ON ABELIAN FIELDS*

BY

LEONARD CARLITZ†

1. INTRODUCTION

By Kronecker's‡ Theorem on Abelian fields, all such fields are subfields of cyclotomic fields, that is, fields generated by a root of unity. Abelian fields may then be classified by considering all cyclotomic fields and sorting the subfields in some manner that will exclude repetition. For example this is done, in part at least, by Weber by making use of the notion of *primary* subfields: a subfield of Ω_m, the field generated by a primitive mth root of unity, is a primary subfield if it is not contained in an $\Omega_{m'}$ $(m'<m)$. We here make use of what we shall call *simple*§ (primary) subfields as defined below. If then the (known) discriminants of Abelian fields are set up on this basis, a number of properties of Abelian fields become apparent. In particular is this true of the fields contained in a fixed simple subfield (see §5).

In §6 some results on common index divisors (that is, common inessential discriminantal divisors) are obtained. Using a necessary and sufficient condition valid for any algebraic field it is shown how to derive for the case of Abelian fields very simple criteria that a given rational prime be a common index divisor. The criteria are of two kinds. A typical instance of the first kind is the following.

Let q and l be odd primes such that $l\equiv 1 \pmod q$; let C denote that cyclic subfield of Ω_l that is of degree q. Then a necessary and sufficient condition that a prime $p(p<q)$ be a common index divisor of C is that

$$p^{(l-1)/q} \equiv 1 \pmod q.$$

As an instance of the criteria of the second kind, we quote the following theorem:

Let K be Abelian of degree q^n and type $(1, 1, \cdots)$. *Then if d is the discriminant of K, and if*

---

* Presented to the Society, November 29, 1930; received by the editors March 11, 1932.

† International Research Fellow.

‡ See Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker Vereinigung, vol. 4 (1894–1895),Theorem 131.

§ Called "Ausgangs-Kreiskörper" by M. Gut, *Die Zetafunktion, die Klassenzahl und die Kronecker'sche Grenzformel eines beliebigen Kreiskörpers*, Commentarii Mathematici Helvetici, vol. 1 (1929), p. 160.

(i) p *does not divide* d, $p \leqq q^{n/q}$;

(ii) $p \mid d$,* $p \leqq q^{(n-1)/q}$,

p is surely a common index divisor of K.

We shall suppose in what follows that all the discriminants are *odd* unless the contrary is explicitly stated; this makes for a considerable simplification and avoids listing a great many exceptional cases.

2. Classification

Let m be an integer $\geqq 3$, and let Ω_m be the field defined by a primitive mth root of unity. We suppose the group† G_ϕ of Ω_m exhibited by a reduced residue system (mod m); ϕ stands for $\phi(m)$. Let m be divisible by exactly n (odd) primes:

$$m = q_1^{f_1} \cdots q_n^{f_n};$$

put

$$\phi_i = \phi(q_i^{f_i}) = q_i^{f_i-1}(q_i - 1) \qquad (i = 1, \cdots, n).$$

Let r_i' denote fixed primitive roots (mod $q_i^{f_i}$), respectively, and let r_i be defined (mod m) by

$$(1) \qquad \begin{aligned} r_i &\equiv r_i' \pmod{q_i^{f_i}}, \\ r_i &\equiv 1 \pmod{q_j^{f_j}} \qquad (i \neq j). \end{aligned}$$

Then G_ϕ is generated by $r_1, \cdots, r_n$:

$$(2) \qquad G_\phi = \{r_1, \cdots, r_n\}.$$

We now define a *simple* (primary) subfield of Ω_m as one corresponding‡ to a group

$$(3) \qquad G_\mu = \{r_1^{\nu_1}, \cdots, r_n^{\nu_n}\},$$

where

$$(4) \qquad \phi_i = \mu_i \nu_i, \quad q_i \text{ does not divide } \mu_i \qquad (i = 1, \cdots, n),$$

G_μ is evidently of order $\mu = \mu_1 \cdots \mu_n$, and K, the field corresponding to G_μ, is of degree $\nu = \nu_1 \cdots \nu_n$. That K is indeed primary follows from the second part of equations (4).

It is now a simple matter to exhibit our mode of classification. We notice to begin with that any primary subfield k of Ω_m is contained, properly or

* As usual, read for $a \mid b$, "a divides b."

† Hilbert, loc. cit , p. 248.

‡ Hilbert, loc. cit., p. 250.

improperly, in a *unique* minimal simple subfield of Ω_m; for it is clear from (2) that the greatest common subfield of two simple subfields is itself a simple subfield of Ω_m. Let us then fix our attention on a particular simple subfield K. Choose any maximal subfield k_1 of K. If k_1 is primary (with respect to Ω_m), choose k_2, some maximal subfield of k_1; we continue this process until we arrive either at another simple subfield or else at a k_j none of whose subfields is primary. To illustrate the process, let us classify the primary subfields of Ω_m, $m = 5^3 \cdot 11^2$.

Let r_1, r_2 appertain to $5^2 \cdot 4$, $11 \cdot 10$, respectively (see (1) above). Then, if the group generated by $A, B, \cdots$ be denoted by $\{A, B, \cdots\}$, we get among others the following chains:

I. $\{1\} \sim \Omega_m$,

$$\{r_1^{50} r_2^{55}\} \sim k_1 \text{ of degree } \phi(m)/2,$$

$$\{r_1^{50}, r_2^{55}\} \sim k_2 \text{ (simple) of degree } \phi(m)/4.$$

II. Starting with k_2 we may choose one of

$$\{r_1^{50}, r_2^{55}, r_1^{10} r_2^{11i}\} \sim k_{2i} \text{ of degree } \phi(m)/20 \quad (i = 1, \cdots, 4),$$

or

$$\{r_1^{25}, r_2^{55}\} \sim k_3 \text{ (simple) of degree } \phi(m)/8; \text{ etc.}$$

III. Starting with k_3, we may choose one of

$$\{r_1^{25}, r_2^{55}, r_1^{5} r_2^{11i}\} \sim k_{3i} \text{ of degree } \phi(m)/40 \quad (i = 1, \cdots, 4);$$

no subfield of any k_{3i} is primary.

IV. In place of k_1 (of I) we may take

$$\{r_1^{20} r_2^{22i}\} \sim k_{1i}' \text{ of degree } \phi(m)/5 \qquad (i = 1, \cdots, 4),$$

$$\{r_1^{20}, r_2^{22}\} \sim k_2' \text{ (simple) of degree } \phi(m)/25,$$

and contained in each k_{1i}'.

These four chains will suffice to indicate how the classification may be carried out in any special case; the utility of this method of arrangement will appear below.

3. The discriminants

The form of the discriminant of an Abelian field is known, at least in the sense that the discriminant of any subfield of an Ω_m can be explicitly written

down.* As the explicit expression for the discriminants will be required they will be stated here in the form of lemmas. It is convenient, and indeed leads to an important result, first to calculate the discriminant of an arbitrary simple field, and then proceed to the case of an entirely arbitrary subfield.

LEMMA 1. *The discriminant of a simple primary subfield K of Ω_m is determined by*

$$d(K) = \pm \prod_{i=1}^{n} q_i^{t_i} \tag{5}$$

where

$$t_i = \frac{1}{\mu}\left(\frac{\phi s_i}{\phi_i} - (\mu_i - 1)\frac{\mu\nu}{\mu_i\nu_i}\right),$$

$$s_i = q_i^{f_i-1}(f_i(q_i - 1) - 1), \tag{6}$$

and $\mu_i, \nu_i, \phi_i, \mu, \nu$ are defined by (4).

If now k is any primary subfield of Ω_m, then as seen in §2 it either is itself simple or else is contained in a unique minimal simple subfield. Calling this field K, and assuming all the above notation for a simple field, we get

LEMMA 2. *The relative discriminant of K with respect to k is the unit ideal of k.*

Now by a general theorem†

$$d(K) = d^{\rho}(k)N(D),$$

where ρ is the relative degree of K/k, D is the relative discriminant of K/k, and $N(D)$ denotes the norm in k. Hence Lemmas 1 and 2 immediately imply

LEMMA 3. *The discriminant of an arbitrary primary k is determined by*

$$d(k) = d^{1/\rho}(K) = \pm \prod_{i=1}^{n} q_i^{t_i/\rho},$$

where t_i is defined by (6).

4. THE SUBFIELDS OF A SIMPLE SUBFIELD

Let us fix some K, a simple subfield of Ω_m, defined by equations (3) and (4), say. We shall consider the set of fields $\{k\}$ satisfying the following conditions:

(i) k is a primary subfield of Ω_m;

* See, for example, Gut, loc. cit.

† Hilbert, loc. cit., Theorem 39.

(ii) K is the minimal simple field containing k. We shall call $\{k\}$ the set of fields belonging to K.

By means of Lemma 3, once we have calculated the discriminant of K, we determine at once the discriminant of k, a member of the set of fields belonging to K, if we know merely the relative degree of K/k. Furthermore *if two fields in* $\{k\}$ *have the same degree their discriminants must coincide.* It is not difficult to determine the conditions K must satisfy in order that there be several fields of the set of equal degree; however, we shall consider only the special case of a K of type $(1, 1, \cdots)$.

Let K be an Abelian field of degree q^n and type $(1, 1, \cdots)$, q an odd prime. From Hilbert's proof of Kronecker's Theorem on Abelian fields, we may deduce that K is a subfield of Ω_m, where

$$m = q^2 q_1 \cdots q_t \quad \text{or} \quad m = q_1 \cdots q_t,$$
$$q_i \equiv 1 \pmod{q} \qquad (i = 1, \cdots, t),$$

according as q does or does not divide the discriminant of K. Evidently K is simple only if the number of distinct primes dividing m is equal to n, i.e.

$$m = q^2 q_1 \cdots q_{n-1} \quad \text{or} \quad m = q_1 \cdots q_n.$$

Now if K is not simple, it is readily seen that the simple field to which it belongs is itself of type $(1, 1, \cdots)$. Let us then assume K simple, and for the sake of definiteness let us suppose $q \mid m$. Then if the r_i are defined as in (1), K corresponds to the group $(q_0 = q)$

$$G_\mu = \{r_0^q, \cdots, r_{n-1}^q\}.$$

We can now easily determine the set of fields belonging to K:

(i) Let us consider first *all* the cyclic subfields of K; from a well known result concerning Abelian groups, we see at once that the number of such fields is

$$(q^n - 1)/(q - 1).$$

They may be sorted by considering the number of primes contained in their discriminants. There are first of all n fields whose discriminants contain but a single prime; each corresponds to a subgroup of the type

$$\{r_0^q, r_1, \cdots, r_{n-1}\}.$$

Secondly, there are

$$\binom{n}{2}(q - 1) = \frac{n(n-1)}{2!}(q - 1)$$

fields whose discriminants contain exactly two primes. They fall into $n(n-1)/2$ sets of $(q-1)$ fields, all the fields in a set having the property that their discriminants are divisible by the same primes. Thus a particular set corresponds to

$$\{r_0^q, r_0^{a_1} r_1^{-a_0}, r_1^q, r_2, \cdots, r_{n-1}\},$$
$$a_0, a_1 = 1, \cdots, q-1, \quad a_0 a_1 \equiv 1 \pmod{q}.$$

Thirdly, there are

$$\binom{n}{3}(q-1)^2$$

fields whose discriminants are divisible by exactly three primes; they fall into $n(n-1)(n-2)/6$ sets of $(q-1)^2$ fields each, all the fields in a set having the property that their discriminants contain the same primes. A particular set corresponds to

$$\{r_0^q, r_1^q, r_2^q, r_0^{a_1} r_1^{-a_0}, r_0^{a_2} r_2^{-a_0}, r_3, \cdots, r_{n-1}\},$$
$$a_0, a_1, a_2 = 1, \cdots, q-1, \quad a_0 a_1 a_2 \equiv 1 \pmod{q}.$$

Finally there are

$$\binom{n}{n}(q-1)^{n-1} = (q-1)^{n-1}$$

fields whose discriminants contain all n primes; they comprise a single set of fields. Each field in the set corresponds to a particular*

$$(7) \qquad G^{(a_0, \cdots, a_{n-1})} = \{r_0^q, \cdots, r_{n-1}^q, r_0^{a_1} r_1^{-a_0}, \cdots, r_0^{a_{n-1}} r_{n-1}^{-a_0}\},$$
$$a_i = 1, \cdots, q-1, \quad a_0 a_1 \cdots a_{n-1} \equiv 1 \pmod{q}.$$

It will be convenient for a later application to denote the field corresponding to

$$G^{(a_0, \cdots, a_{n-1})} \text{ by } k^{(a)} = k^{(a_0, \cdots, a_{n-1})}.$$

The fields $k^{(a)}$ are the only primary (cyclic) subfields of K and hence are the only cyclic fields in the set belonging to K.

(ii) To determine $A_n^{(s)}$, the number of fields of degree q^s (and of type $(1, 1, \cdots)$) in the set belonging to K, we notice first that the *total* number of subfields of K of degree q^r (and necessarily of type $(1, 1, \cdots)$) is equal to

* While it may appear from (7) that r_0 plays a special rôle, this is by no means the case. Thus it is easily verified that $G^{(a_0, \cdots, a_{n-1})}$ contains all numbers of the form $r_i^{a_j} r_j^{-a_i}$ and therefore any r_i might be used in place of r_0 in defining the group.

$$\begin{bmatrix} n \\ s \end{bmatrix} = \frac{(q^n - 1) \cdots (q^{n-s+1} - 1)}{(q - 1) \cdots (q^s - 1)}.$$

Then by an argument similar to that employed in the special case (i), we see that

$$\sum_{j=s}^{n} \binom{n}{j} A_j^{(s)} = \begin{bmatrix} n \\ s \end{bmatrix}. \tag{8}$$

To solve (8) for $A_n^{(s)}$ we may proceed thus:

$$\begin{aligned} \sum_{k=s}^{n} (-1)^{n-k} \binom{n}{k} \begin{bmatrix} k \\ s \end{bmatrix} &= \sum_{k=s}^{n} (-1)^{n-k} \binom{n}{k} \sum_{j=s}^{k} \binom{k}{j} A_j^{(s)} \\ &= \sum_{j=s}^{n} (-1)^{n-j} \binom{n}{j} A_j^{(s)} \sum_{k=j}^{n} (-1)^{k-j} \binom{n-j}{k-j} \\ &= \sum_{j=s}^{n} (-1)^{n-j} \binom{n}{j} A_j^{(s)} (1-1)^{n-j} = A_n^{(s)}. \end{aligned} \tag{9}$$

Further transformation of the left member of (9) leads to an unexpected connection between $A_n^{(s)}$ and generalisations of certain important quantities in finite differences. We make use of the formula (the q-generalisation of the binomial theorem)

$$(x+1)(x+q) \cdots (x+q^{s-1}) = \sum_{\alpha=0}^{s} \begin{bmatrix} s \\ \alpha \end{bmatrix} q^{\alpha(\alpha-1)/2} x^{s-\alpha};$$

then

$$\begin{aligned} (q^n - 1)(q^{n-1} - 1) \cdots (q^{n-s+1} - 1) &= q^{-s(s-1)/2} (q^n - 1)(q^n - q) \cdots (q^n - q^{s-1}) \\ &= q^{-s(s-1)/2} \sum_{\alpha=0}^{s} (-1)^{\alpha} \begin{bmatrix} s \\ \alpha \end{bmatrix} q^{\alpha(\alpha-1)/2 + n(s-\alpha)}, \end{aligned}$$

so that

$$\begin{aligned} A_n^{(s)} &= \frac{q^{-s(s-1)/2}}{(q^s - 1) \cdots (q - 1)} \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \sum_{\alpha=0}^{s} (-1)^{\alpha} \begin{bmatrix} s \\ \alpha \end{bmatrix} q^{\alpha(\alpha-1)/2 + k(s-\alpha)} \\ &= \frac{q^{-s(s-1)/2}}{(q^s - 1) \cdots (q - 1)} \sum_{\alpha=0}^{s} (-1)^{\alpha} \begin{bmatrix} s \\ \alpha \end{bmatrix} (q^{s-\alpha} - 1)^n q^{\alpha(\alpha-1)/2}. \end{aligned} \tag{10}$$

Let us think for the moment of q as an arbitrary parameter, and write $[x]$ for the so-called "basic" number

$$(q^x - 1)/(q - 1)$$

which reduces to x when $q = 1$. Further, defining $[m]!$ by

$$[m]! = [m][m-1]\cdots[1],$$

(10) becomes

$$(11)\qquad A_n^{(s)} = (q-1)^{n-s}\frac{q^{-s(s-1)/2}}{[s]!}\sum_{\alpha=0}^{s}(-1)^{\alpha}\begin{bmatrix} s \\ \alpha \end{bmatrix}[s-\alpha]^n q^{\alpha(\alpha-1)/2},$$

which, but for the $(q-1)^{n-s}$, is a q-generalisation of what are sometimes called Stirling numbers.

Before leaving the $A_n^{(s)}$ we derive one other important formula connecting them. From (9)

$$\begin{aligned} A_{n+1}^{(s)} - A_n^{(s-1)} &= \sum_{j=s}^{n+1}(-1)^{n+1-j}\left\{\binom{n+1}{j}\begin{bmatrix} j \\ s \end{bmatrix} - \binom{n}{j-1}\begin{bmatrix} j-1 \\ s-1 \end{bmatrix}\right\} \\ (12)\qquad &= \sum_{j=s}^{n+1}(-1)^{n+1-j}\left\{\binom{n}{j}\begin{bmatrix} j \\ s \end{bmatrix} + \binom{n}{j-1}\begin{bmatrix} j \\ s \end{bmatrix}\right. \\ &\qquad \left. - \binom{n}{j-1}\begin{bmatrix} j-1 \\ s-1 \end{bmatrix}\right\}; \end{aligned}$$

but

$$\begin{bmatrix} j \\ s \end{bmatrix} - \begin{bmatrix} j-1 \\ s-1 \end{bmatrix} = q^s\begin{bmatrix} j-1 \\ s \end{bmatrix},$$

so that the right member of (12) becomes

$$\begin{aligned} &\sum_{j=s}^{n}(-1)^{n+1-j}\binom{n}{j}\begin{bmatrix} j \\ s \end{bmatrix} + q^s\sum_{j=s+1}^{n+1}(-1)^{n+1-j}\binom{n}{j-1}\begin{bmatrix} j-1 \\ s \end{bmatrix} \\ &\qquad = (q^s-1)\sum_{j=s}^{n}(-1)^{n-j}\binom{n}{j}\begin{bmatrix} j \\ s \end{bmatrix}. \end{aligned}$$

Therefore, finally

$$(13)\qquad A_{n+1}^{(s)} = A_n^{(s-1)} + (q^s-1)A_n^{(s)}.$$

5. Simple subfields as relative Abelian fields

We return to the consideration of the general case defined at the beginning of §4, that of a simple subfield K and the set of fields $\{k\}$ belonging to it. By Lemma 2, the relative discriminant of K with respect to any k of $\{k\}$ is the unit ideal of k; further it is clear that K/k is relative Abelian. Let us then for brevity say that K has the property* A with respect to k.

*K is of course part of the Klassenkörper of each k. For definition and proof of the existence of the Klassenkörper of an arbitrary algebraic field, see Furtwängler, Mathematische Annalen, 1907, pp. 1–37; Takagi, Journal of the College of Science, Imperial University of Tokyo, vol. 41 (1920). As no use of the existence of the Klassenkörper is being made here, it is found convenient to use the terminology defined above.

Let $K, k_1, \cdots, k_j$, where the fields $k_1, \cdots, k_j$ are all in $\{k\}$, the set belonging to K, be a chain of fields as in §2. Then it is clear that each k has the property A with respect to any succeeding k of the chain. Conversely, we shall now prove that if any Abelian field F have the property A with respect to a k of the chain, then F itself is a member of the chain, and lies somewhere between K and k (possibly at an end).

By hypothesis the relative discriminant of F/k is the unit ideal of k, so that the only primes dividing the discriminant of F are those dividing the discriminant of k and therefore of Ω_m, the cyclotomic field of which k is a primary subfield. Then F is a primary subfield of an $\Omega_{m'}$, where

$$m = q_1^{f_1} \cdots q_n^{f_n} \text{ and } m' = q_1^{f_1'} \cdots q_n^{f_n'} \qquad (f_i' \geqq f_i). \tag{14}$$

Let K' be that simple subfield of $\Omega_{m'}$ to which F belongs; clearly K' must have the property A with respect to k. Let μ_i, ν_i, μ, ν be the numbers determining K (see (3) and (4)); $\mu_i', \nu_i', \mu', \nu'$ the corresponding numbers for K'. Let ρ be the relative degree of K/k, w the relative degree of K'/k. Now ν, ν' are the degree of K and K', respectively, so that

$$\nu' = \frac{w\nu}{\rho}. \tag{15}$$

By Lemmas 1 and 3, the discriminants of k and K' are

$$\Pi q_i^{t_i/\rho} \text{ and } \Pi q_i^{t_i'},$$

respectively, where

$$t_i = \frac{\nu}{\phi_i}(s_i - \mu_i + 1), \quad t_i' = \frac{\nu'}{\phi_i'}(s_i' - \mu_i' + 1), \tag{16}$$

and s_i, s_i' are defined by (6). If now we use the fact that the relative discriminant of K'/k is the unit ideal,

$$d(K') = d^w(k), \text{ and } t_i' = wt_i/\rho.$$

Using this last equality, together with (15) and (16), we get

$$\frac{s_i - \mu_i + 1}{q_i^{f_i - 1}} = \frac{s_i' - \mu_i' + 1}{q_i^{f_i' - 1}} \qquad (i = 1, \cdots, n),$$

that is,

$$f_i(q_i - 1) - \frac{\mu_i - 1}{q_i^{f_i - 1}} = f_i'(q_i - 1) - \frac{\mu_i' - 1}{q_i^{f_i' - 1}} \quad (i = 1, \cdots, n). \tag{17}$$

Since μ_i and $\mu_i' < q$ it follows from (17), first, that $f_i' = f_i$, and then immediately $\mu_i' = \mu_i$. But this shows that K' and K are identical. We may now state the theorem.

THEOREM 1. *Let K be any simple subfield of Ω_m, and let $\{k\}$ be the set of fields belonging to K. Then K has the property A with respect to each k. Conversely, any Abelian field that has the property A with respect to some k is necessarily a subfield of K.*

Some information about the class number of the fields considered can be derived from this general theorem.* *If F is relative Abelian with respect to G and the relative discriminant of F/G is the unit ideal of G, then the class number of G is divisible by ρ, the relative degree of F/G.* Actually Hilbert proves the theorem only in the case ρ a prime, but as he remarks there is no great difficulty in extending the result to the general case. Hence we obtain

THEOREM 2. *Let k be any primary subfield of Ω_m, and K the minimal simple field containing k. Then if ρ denote the relative degree of K/k, the class number of k is a multiple of ρ.*

6. COMMON INDEX DIVISORS

A rational prime p is called a common index divisor of an arbitrary algebraic field F if, for every integer ω of the field,

$$p \Big| \frac{d(\omega)}{d},$$

where d is the discriminant of F, and $d(\omega)$ that of ω. The following criterion deduced from a result of Dedekind's is given by Hensel.†

Let the prime-ideal decomposition of p in F be

$$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}, \quad N(\mathfrak{p}_i) = p^{f_i}. \tag{18}$$

Let $\psi(f)$ denote the number of primary irreducible polynomials (mod p) *of degree f:*

$$\psi(f) = \frac{1}{f} \sum_{d|f} \mu(d) p^{f/d} = \frac{1}{f}(p^f - \sum p^{f/p_1} + \sum p^{f/(p_1 p_2)} - \cdots). \tag{19}$$

Then a necessary and sufficient condition that p be a common index divisor of F is that, for at least one i,

$$\psi(f_i) < g(f_i),$$

$g(f)$ denoting the number of $\mathfrak{p}$'s in (18) *of degree f.*

---

* Hilbert, loc. cit., Theorem 94.

† Bachmann, *Zahlentheorie* V: *Allgemeine Arithmetik der Zahlenkörper*, 1926, p. 276.

To apply this something must be known about the decomposition of primes in the field to be considered. For an Abelian field this information is given by another theorem of Dedekind's.*

DECOMPOSITION RULE.† *Let Ω_m be a cyclotomic field and F any subfield. Let the group of Ω_m be represented by a reduced residue system* (mod m) *and let (h) denote the subgroup corresponding to F. Let p^k be the highest power of the prime p dividing m, $m = p^k m'$; and let the number of those numbers of (h) that are $\equiv 1 \pmod{m'}$ be $\phi(p^k)/g$, thus defining g. Let f be the smallest positive integer such that*

$$p^f \equiv (h) \pmod{m'}, \tag{20}$$

that is, to one of the numbers in (h). Then the prime-ideal decomposition of p in F is

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_e)^g, \quad N(\mathfrak{p}_i) = p^f,$$

where $e \cdot f \cdot g$ is the degree of F.

We take first the simplest and perhaps the most interesting case, that of a cyclic field C of odd prime degree q and of discriminant divisible by a single prime. Then the discriminant is, by Kronecker's Theorem and Lemma 1, either

$$\text{(a)} \qquad q^{2(q-1)}; \quad \text{or (b)} \qquad l^{q-1},$$

where l is a prime such that $l \equiv 1 \pmod{q}$. By the Decomposition Rule (or directly, using well known theorems on the decomposition of a prime in a Galois field) the condition that a prime p factor in C is either

$$\text{(21) or} \quad \begin{cases} \text{(a)} & p^{q-1} \equiv 1 \pmod{q^2} & (p \neq q); \\ \text{(b)} & p^{(l-1)/q} \equiv 1 \pmod{l} & (p \neq l). \end{cases}$$

Now if p factor in C it factors into q distinct prime ideals (of the first degree). Hence, applying the criterion for common index divisors, and noticing that $\psi(1) = p$, we deduce one of the theorems stated in the Introduction.

THEOREM 3.‡ *Let C be a cyclic field of prime degree q and of discriminant divisible by a single prime. Then a necessary and sufficient condition that a prime $p (p < q)$ be a common index divisor of C is furnished by equations* (21).

---

* Gesammelte Werke, vol. 1, p. 233.

† This theorem is implicitly proved by Gut, loc. cit., §§5 and 8.

‡ For an equivalent criterion for cubic fields see Hensel, Journal für Mathematik, vol. 113 (1894), p. 147.

The necessity of the condition follows from the theorem* that a common index divisor of any field is less than the degree of the field.

Turning now to the case of the general cyclic field C of odd prime degree, we remark first that its discriminant, d, is either

$$\text{(a)}\quad (q^2q_1\cdots q_n)^{q-1};\quad \text{or}\quad \text{(b)}\quad (q_1\cdots q_n)^{q-1};\quad q_i\equiv 1 \pmod q.$$

Using the notation of §4 (i), let C correspond to the group

$$\text{(a)}\qquad G^{(a_0,\cdots,a_n)}\quad \text{or}\quad \text{(b)}\qquad G^{(a_1,\cdots,a_n)}.$$

To determine the condition that a prime p(p does not divide d) factor in C we use the Decomposition Rule. We need consider but one case in detail; let us take case (a). It is plain that $m=q^2q_1\cdots q_n$, and clearly the condition that p factor is that f in (20) be one; or putting

$$p\equiv r_0^{c_0}\cdots r_n^{c_n} \pmod m \qquad (1\leqq c_i\leqq \phi(q_i)) \tag{22a}$$

p factors provided that integers s, t can be found such that

$$r_0^{c_0}\cdots r_n^{c_n}\equiv r_0^{qs_0}\cdots r_n^{qs_n}(r_0^{a_1}r_1^{-a_0})^{t_1}\cdots(r_0^{a_n}r_n^{-a_0})^{t_n} \pmod m.$$

But this congruence is equivalent to the system

$$\begin{aligned} c_0 &\equiv qs_0+a_1t_1+\cdots+a_nt_n && \pmod{\phi(q^2)},\\ c_i &\equiv qs_i-a_0t_i && \pmod{\phi(q_i)} \qquad (i=1,\cdots,n),\end{aligned}$$

which is equivalent to

$$a_0c_0+\cdots+a_nc_n\equiv 0 \pmod q, \tag{23a}$$

the condition sought.

THEOREM 4. *A necessary and sufficient condition that p ($p<q$) be a common index divisor of $C=C^{(a_0,\cdots,a_n)}$ is furnished by* (22a) *and* (23a). *Similarly a necessary and sufficient condition that p($p<q$) be a common index divisor of*

$$C=C^{(a_1,\cdots,a_n)}$$

is furnished by

$$p\equiv r_1^{c_1}\cdots r_n^{c_n} \pmod m, \tag{22b}$$

and

$$a_1c_1+\cdots+a_nc_n\equiv 0 \pmod q. \tag{23b}$$

* Proved by von Zylinski, Mathematische Annalen, vol. 73 (1913), p. 273.

Turning next to the simple field K defined by (3) and (4), the Decomposition Rule shows that if p does not divide $d(K)$,

$$p = \mathfrak{p}_1 \cdots \mathfrak{p}_e, \quad N(\mathfrak{p}_i) = f, \quad ef = \nu;$$

and

$$f \mid \omega, \ \omega = \text{L.C.M.}(\nu_1, \cdots, \nu_n).$$

If then $\psi(f)$, the number of primary irreducible polynomials (mod p) of degree f, is less than e, p is a common index divisor of K. But evidently

$$\psi(f) \leqq p^f \leqq p^\omega;$$

and

$$e = \frac{\nu}{f} \geqq \frac{\nu}{\omega}.$$

If then $\omega p^\omega < \nu$, surely $\psi(f) < e$. Hence we have

THEOREM 5. *Let K be the simple field of degree ν defined by* (3) *and* (4). *If p does not divide $d(K)$, and*

$$\omega p^\omega < \nu, \ \omega = \text{L.C.M.}(\nu_1, \cdots, \nu_n), \tag{24}$$

then p is surely a common index divisor of K. The inequality (24) *may be replaced by the weaker condition*

$$\omega \cdot \max_{f \mid \omega} \psi(f) < \nu. \tag{24}'$$

Theorem 5 could without much difficulty be refined in several directions. And it would also be possible to frame a great many theorems analogous to Theorem 4 for various kinds of Abelian fields. However we shall limit ourselves to the case of fields of type $(1, 1, \cdots)$. Assume first that the prime p does not divide the discriminant of the field. Then by the Decomposition Rule or directly it may easily be shown that either

(i) $\quad p = \mathfrak{p}_1 \cdots \mathfrak{p}_{q^n}$, each $\mathfrak{p}$ of degree 1;

or

(ii) $\quad p = \mathfrak{p}_1 \cdots \mathfrak{p}_{q^{n-1}}$, each $\mathfrak{p}$ of degree q;

the field being of degree q^n. If p divides the discriminant, we get, in place of (i) and (ii),

(iii) $\quad p = (\mathfrak{p}_1 \cdots \mathfrak{p}_{q^{n-1}})^q$, each $\mathfrak{p}$ of degree 1;

or,

(iv) $$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_{q^{n-2}})^q, \text{ each } \mathfrak{p} \text{ of degree } q.$$

Now

$$\psi(1) = p, \text{ and } \psi(q) = \frac{p^q - p}{q}.$$

Application of the Hensel criterion leads to

THEOREM 6. *Let K be of degree q^n and type $(1, 1, \cdots)$. Then if*

(i) $$p \text{ does not divide } d(K), \quad p \leqq q^{n/q};$$

or

(ii) $$p \mid d(K), \qquad p \leqq q^{(n-1)/q},$$

p is surely a common index divisor of K.

It is perhaps worth remarking that in Theorem 6 either q or $d(K)$ may be even.

Theorem 6 evidently implies that, if q be fixed, then, for sufficiently large n, an assigned prime p will be a common index divisor in any field of type $(1, 1, \cdots$ to n units). Thus for example the primes 2, 3, 5, 7 are common index divisors of

$$k((-3)^{1/2}, 5^{1/2}, (-11)^{1/2}, 13^{1/2}, 17^{1/2}, (-19)^{1/2}).$$

We consider finally a refined form of Theorem 6 for the case in which the (odd) discriminant is divisible by exactly n primes. The field is then simple. To determine the decomposition of rational primes in such a field we could of course apply once more the decomposition rule. It is however somewhat simpler and perhaps more interesting to proceed differently. The field K under consideration is, by Kronecker's Theorem, composed of the n cyclic fields $C(q_i)$, each of degree q and of discriminant a power of q_i. Here q_i is either a prime $\equiv 1 \pmod q$; or, if $q \mid d(K)$, one of them is q^2. From Theorem 3 we already know when a prime $p (p \neq q_i)$ will factor in $C(q_i)$; as for q_i we have of course (in $C(q_i)$) either

$$q_i = \mathfrak{q}^q,$$

or

$$q = \mathfrak{q}^q \text{ for } q_i = q^2.$$

Now p may decompose in K in one of four possible ways (see the proof of the preceding theorem). It is now fairly clear that if p does not divide $d(K)$, and

(25) $$p^{\phi(q_i)/q} \equiv 1 \pmod{q_i} \quad \text{for} \quad i = 1, \cdots, n,$$

then

$$p = \mathfrak{p}_1 \cdots \mathfrak{p}_q{}^n, \quad N(\mathfrak{p}_i) = p;$$

if (25) fails for at least one i, then

$$p = \mathfrak{p}_1 \cdots \mathfrak{p}_q{}^{n-1}, \quad N(\mathfrak{p}_i) = p^q;$$

if $p \mid d(K)$, and

$$(25)' \qquad p^{\phi(q_i)/q} \equiv 1 \pmod{q_i},$$

for all i such that p does not divide q_i, then

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_q{}^{n-1})^q, \quad N(\mathfrak{p}_i) = p;$$

but if (25)′ fail for at least one i, then

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_q{}^{n-2})^q, \quad N(\mathfrak{p}_i) = p^q.$$

We are now able to apply the Hensel criterion and we have at once

THEOREM 7. *Let K be of degree q^n and type $(1, 1, \cdots)$; and let $d(K)$ be divisible by exactly n primes. Let p be a prime $<q^n$; then if p does not divide $d(K)$, and*

(i) *if* (25) *hold, p is a common index divisor;*

(ii) *if* (25) *fails for at least one i, then p is a common index divisor only if*

$$p^q - p < q^n;$$

if $p \mid d(K)$, and

(iii) *if* (25)′ *hold, p is a common index divisor if*

$$p < q^{n-1};$$

(iv) *if* (25)′ *fails for at least one i, then p is a common index divisor only if*

$$p^q - p < q^{n-1}.$$

CAMBRIDGE UNIVERSITY,
CAMBRIDGE, ENGLAND