 > 0$. This proves the criterion for the minimum. When the criterion is satisfied, there are clearly b classes with $a+1$ objects and $q-b$ classes with a objects and so the minimum value of the sum is $b\binom{a+1}{2} + (q-b)\binom{a}{2} = \chi(m,q)$. □

REMARK. Suppose $m = m' + m''$ and $q = q' + q''$. Then $\chi(m,q) \leqslant \chi(m',q') + \chi(m'',q'')$ since a set of m objects can be divided into q classes by first partitioning it into two subsets of m' and m'' objects each, and then dividing the subsets into q' and q'' classes, respectively.

We can now deal with the general case:

PROPOSITION 2.6. *Suppose that we have r boxes with q subdivisions each and containing respectively $n_1,\dots,n_r$ objects distributed among the subdivisions in the following way*:

$$n_i = n_{i,1} + \cdots + n_{i,q}, \quad n_{i,j} \geqslant 0; \qquad 1 \leqslant i \leqslant r.$$

Let $0 = e_0 \leqslant e_1 \leqslant \cdots \leqslant e_r$ be arbitrary real numbers. Assign to any unordered couple of objects in the same subdivision of the boxes i, j the weight $\min\{e_i, e_j\}$ and let M be the sum of all these weights. Then we have

$$M \geqslant \sum_{i=1}^{r} \chi(m_i,q)(e_i - e_{i-1}), \tag{6}$$

where $m_i = \sum_{t=i}^{r} n_t$ for all i. Let $m_{i,j} = \sum_{t=i}^{r} n_{t,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant q$. The condition

$$\max_{0 \leqslant j < k \leqslant q} \left\{ |m_{i,j} - m_{i,k}| \right\} \leqslant 1 \quad \text{for all } 1 \leqslant i \leqslant r \tag{7}$$

is sufficient to assure that equality holds in (6). *If $0 \leqslant e_1 < \cdots < e_r$, this condition is also necessary.*

PROOF. For every $1 \leqslant i \leqslant r$, the total number of couples of objects of the boxes $i, i+1,\dots,r$ in coincident subdivisions is equal to

$$a_i = \sum_{j=1}^{q} \binom{m_{i,j}}{2}.$$

On the other side, it is clear that

$$M = \sum_{i=1}^{r} a_i(e_i - e_{i-1}). \tag{8}$$

In fact, for every couple of objects of two boxes $i \leqslant j$ in the same subdivision, the right member of (8) counts a weight of $e_1 + (e_2 - e_1) + \cdots + (e_i - e_{i-1}) = e_i$, as does the left one. Now by Proposition 2.5, $a_i \geqslant \chi(m_i,q)$ for all i, and (7) is equivalent to $a_i = \chi(m_i,q)$ for all i. Hence, the first two assertions are proven. If

$e_i - e_{i-1} > 0$ for all i, we have, conversely, that the equality in (6) implies that $a_i = \chi(m_i, q)$ for all i. □

REMARK. It is easy to see that, for fixed $n_1, \ldots, n_r$, the $n_{i,j}$ may be chosen in such a manner that (7) is satisfied. One proceeds by distributing the objects of the rth box as uniformly as possible among the q subdivisions, and then doing the same with the objects of the $(r-1)$st box, taking care to add the excess elements first to those subdivisions which came out short in the previous distribution, etc.

The last step in order to prove Theorem 2.1 is to check that the bounds on the n_i's, $i \geqslant 2$, assure that Γ is almost in that ideal case. By Lemma 2.3 only Eisenstein polynomials of the same degree may have $R_p(f, g) > \min\{\deg(f(X)), \deg(g(X))\}$. By Lemma 2.4 we are led to seek, for $L \in \mathrm{E}^{\mathrm{ram}}$ fixed, the maximum number of Eisenstein polynomials of S_L with last terms pairwise noncongruent mod p^2.

It is well known that a tamely-ramified extension $L/\mathbf{Q}_p$ of degree e can be defined by a root of a binomial $X^e + pa$, $p \nmid a$, and that reciprocally, such a binomial has a root in L if and only if the class of a in $\mathbf{F}_p^*/\mathbf{F}_p^{*e}$ is a fixed one, which at the beginning of the section we have denoted by $N(L)$. We need to prove that the same is true not only for binomials but for Eisenstein polynomials in general.

PROPOSITION 2.7. *Let e be a positive integer not divisible by p and let $f(X) = X^e + a_1 X^{e-1} + \cdots + a_3 \in S_e^E$. Then, $\pi(f(X)) = \pi(X^e + a_e)$.*

PROOF. Let $\zeta \in \Omega$ be a primitive eth root of unity. Since $p \nmid e$, $\mathbf{Q}_p(\zeta)/\mathbf{Q}_p$ is nonramified and $v_p(\zeta^i - \zeta^j) > 0$ if and only if $i \equiv j \pmod{e}$. Denote $g(X) = X^e + a_e$; let $\beta \in \Omega$ be any root of $g(X)$ and $\beta_i = \zeta^i \beta$, $0 \leqslant i < e$, the other roots of $g(X)$. If $\beta_i \neq \beta_j$ we have

$$v_p(\beta_i - \beta_j) = v_p(\zeta^i - \zeta^j) + v_p(\beta) = v_p(\beta) = 1/e.$$

By Lemma 2.4, there exists an index, $1 \leqslant k < e$, such that $R_p(f, g) = e \cdot v_p(a_k) + e - k$. Hence, if $\alpha_1, \ldots, \alpha_e \in \Omega$ are the roots of $f(X)$, from

$$R_p(f, g) = \sum_{i,j} v_p(\alpha_i - \beta_j) = e \sum_i v_p(\alpha_i - \beta)$$

we conclude that there exists a root α of $f(X)$ such that

$$v_p(\alpha - \beta) \geqslant \frac{v_p(a_k)}{e} + \frac{e-k}{e^2} > \frac{k}{e^2} + \frac{e-k}{e^2} = \frac{1}{e},$$

the last inequality since $v_p(a_k) \geqslant 1 > k/e$. By Krasner's lemma, $\pi(f(X)) = \pi(g(X))$. □

COROLLARY 2.8. *Let e be a positive integer, $e = p^t e_0$, $p \nmid e_0$. If for any $f(X) = X^e + a_1 X^{e-1} + \cdots + a_e \in S_e^E$ we define $N(f(X))$ to be the class in $\mathbf{F}_p^*$ of a_e/p, the following diagram is commutative:*

$$\begin{array}{ccc} S_e^E & \xrightarrow{N} & \mathbf{F}_p^* \\ \pi \downarrow & & \downarrow \\ \mathrm{E}_e^{\mathrm{ram}} & \xrightarrow{\tilde{N}} & \mathbf{F}_p^*/\mathbf{F}_p^{*e_0} \end{array}$$

PROOF. If $p \nmid e$, it is clear from Proposition 2.7. In the general case, let $f(X) = X^e + a_1 X^{e-1} + \cdots + a_e \in S_e^E$ and let $L = \pi(f(X))$. For any root $\alpha \in L$ of $f(X)$ we have

$$N_{L/\mathbf{Q}_p}(\alpha) = N_{L_0/\mathbf{Q}_p}\big(N_{L/L_0}(\alpha)\big) = (-1)^e a_e,$$

where L_0 is the only tamely-ramified extension, $\mathbf{Q}_p \subset L_0 \subset L$, of degree e_0. Now, $N_{L/L_0}(\alpha)$ is a prime element of L_0, hence, its minimal polynomial over $\mathbf{Q}_p$ is an Eisenstein polynomial of S_{L_0}. By the corollary in the tamely-ramified case, the class of a_e/p in $\mathbf{F}_p^*/\mathbf{F}_p^{*e_0}$ coincides with $\tilde{N}(L_0)$. □

COROLLARY 2.9. *Let* $L \in \mathrm{E}_e^{\mathrm{ram}}$, $e = p^t e_0$, $p \nmid e_0$. *The maximum number of Eisenstein polynomials of* S_L *with the property that* $R_p(f, g) = e$ *for any two of them is exactly* $(p-1)/(e_0, p-1)$.

PROOF. By Corollary 2.8, any Eisenstein polynomial $f(X) \in S_L$ has a last term of the type pc, where the class of c in $\mathbf{F}_p^*/\mathbf{F}_p^{*e_0}$ is equal to $\tilde{N}(L)$. On the other side, if we take any $m = (p-1)/(e_0, p-1) = \mathrm{card}\{\mathbf{F}_p^{*e_0}\}$ Eisenstein polynomials of degree e with last terms $pc_1, \ldots, pc_m$ such that the subset $\{\bar{c}_1, \ldots, \bar{c}_m\}$ of $\mathbf{F}_p^*$ coincides with the class $\tilde{N}(L)$ of $\mathbf{F}_p^*/\mathbf{F}_p^{*e_0}$, by Corollary 2.8 they will all belong to S_L and, by Lemma 2.4, $R_p(f, g) = e$ for any two of them. □

Finally, let us quote a result of Hensel which leads to Engstrom's formula for the value of $I_p(n\mathbf{Q}_p)$.

LEMMA 2.10 (HENSEL). *Let* n *be a positive integer and let* $\Gamma = n\mathbf{Q}_p \in \mathscr{E}$.

$$I_p(\Gamma) = \sum_{s \geqslant 1} \chi(n, p^s),$$

and this value is attained by the Γ*-family* $X - 1, \ldots, X - n$.

REMARK. Although this formula is obtained by Engstrom, it is a trivial application of a result of Hensel [**4**, p. 351]. The really interesting contribution of Engstrom was to prove that this value coincides with $i_p(K)$ for any number field K of degree n in which p is totally decomposed.

PROOF OF THEOREM 2.1. By Lemmas 2.3 and 2.4, Corollary 2.9 and Lemma 2.10, the bounds on the n_i's, $i \geqslant 2$, assure the existence of a Γ-family with a standard Γ-distribution such that for all the polynomials in the family $i_p(f) = 0$ and such that for any couple of polynomials not both in $S_{\mathbf{Q}_p}$, $R_p(f, g) = \min\{\deg(f(X)), \deg(g(X))\}$. Moreover, if we take the polynomials of $S_{\mathbf{Q}_p}$ to be $X - 1, \ldots, X - n_1$, by Proposition 2.6 and Lemma 2.10, for such a Γ-family, $\Sigma_{i<j} R_p(f_i, f_j)$ takes the value (5). We have only to prove that this value is minimum among all the Γ-families. It is not a direct consequence of Proposition 2.6 just because of the presence of polynomials of $S_{\mathbf{Q}_p}$ with $R_p(f, g) > 1$. Let

$$n_i = n_{i,0} + \cdots + n_{i,p-1}, \quad n_{i,j} \geqslant 0; \qquad 1 \leqslant i \leqslant r,$$

be an arbitrary Γ-distribution. Let $n = n_1 + \cdots + n_r$ and $f_1(X), \ldots, f_n(X)$ be any Γ-family with this distribution. Suppose that $f_1(X), \ldots, f_{n_1}(X)$ are the polynomials

belonging to $S_{\mathbf{Q}_p}$ and denote $A = \Sigma_{1 \leqslant i < j \leqslant n_1} R_p(f_i, f_j)$. By Lemma 2.3 and Proposition 2.6 we have

$$\sum_{1 \leqslant i < j \leqslant n} R_p(f_i, f_j) \geqslant \sum_{i=1}^{r} \chi(m_i, p) - \sum_{j=0}^{p-1} \chi(n_{1,j}, 1) + A,$$

where in the right member we can think that we have counted first

$$\min\{\deg(f_i(X)), \deg(f_j(X))\}$$

instead of $R_p(f_i, f_j)$ for every couple of polynomials with $R_p(f_i, f_j) > 0$ and then replaced the sum $\Sigma_{j=0}^{p-1} \chi(n_{1,j}, 1)$ corresponding to the couples of polynomials both in $S_{\mathbf{Q}_p}$ by the correct value. By Lemma 2.10, for any $0 \leqslant j < p$, the $n_{1,j}$ polynomials of the family congruent (mod p) to $X - j$ will have $\Sigma_{i<j} R_p(f_i, f_j)$ greater than or equal to the sum provided by the polynomials $X - j$, $X - (j + p), \ldots, X - (j + (n_{1,j} - 1)p)$. Hence,

$$A \geqslant \sum_{j=0}^{p-1} \sum_{s \geqslant 0} \chi(n_{1,j}, p^s).$$

Therefore, we have only to prove that

$$\sum_{j=0}^{p-1} \sum_{s \geqslant 1} \chi(n_{1,j}, p^s) \geqslant \sum_{s \geqslant 2} \chi(n_1, p^s).$$

We prove this inequality showing that for each $s \geqslant 2$ we have

$$\sum_{j=0}^{p-1} \chi(n_{1,j}, p^{s-1}) \geqslant \chi(n_1, p^s). \tag{9}$$

This last inequality follows from the remark following Proposition 2.5 observing that $n_1 = \Sigma_{j=1}^{p} n_{1,j}$ and $p^s = \Sigma_{j=1}^{p} p^{s-1}$. □

3. On Ore's conjecture. We can define a decomposition type (d.t.) as a family $n_{f,e}$, with f, e, $n_{f,e}$ integers, $f, e > 0$, $n_{f,e} \geqslant 0$, such that $\Sigma_{f,e} n_{f,e} < \infty$. We define the d.t. of a prime $p \in \mathbf{Z}$ in a number field K taking $n_{f,e}$ to be the number of prime ideals of K lying over p with residual degree f and ramification index e. In [7] Ore proved that for any prime p and arbitrary d.t. there exist number fields K such that p has this d.t. in K; and in [8] he conjectured that for these fields $i_p(K)$ can take different values. This was confirmed by Engstrom [2] showing that the number fields of degree 8 in which $3 = (\mathrm{P}_1 \cdot \mathrm{P}_2 \cdot \mathrm{P}_3 \cdot \mathrm{P}_4)^2$ have $i_3(K) = 2$ or 3. Our Theorem 1.1 provides a large family of d.t.'s which determine the value of $i_p(K)$:

COROLLARY 3.1. *Let* $\{n_{f,e}\}$ *be a d.t. such that*

$$n_{f,e} > 0 \Rightarrow p \nmid e \quad \textit{and} \quad (e, p^f - 1) = 1.$$

Then, $i_p(K)$ *takes the same value for all the number fields* K *in which* p *has this d.t.*

PROOF. Under this condition on e and f, there is a unique element of E with residual degree f and ramification index e. Hence, all the number fields in which p has this d.t. have the same $e_p(K)$. □

REMARK. In particular, this is the case when p is not ramified.

By Theorem 2.1, the d.t.'s with $n_{f,e} = 0$ for all $f > 1$ and $n_{1,e}$ suitably bounded will also determine $i_p(K)$. In order to cover the case in which $\tilde{N}(K_{\mathrm{P}_i})$ is the same for all the P_i lying over p with residual degree 1 and ramification index e, the bound must be $n_{1,e} \leqslant p(p-1)/(e_0, p-1)$, where $e = p^t e_0$, $p \nmid e_0$. In order to give a more complete result we need the following:

LEMMA 3.2. *Let $L \in \mathrm{E}$ have residual degree f and ramification index e. For any irreducible polynomial $\varphi(X) \in \mathbf{F}_p[X]$ of degree f there exist polynomials $f(X) \in S_L$ such that $f(X) \equiv \varphi(X)^e \pmod p$ and $i_p(f) = 0$.*

PROOF. Take the minimal polynomial of $\pi + \tau$, where $\pi \in L$ is any integer such that $v_p(\pi) = 1/e$ and $\tau \in L$ is any $(p^f - 1)$th root of unity such that $\bar{\tau}$ is a root of $\varphi(X)$. □

For any positive integer f, let $\rho(f)$ denote the number of irreducible polynomials of $\mathbf{F}_p[X]$ of degree f. We can now state the

COROLLARY 3.3. *Let $\{n_{f,e}\}$ be a d.t. such that*

$$\sum_e n_{f,e} \leqslant \rho(f) \quad \text{for all } f > 1, \tag{10}$$

$$n_{1,e} \leqslant p(p-1)/(e_0, p-1) \quad \text{for all } e > 1, \tag{11}$$

where $e = p^t e_0$, $p \nmid e_0$. Then, for all number fields K in which p has this d.t., $i_p(K)$ is equal to

$$i_p(K) = \sum_{s \geqslant 2} \chi(n_1, p^s) + \sum_{e \geqslant 1} \chi(m_e, p),$$

where we have denoted $n_e = n_{1,e}$ and $m_e = \sum_{i \geqslant e} n_i$.

PROOF. Let K be a number field in which p has this d.t. Let $\mathrm{P}_1, \ldots, \mathrm{P}_k$ be the prime ideals of K lying over p with residual degree greater than one. By Lemma 3.2 and (10), we can take an $e_p(K)$-family such that the polynomials $f_i(X) \in S_{K_{\mathrm{P}_i}}$ satisfy $i_p(f_i) = 0$ and $R_p(f_i, g) = 0$ for all other $g(X)$ in the family. Hence, $\Gamma = e_p(K) - K_{\mathrm{P}_1} - \cdots - K_{\mathrm{P}_k} \in \mathscr{E}^{\mathrm{ram}}$ and $i_p(K) = I_p(e_p(K)) = I_p(\Gamma)$. By (11), Γ satisfies the hypothesis of Theorem 2.1. □

REMARKS. (1) Note that in the expression $\sum_{e \geqslant 1} \chi(m_e, p)$, the sum is extended over all the integer values of e, those with $n_e = 0$ included.

(2) This corollary shows that even in the case when p is determined by the d.t. of p in K, the formula of Sukallo [**10**] is incorrect.

In fact, Theorem 1.1 completely clarifies Ore's conjecture. The fact that there is not in general a unique element of E with prefixed residual degree and ramification index means that fields K in which p has the same d.t. can have $e_p(K)$ different and therefore $i_p(K) = I_p(e_p(K))$ possibly different. We can also give a complete explanation of Engstrom's discovery: There are only two quadratic ramified extensions of $\mathbf{Q}_3$,

$$L_1 = \mathbf{Q}_3(\sqrt{3}) \quad \text{and} \quad L_2 = \mathbf{Q}_3(\sqrt{-3}).$$

By Proposition 2.7, an Eisenstein polynomial $X^2 + 3a + 3b$ belongs to S_{L_1} or to S_{L_2} according to $b = -1$ or $1 \pmod 3$; hence, by Lemma 2.4, if $f(X), g(X) \in S_2^E$, $R_3(f, g) = 2$ if and only if $\pi(f(X)) \neq \pi(g(X))$. Now, for every number field K of degree 8 in which $3 = (\mathrm{P}_1 \cdot \mathrm{P}_2 \cdot \mathrm{P}_3 \cdot \mathrm{P}_4)^2$, all $e_3(K)$-families have two polynomials $f(X), g(X)$ congruent (mod 3) to a power of the same $X - j$. If $e_3(K) = 4L_1$ or $4L_2$, it must be $\pi(f(X)) = \pi(g(X))$ and $i_3(K) = 3$, whereas in all other cases we can make $\pi(f(X)) \neq \pi(g(X))$ and $i_3(K) = 2$.

Moreover, it is clear that this phenomenon will occur whenever, for e, f not satisfying the condition of Corollary 3.1, there is an accumulation of prime ideals lying over p with the same residual degree f and ramification index e.[1] In that case, $i_p(K)$ will take a higher value for the number fields with an $e_p(K)$ containing more repetitions of elements $L \in \mathrm{E}$ with the same $\tilde{N}(L)$. Let us discuss an example, continuing with $p = 3, f = 1, e = 2$.

EXAMPLE 3.4. The number fields of degree 14 in which $3 = (\mathrm{P}_1 \cdots \mathrm{P}_7)^2$ have $i_3(K) = 11, 12, 13$, or 14, respectively, according to $e_3(K) = 4L_1 + 3L_2, 5L_1 + 2L_1, 6L_1 + L_2$ or $7L_1$, and the same values if we interchange L_1 and L_2.

In fact, if $f(X) = X^2 + 3aX + 3b$, $g(X) = X^2 + 3a' + 3b'$ are Eisenstein polynomials belonging to S_{L_1}, by Lemma 2.4 we have $R_3(f, g) \geqslant 3$ and $R_3(f, g) = 3$ if and only if $a \not\equiv a' \pmod 3$. Hence, if we restrict ourselves to polynomials with $i_3(f) = 0$ and consider the distributions

$$\begin{aligned}
&2 + 1 + 1; 1 + 1 + 1 && \text{if } e_3(K) = 4L_1 + 3L_2,\\
&2 + 2 + 1; 0 + 1 + 1 && \text{if } e_3(K) = 5L_1 + 2L_2,\\
&2 + 2 + 2; 0 + 0 + 1 && \text{if } e_3(K) = 6L_1 + L_2,\\
&3 + 2 + 2 && \text{if } e_3(K) = 7L_1,
\end{aligned}$$

we have $\Sigma R_3(f_i, f_j) = 11, 12, 13$ and 15 respectively. In the first three cases this is the minimum possible value. Now, assume, in the case $e_3(K) = 7L_1$, that the three polynomials in the same class are congruent to $X^2 \pmod 3$. If we replace one of the three Eisenstein polynomials by the polynomial $h(X) = X^2 + 15X + 9$, by Lemma 2.3 we have $R_3(h, f) = 2$ for any Eisenstein polynomial $f(X)$ of degree two. Hence, the total sum $\Sigma R_3(f_i, f_j)$ is equal to 13 in this case; since $i_3(h) = 1$, we have $i_3(K) = 14$.

Also, this example shows that it is not always possible to obtain the minimum value of (2) taking only polynomials with $i_p(f) = 0$.

Restricted to the Galois case, Ore's conjecture seems to reopen. For instance, the Galois number fields K of degree 8 (resp. 14) in which $3 = (\mathrm{P}_1 \cdots \mathrm{P}_4)^2$ (resp. $3 = (\mathrm{P}_1 \cdots \mathrm{P}_7)^2$) have only two possibilities, $e_3(K) = 4L_1$ or $4L_2$ (resp. $7L_1$ or $7L_2$), and in both cases $i_3(K) = 3$ (resp. $i_3(K) = 14$). We believe the following is true.

CONJECTURE 3.5. If $L, L' \in \mathrm{E}$ are Galois and have the same ramification numbers, then $I_p(nL) = I_p(nL')$ for all n.

[1] It is valid although, strictly speaking, we have proved it only in the case $f = 1$.

ACKNOWLEDGEMENTS. The contents of this paper are part of the author's Ph. D. Thesis at the Universitat Autònoma de Barcelona. The author wishes to express his sincere gratitude to Pascual Llorente for his many helpful suggestions and encouragement. The author is also grateful to the referee, Leon McCulloh, for his valuable suggestions concerning the combinatorial results contained in Propositions 2.5 and 2.6 and the remarks following them.

REFERENCES

1. R. Dedekind, *Über den Zusammenhang der Theorie der Ideale und der Theorie der höhere Kongruenzen*, Abh. Königl. Ges. Wiss. Göttingen **23** (1878), 1–23.

2. H. T. Engstrom, *On the common index divisors of an algebraic field*, Trans. Amer. Math. Soc. **32** (1930), 223–237.

3. H. Hasse, *Number theory*, Springer-Verlag, Berlin and New York, 1980.

4. K. Hensel, *Über den grössten gemeinsamen Teiler aller Zahlen welche durch eine ganze Funktion von n Veränderlichen darstellbar sind*, J. Reine Angew. Math. **116** (1896), 350–356.

5. M. Krasner, *Nombre des extensions d'un degreé donné d'un corps* P-*adique*, Coll. Tend. Géom. en Algèbre, Paris, 1966, pp. 143–169.

6. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Monograf. Mat., No. 57, PWN, Warsaw, 1974.

7. Ö. Ore, *Zur Theorie der algebraischen Körper*, Acta Math. **44** (1923), 219–314.

8. _____, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), 84–1117.

9. J. Śliwa, *On the nonessential discriminant divisor of an algebraic number field*, Acta Arith. **42** (1982), 57–72.

10. A. A. Sukallo, *On determination of the index of a field of algebraic numbers*, Rostov. Gos. Univ. Uc. Zap., Fiz.-Mat. Fak. **32** (1955), 37–42. (Russian)

SECCIÓ DE MATEMÀTIQUES, UNIVERSITAT AUTÒNOMA DE BARCELONA, BELLATERRA, BARCELONA, CATALUNYA, ESPANYA