THEOREM. *Equation* (4) *is a necessary and sufficient condition that the two families* $\phi = const.$ *and* $\psi = const.$ *form a net without detours.*

The choice of signs corresponds to the choice of orientation of the two families. If both signs hold, that is, if both sides of (4) vanish identically, then any orientation is possible.

If one of the families, say $\phi = \text{const.}$, is given in the form $M\,du + N\,dv = 0$, then substitution of M and N for ϕ_u and ϕ_v in (4) gives a condition applicable to that case, for at no point was use made of the integrability condition for ϕ_u and ϕ_v.

Equivalent conditions for a net without detours have been given for the plane by Scheffers* and for surfaces by Rothe,† but neither of these writers gives the conditions in the invariant forms (2) and (4).

DARTMOUTH COLLEGE

INDICES IN CUBIC FIELDS‡

BY MARSHALL HALL

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

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0, \tag{1}$$

whose coefficients are rational integers. If d_θ is the discriminant of θ, then $d_\theta = k_\theta^2 d$, where k_θ is a rational integer called the index of θ. The ring of polynomials in θ with rational integral coefficients, $P(\theta)$, is a subring of index k_θ of $R(\theta)$, the ring of algebraic integers of $K(\theta)$. In particular, if $k_\theta = 1$, $P(\theta)$ is identical with $R(\theta)$. Dedekind§ first showed that it is not always possible to find an integer α in a given field such that $k_\alpha = 1$, by exhibiting certain fields of third and fourth degree in which there is a divisor common to the index of every integer of the field. Extensive researches have been made as to what these common index divisors may be for fields of a given degree. For p to be a common index divisor of some field of degree n, the condition $p < n$

* Leipziger Berichte, vol. 57 (1905), p. 353.

† Berliner Mathematische Sitzungsberichte, vol. 7 (1908), pp. 14–15.

‡ Presented to the Society, April 19, 1935.

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

was shown to be sufficient by Bauer* in 1907 and necessary by von Zylinsky† in 1913. H. T. Engstrom‡ has investigated what powers of these primes may occur as common index divisors.

It is an interesting question to ask whether all multiples of this common index divisor occur as indices of properly chosen integers in the field, and more particularly to inquire if, in fields with common index divisor unity, there is an integer whose index is one. By restricting our attention to cubic fields, it is possible to find considerable information on these questions. This paper shows that (a) the indices of integers in a cubic field are precisely the rational integers represented by a homogeneous binary§ cubic called the indicial form, (b) an explicit form can be given for pure cubic fields $K(D^{1/3})$, and (c) there exists a cubic field whose minimum index is greater than any previously assigned number. This last result stands in strong contrast to the known result that the greatest common index divisor of a cubic field is either 1 or 2.

2. *Derivation of the Indicial Form.* Consider a cubic field $K(\theta)$ generated by a root of

$$x^3 + a_1x^2 + a_2x + a_3 = 0, \tag{2}$$

the a's being rational integers. Integers of $K(\theta)$, ω_1, ω_2, and ω_3 are said to form an integral basis for $K(\theta)$ if every integer α of the field may be written as $\alpha = r\omega_1 + s\omega_2 + t\omega_3$ with rational integers r, s, and t.

LEMMA. *$K(\theta)$ has an integral basis of the form $\omega_1 = 1$, $\omega_2 = (\theta + b_1)/k_1$, $\omega_3 = (\theta^2 + b_2\theta + b_3)/(k_1^2 k_2)$, and $k_\theta = k_1^3 k_2$.*

It is well known that every integer of $K(\theta)$ may be written in the form $(A\theta^2 + B\theta + C)/k_\theta$, where the A, B, and C are rational integers. As these integers form a modulus, the A's must

* N. 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.

‡ H. T. Engstrom, *On the common index divisors of an algebraic field*, Transactions of this Society, vol. 32 (1930), pp. 223–237.

§ The form given by K. Hensel in *Arithmetische Untersuchungen über die gemeinsamer ausserwesentlicher Discriminantenteiler einer Gattung*, Journal für Mathematik, vol. 113 (1894), pp. 128–160, would in this case be ternary.

also form a modulus, and consequently must all be multiples of A_1, the least positive A. Let $\omega_3=(A_1\theta^2+B_1\theta+C_1)/k_\theta$ be one of the integers for which A has its least positive value. If α is any integer of $K(\theta)$, then $\alpha=(tA_1\theta^2+B\theta+C)/k_\theta$ and $\alpha-t\omega_3$ is an integer of the form $(B\theta+C)/k_\theta$. These again form a modulus and all such B's are multiples of the least positive one, B_0, say in $\omega_2=(B_0\theta+C_0)/k_\theta$, and so $\alpha-t\omega_3-s\omega_2$ is rational and an integer and hence is some rational integer $r=r\cdot 1=r\omega_1$. Then $\alpha=r\omega_1+s\omega_2+t\omega_3$, and ω_1, ω_2, ω_3 form an integral basis of $K(\theta)$, where $\omega_1=1$, $\omega_2=(B_0\theta+C_0)/k_\theta$, $\omega_3=(A_1\theta^2+B_1\theta+C_1)/k_\theta$. The integers $(B\theta+C)/k_\theta$ include $\theta=k_\theta\theta/k_\theta$, whence k_θ is a multiple of B_0, $k_\theta=B_0k_1$. Hence $\omega_2=(B_0\theta+C_0)/(k_1B_0)$ and $k_1\omega_2-\theta=C_0/B_0$, which must be an integer b_1. This yields $\omega_2=(B_0\theta+B_0b_1)/(k_1B_0)=(\theta+b_1)/k_1$. The integers $(A\theta^2+B\theta+C)/k$ include $\omega_2^2=(\theta^2+2b_1\theta+b_1^2)/k_1^2$, which must be of the type $(k_2A_1\theta^2+B\theta+C)/k_2$, whence, by comparing coefficients of θ^2, we find $k_\theta=k_1^2k_2A_1$. Therefore $\omega_3=(A_1\theta^2+B_1\theta+C_1)/(k_1^2k_2A_1)$, and since $k_2\omega_3-\omega_2^2$ is an integer of the form $(B\theta+C)/k_\theta$, it must be expressible as $r\omega_1+s\omega_2$. Taking $k_2\omega_3=\omega_2^2+r\omega_1+s\omega_2$, we shall have

$$\omega_3=\frac{\omega_2^2+r\omega_1+s\omega_2}{k_2}=\frac{\theta^2+b_2\theta+b_3}{k_1^2k_2}.$$

Moreover

$$k_\theta=\frac{\left|\,1,\ \theta',\ \theta''^2\,\right|}{\left|\,\omega_1,\ \omega_2',\ \omega_3''\,\right|}=k_1^3k_2.$$

We call k_1 the removable index factor of θ, since the index of $\Theta=(\theta+b_1)/k_1$ is k_2.

THEOREM 1. *The indices of the integers of $K(\theta)$ are precisely the rational integers represented by a homogeneous binary cubic, called the indicial form.*

Let α be any integer of $K(\theta)$. Then $\alpha=r\omega_1+s\omega_2+t\omega_3$, where r, s, and t are rational integers. Since the index of $\bar{\alpha}=\alpha-r=s\omega_2+t\omega_3$ is the same as the index of α, we need consider only integers of this form in determining all possible indices of integers in $K(\theta)$.

If

$$\omega_2^2 = c\omega_1 + d\omega_2 + e\omega_3,$$
$$\omega_2\omega_3 = f\omega_1 + g\omega_2 + h\omega_3,$$
$$\omega_3^2 = i\omega_1 + j\omega_2 + k\omega_3,$$

then

$$\bar{\alpha}^2 = s^2\omega_2^2 + 2st\omega_2\omega_3 + t^2\omega_3^2 = (cs^2 + 2fst + it^2)\omega_1 + (ds^2 + 2gst + jt^2)\omega_2 + (es^2 + 2hst + kt^2)\omega_3.$$

Now

$$k_\alpha = k_{\bar{\alpha}} = \frac{|\,1,\ \bar{\alpha}',\ \bar{\alpha}''^2\,|}{|\,\omega_1,\ \omega_2',\ \omega_3''\,|} = \begin{vmatrix} s & , & t \\ ds^2 + 2gst + jt^2, & es^2 + 2hst + kt^2 & \end{vmatrix}.$$

Hence we have

$$k_\alpha = es^3 + (2h - d)s^2t + (k - 2g)st^2 - jt^3. \tag{3}$$

This is called the *indicial form* of the field $K(\theta)$. Since to every α of $K(\theta)$ correspond two rational integers s and t in the representation $\alpha = r\omega_1 + s\omega_2 + t\omega_3$, and since to any two rational integers s and t there corresponds the set of integers $r\omega_1 + s\omega_2 + t\omega_3$, $(r = 0, \pm 1, \pm 2, \cdots)$, it is seen that the indices of the integers of $K(\theta)$ are precisely the rational integers represented by the homogeneous binary cubic (3). The removable index factor, k_1, is the greatest common divisor of s and t. If we divide the integers of $K(\theta)$ into *index classes* so that two integers are in the same index class if and only if their difference is a rational integer, then all integers in the same index class have the same index, and in consequence of the Thue-Siegel Theorem, only a finite number of index classes have the same index.

3. *The Pure Cubics.* Dedekind* has shown that the cubic field $K(D^{1/3}) = K[(ab^2)^{1/3}]$, where $D = ab^2c^3$, with a, b relatively prime and square-free, has a basis 1, $(ab^2)^{1/3}$, $(a^2b)^{1/3}$, if $a^2 \not\equiv b^2 \pmod 9$. If $a^2 \equiv b^2 \pmod 9$, we choose the signs of a and b so that $a \equiv b \equiv 1 \pmod 3$ and a basis is given by $1, (ab^2)^{1/3}, (1 + (ab^2)^{1/3} + (a^2b)^{1/3})/3$.

* R. Dedekind, Werke, vol. 2, p. 158.

Applying the methods of §2, we find that the indicial form is $as^3-bt^3=k_\alpha$ in the first case, and $3as^3+3as^2t+ast^2+[(a-b)/9]t^3=k_\alpha$ in the second case. It is more convenient to write the second $a(3s+t)^3-bt^3=9k_\alpha$. Hence the indices of $K[(ab^2)^{1/3}]$ are represented by ax^3-by^3 or $(ax^3-by^3)/9$ according as $a^2\not\equiv b^2 \pmod 9$ or $a^2\equiv b^2 \pmod 9$.

THEOREM 2. *Given a large positive integer N, it is possible to find a cubic field $K[(ab^2)^{1/3}]$ in which every integer has an index greater than N.*

Since the indicial form is either ax^3-by^3 or $(ax^3-by^3)/9$, it is sufficient to find values of a and b, relatively prime and square-free, such that the form $I=ax^3-by^3$ does not represent any integer $\neq 0$ numerically less than or equal to $9N$.

If $a\equiv 2$, $b\equiv 0 \pmod 7$, then $I\equiv 2x^3\equiv 0, \pm 2 \pmod 7$ and so $I\neq \pm 1$. To exclude $I=\pm 2$ we may take $a\equiv 1$, $b\equiv 0 \pmod{13}$, which yields $I\equiv x^3\equiv 0, \pm 1, \pm 5 \pmod{13}$, whence $I\neq \pm 2$. These conditions also imply $I\neq \pm 3, \pm 4$, leaving $I=\pm 5$ as the least possible value. Take $a\equiv 1$, $b\equiv 0 \pmod{19}$, whence $I\equiv 0, \pm 1, \pm 7, \pm 8 \pmod{19}$ and so $I\neq \pm 5$.

We may continue to exclude values for I indefinitely. To exclude $I=\pm n$, we take a prime $p=3k+1$ not previously used and not dividing n. Then set $a\equiv r$, $b\equiv 0 \pmod p$, where r has a different cubic character from that of $n \pmod p$. Since $I\equiv rx^3 \pmod p$ and we cannot find an x such that $n\equiv rx^3 \pmod p$, we cannot have $I=\pm n$. These congruences have solutions a and b which are relatively prime and square-free. We may take $b=p_1p_2\cdots p_i$ the product of the primes used as moduli, and take a as a prime satisfying the conditions imposed. This will always be possible since the restriction on a is merely that it lie in an arithmetic progression $bn+r$, where $(b, r)=1$.

In practice it is found that such congruences may be combined with greater economy. For $a=31$, $b=7\cdot 13=91$, we have $a^2\not\equiv b^2 \pmod 9$, whence $I=k_\alpha=31x^3-91y^3$. Here $31x^3-91y^3\equiv 0, \pm 3 \pmod 7\equiv 0, \pm 1, \pm 5 \pmod{13}\equiv 0, \pm 1, \pm 2, \pm 4, \pm 8, \pm 16 \pmod{31}$, whence I does not represent any number numerically less than 31. But for $x=1$, $y=0$, we have $k_\alpha=31$, α being $87451^{1/3}$. Hence the minimum index in $K(87451^{1/3})$ is 31.

YALE UNIVERSITY