PACIFIC JOURNAL OF MATHEMATICS
Vol. 85, No. 2, 1979

ARITHMETIC PROPERTIES OF THE IDÈLE DISCRIMINANT

DONALD MAURER

A theorem of Hecke asserts that the discriminant $\mathfrak{d}_{K/F}$ of an extension of algebraic number fields K/F is a square in in the absolute class group. In 1932 Herbrand conjectured the following related theorem and was able to prove it for metacyclic extensions: If K/F is normal, then $\mathfrak{d}_{K/F}$ can be written in the form $\mathfrak{A}^2(\theta)$, $\theta \in F$; where (i) $\theta \equiv 1 \pmod{\mathfrak{B}}$, $\mathfrak{B}$ is the greatest divisor of 4 which is prime to $\mathfrak{d}_{K/F}$, and (ii) $\theta > 0$ at each real prime υ except when $K \otimes_F F_\upsilon$ is a direct sum of copies of the complex field and $(K:F) \equiv 2 \pmod 4$.

More recently, A. Fröhlich gave a unified treatment of these and related questions using the concept of an idèle discriminant. The purpose of this paper is to present a generalization of these results with some connections with the structure of the Galois group.

Our notation will be as follows. Let $\mathscr{M}_F$ denote the finite prime divisors of F. The ring of integers in F will be denoted by $\mathfrak{O}$ (or $\mathfrak{O}_F$), and for each $\upsilon \in \mathscr{M}_F$, $\mathscr{O}_\upsilon$ will be the integers of the completion F_υ. Also, for $\alpha \in F_\upsilon$ we write $\upsilon(\alpha)$ for the order of α, so that if the prime ideal $\mathfrak{P}_\upsilon$ of $\mathfrak{O}_\upsilon$ is generated by π_υ, then $\upsilon(\pi_\upsilon) = 1$. If x is an idèle with υ-component x_υ, then we shall write $x = (x_\upsilon)$, and $\upsilon(x) = \upsilon(x_\upsilon)$. If $\alpha \in F^*$ then, unless otherwise stated, (α) will denote the principal idèle defined by $\alpha_\upsilon = \alpha$. The idèle group J_F contains, as a subgroup, the unit idèles U_F consisting of those x such that $x_\upsilon \in U_\upsilon$, the unit group in F_υ, for all υ. The idèle discriminant $d(K/F)$ defined in [1] is an element of J_F/U_F^2. The classical ideal discriminant is simply the ideal naturally determined by $d(K/F)$.

1. The general theory.

Throughout the paper, p will be a fixed prime, and we shall assume that F contains ζ_p, a primitive pth-root of unity.

Our first results pertain to the case of cyclic p-extensions K/F. Let G denote the Galois group.

LEMMA 1.1. *Let K/F be cyclic of degree p. Then there is an element $\alpha \in F$ such that $K = F(\alpha^{1/p})$ and $\alpha \equiv 1 \pmod{\mathfrak{B}}$, where $\mathfrak{B}$ is the greatest divisor of $(\zeta_p - 1)^p$ which is relatively prime to the discriminant $\mathfrak{d}_{K/F}$. Moreover, υ splits in K if and only if $\alpha \in F_\upsilon^p$.*

Proof. For each $\upsilon \in \mathscr{M}_F$, let $K_\upsilon = K \otimes_F F_\upsilon$; then K_υ is algebra-isomorphic to a direct product $\prod_{\omega/\upsilon} K_\omega$ of local field extensions K_ω/F_υ. Similarly, if we let $(\mathfrak{O}_K)_\upsilon = \mathfrak{O}_K \otimes_{\mathfrak{o}} \mathfrak{O}_\upsilon$, then $(\mathfrak{O}_K)_\upsilon = \prod_{\omega/\upsilon} \mathfrak{O}_\omega$. Let $\mathscr{P}$ be the set of all υ which divide p (i.e., $\upsilon(p) > 0$) but do not divide $\mathfrak{d}_{K/F}$. Then for each $\upsilon \in \mathscr{P}$, K_υ is nonramified, and so K_υ has a normal $\mathfrak{O}_\upsilon$-integral basis $\{x_g^{(\upsilon)}\}_{g \in G}$. By the strong approximation theorem, it is then possible to find a normal F-basis $\{x_g\}_{g \in G}$ of K which is an $\mathfrak{O}_\upsilon$-integral basis of $(\mathfrak{O}_K)_\upsilon$ at each $\upsilon \in \mathscr{P}$. Moreover, we may also assume that $\sum_{g \in G} x_g = 1$.

Now for each character $\chi: G \to \boldsymbol{C}$ (the complex field) set $\theta_\chi = \sum_{g \in G} \chi(g) x_g$. It is well known that $\alpha_\chi = \theta_\chi^p \in F$, and $K = F(\alpha^{1/p})$ for a nontrivial χ. Fix such a χ, and write $\alpha = \alpha_\chi$. We have

$$\theta_\chi = 1 + \sum_{g \neq 1} (\chi(g) - 1) x_g \ .$$

But in the field $\boldsymbol{Q}_p$ of the pth roots of unity over the rational field we can write

$$\chi(g) - 1 = c_\chi(\zeta_p - 1) \qquad (c_\chi \text{ integral in } \boldsymbol{Q}_p) \ .$$

Hence $\theta_\chi = 1 + h'_\chi(\zeta_p - 1)$ with $h'_\chi \in K$. It follows that $\alpha = 1 + h_\chi(\zeta_p - 1)^p$ with $h_\chi \in F$. Moreover, if $\upsilon \in \mathscr{P}$, then $h_\chi \in \mathfrak{O}_\upsilon$. Thus the lemma is proved.

We continue to suppose that K/F is a cyclic p-extension. For $\upsilon \in \mathscr{M}_F$, let G_i denote the ith ramification group of a localization K_ω/F_υ. We define the ramification number r_υ to be the smallest integer n such that G_n is trivial. Clearly r_υ is independent of ω. Now υ is nonramified, tamely ramified, or wildly ramified according as $r_\upsilon = 0$, $r_\upsilon = 1$ or $r_\upsilon > 1$ respectively. If $(K: F) = p$, then the ramification numbers r_υ give a complete description of ramification, and $\upsilon(d(K/F)) = r_\upsilon(p - 1)$.

The next lemma gives a partial determination of the ramification numbers r_υ when $(K: F) = p$.

LEMMA 1.2. *Suppose $K = F(\alpha^{1/p})$ with $\alpha \in F$. If υ is ramified and $\upsilon(\alpha) \not\equiv 0 \pmod p$, then $r_\upsilon = 1$ or $\upsilon(\zeta_p - 1)p + 1$.*

Proof. Set $s = \upsilon(\zeta_p - 1)$. If υ is tamely ramified, the lemma is obvious. Therefore we may suppose that υ is wildly ramified; so p divides the ramification number of υ when extended to K, but $\upsilon(\alpha) \not\equiv 0 \pmod p$. Then let $\alpha^{1/p} = \varepsilon\pi_\omega^a$, where ω is the extension of υ to K, π_ω a local prime, $\varepsilon \in U_\omega$ and $(a, p) = 1$. Now there is a $\gamma \in U_\upsilon$ such that $\zeta_p = 1 - \gamma\pi_\upsilon^s$, and an element $\sigma \in \mathrm{Gal}\,(K_\omega/F_\upsilon)$ such that

$$\zeta_p = \frac{\sigma(\alpha^{1/p})}{\alpha^{1/p}} = \left(\frac{\sigma(\pi_\omega)}{\pi_\omega}\right)^a \frac{\sigma(\varepsilon)}{\varepsilon} .$$

Since π_ω^r ($r = r_\upsilon$) is the highest power of π_ω which divides $\sigma(\pi_\omega) - \pi_\omega$, it follows that

$$\frac{\sigma(\pi_\omega)}{\pi_\omega} \in U_{r-1} - U_r ,$$

where $U_m = 1 + \mathfrak{P}_\upsilon^m$. Since $(a, p) = 1$, it is also true that

$$\left(\frac{\sigma(\pi_\omega)}{\pi_\omega}\right)^a \in U_{r-1} - U_r .$$

But $\sigma(\varepsilon)/\varepsilon \in U_r$, whence it follows that $\zeta_p = 1 - \gamma'\pi_\omega^{ps}$ belongs to $U_{r-1} - U_r$.

This completes the proof.

It is not possible to say much about r_υ when $\upsilon(\alpha) \equiv 0 \pmod p$. A slight modification of the previous argument shows that $r_\upsilon \leqq sp$. However, if n is any integer in the range $0 < n \leqq sp$, then according to [5] or [7], for a $y \in F_\upsilon$ with $\upsilon(y) = 1 - n$, the roots of

$$x^p - x - y = 0$$

generate a cyclic extension of degree p with $r_\upsilon = n$.

Let K/F be cyclic of degree p, then a divisor $\upsilon \in \mathscr{M}_F$ will be called *exceptional at* K/F if the congruence $\upsilon(\alpha)\cdot x \equiv r_\upsilon \pmod p$ does *not* have a solution relatively prime to p. That is, υ is exceptional if one, but not both, of $\upsilon(\alpha)$ or r is congruent to $0 (\mathrm{mod}\, p)$. Suppose $\upsilon(\alpha) \not\equiv 0 (\mathrm{mod}\, p)$, but $r_\upsilon \equiv 0 (\mathrm{mod}\, p)$. By Lemma 1.2 $r_\upsilon = 0$, and so K_υ/F_υ is nonramified. Since α is a pth power in K, p must divide $\upsilon(\alpha)$, a contradiction. Hence υ is exceptional if and only if it is totally ramified, and $\upsilon(\alpha)\cdot x \equiv r \pmod p$ is *not* solvable, i.e., $\upsilon(\alpha) \equiv 0 (\mathrm{mod}\, p)$ but $r_\upsilon \not\equiv 0 (\mathrm{mod}\, p)$.

Now let K/F be any finite Galois extension such that $(K: F)$ is divisible by p. In order to state the main theorem, it will be convenient to introduce two functions $\phi_{K/F}$ and $\psi_{K/F}$ on $\mathscr{M}_F$. Suppose K/F is a p-extension, and let T be a subfield such that $(K: T) = p$. We define $\phi_{K/F}(\upsilon) = 0$ unless υ is totally ramified in K/F, and K/T is exceptional at the extension ω of υ to T. In the latter case, $\phi_{K/F}(\upsilon)$ is to be the least positive residue $(\mathrm{mod}\, p)$ of $-r_\omega$. This definition is independent of the choice of T. For suppose that T' also satisfies the condition $(K: T') = p$. We may suppose that υ is totally ramified. The tower formula applied to the localization at υ gives (since υ is totally ramified, we can identify ω and υ when convenient)

$$N(d(K_\upsilon/T_\upsilon)) \equiv N'(d(K_\upsilon/T'_\upsilon)) (\mathrm{mod}\, p) ,$$

where N and N' are the obvious norm maps. Recalling that $\omega(d(K/T)) = r_\omega(p-1)$, this congruence then implies $\phi_{K/F}$ is well defined.

Now we extend our definition to the general case by letting L be the fixed field of a p-Sylow group G_p. We define $\phi_{K/F}$ to be the least nonnegative residue (mod p) of the expression $(L: F)\phi_{K/L}(\omega)/e_{L/F}(\upsilon)$, where ω extends υ to L, and $e_{L/F}(\upsilon)$ denotes the ramification index of υ in L. Again, it can be verified that this definition is independent of the choice of either L or ω. If K/F is finite Galois, we say υ is *exceptional* at K/F if $\phi_{K/F}(\upsilon) \neq 0$. This extends the earlier definition.

The function ψ is defined in a similar manner. If $(K: F) = p$, then $\psi_{K/F}(\upsilon) = 1$ for all exceptional υ. Otherwise $\psi_{K/F}(\upsilon)$ is the least positive residue (mod p), satisfying the congruence $\upsilon(\alpha)\cdot\psi_{K/F}(\upsilon) \equiv r_\upsilon (\mathrm{mod}\, p)$, where $K = F(\alpha^{1/p})$. In the general case, if G_p is cyclic, let T be a subfield such that $(K: T) = p$ and define $\psi_{K/F}(\upsilon) = \psi_{K/T}(\omega)$, where ω extends υ to T. If G_p is noncyclic, define $\psi_{K/F}(\upsilon) = 1$ for all υ. The definition is independent of T, ω or α. We can now state the main theorem of this section.

THEOREM 1.3.[1] *Let $\zeta_p \in F$, and suppose K/F is a finite Galois extension whose group G contains a nontrivial p-Sylow group G_p. Then there are idèles a, b and c in J_F such that*

$$d(K/F) \equiv a^p bc (\mathrm{mod}\ U_F^2) .$$

Moreover, the following conditions are satisfied for all $\upsilon \in \mathscr{M}_F$.

(i) *$c_\upsilon = \theta^{\psi(\upsilon)} (\psi = \psi_{K/F})$ for some $\theta \in F$ satisfying the congruence $\theta \equiv 1 (\mathrm{mod}\ \mathfrak{B})$, where $\mathfrak{B}$ is the greatest divisor of $(\zeta_p - 1)^p$ which is prime to $\mathfrak{d}_{K/F}$.*

(ii) *If υ is exceptional, $\upsilon(c) \equiv 0 (\mathrm{mod}\ p)$*

(iii) *If G_p is noncyclic, then $\theta = 1$. Moreover, if K/F is a cyclic p-extension, a nonramfied υ prime to p splits in K/F if and only if $\theta \in U_\upsilon^p$.*

(iv) $b_\upsilon = \pi_\upsilon^{\phi(\upsilon)} (\phi = \phi_{K/F})$.

We do not deal with the infinite components of $d(K/F)$, for when $p = 2$ this is discussed in [1]; and for $p > 2$, $F_\upsilon = C$ for all infinite υ, whence $d(K/F)_\upsilon$ is trivial. The remainder of this section is devoted to proving the theorem, while in the final section some consequences are discussed. In particular, the case $p = 2$ is developed.

We first deal with p-extensions, so let $(K: F) = p^m$. If $m = 1$, let $K = F(\alpha^{1/p})$, where α satisfies the congruence condition of Lemma

[1] Results of a similar nature, although somewhat weaker, can be proved without the restriction $\zeta_p \in F$.

1.1. A field basis for K is then $1, \gamma, \gamma^2, \cdots, \gamma^{p-1}$ with $\gamma = \alpha^{1/p}$. Therefore $d(K/F)$ will have a local representation at υ of the form

$$d(K/F)_\upsilon \equiv (-1)^{p(p-1)/2} p^p \beta_\upsilon^2 \alpha^{p-1} (\mathrm{mod}\ U_\upsilon^2) ,$$

for some $\beta_\upsilon \in F_\upsilon$. Using the relation $\upsilon(d(K/F)) = r_\upsilon(p-1)$, this gives the congruence $2\upsilon(\beta_\upsilon) \equiv -r_\upsilon + \upsilon(\alpha) (\mathrm{mod}\ p)$. Hence there is a function $\phi'_{K/F}$ which satisfies the congruence equation $2\phi' \equiv \phi (\mathrm{mod}\ p)$. In particular if $p = 2$, then $\phi \equiv 0$ and so there are no exceptional primes. Now if υ is exceptional, then our result implies that $\beta_\upsilon = \varepsilon_\upsilon \pi_\upsilon^{\phi'(\upsilon)}$ for some unit ε_υ. On the other hand, if υ is nonexceptional, then $\upsilon(\alpha) \cdot \psi(\upsilon) \equiv r_\upsilon (\mathrm{mod}\ p)$. Therefore in the above representation for $d(K/F)_\upsilon$ we can replace α by $\alpha^{\psi(\upsilon)}$. Again, β_υ is of the form $\varepsilon_\upsilon \pi_\upsilon^{\phi'(\upsilon)}$. Thus we obtain the global idèle representation

$$d(K/F) \equiv \delta^p \beta^2 \tau^{p-1} (\mathrm{mod}\ U_F^2) ,$$

where each component of β is given by $\beta_\upsilon = \varepsilon_\upsilon \pi_\upsilon^{\phi'(\upsilon)}$, and $\tau_\upsilon = \alpha^{\psi(\upsilon)}$. Moreover, for all nonramified υ, $\alpha \in U_\upsilon^p$ if and only if υ splits in K.

This representation can be generalized to any cyclic p-extension. There is a sequence of subfields

$$F = \Omega_0 \subset \Omega_1 \cdots \subset \Omega_r \subset \Omega_{r+1} = K$$

with $(\Omega_i : \Omega_{i-1}) = p$. For notational simplicity we set $T = \Omega_r$. According to our previous arguments, we have the representation $d(K/T) \equiv \delta_T^p \beta_T^2 \tau_T^{p-1} (\mathrm{mod}\ U_T^2)$. The tower formula gives $d(K/F) \equiv \delta^p \beta^2 \tau^{p-1} (\mathrm{mod}\ U_F^2)$, where $\beta = N_{T/F}(\beta_T)$ and $\tau = N_{T/F}(\tau_T)$. By a straightforward computation, $\beta_\upsilon = \varepsilon_\upsilon \pi_\upsilon^{\phi'(\upsilon)} (\phi' = \phi'_{K/F})$. Similarly, if we define $\alpha = N_{T/F}(\alpha_T)$, then $\tau_\upsilon = \alpha^{\psi(\upsilon)} (\psi = \psi_{K/F})$.

Suppose that υ divides p but not $\mathfrak{d}_{K/F}$. Then an extension ω of υ to T also divides p but not $\mathfrak{d}_{K/T}$; therefore in $\mathfrak{O}_\omega$, $\alpha_T = 1 + h_\omega(\zeta_p - 1)^p$. Since T/F is normal, we have

$$N_{\omega/\upsilon}(\alpha_T) = \prod_\sigma (1 + \sigma(h_\omega)(\zeta_p - 1)^p) ,$$

where σ runs through the elements of the Galois group of T_ω/F_υ. Hence it follows that $\alpha = 1 + h_\upsilon(\zeta_p - 1)^p$ is in $\mathfrak{O}_\upsilon$.

Now we must show that if υ is nonramified in K, and prime to p, then υ splits if and only if $\alpha \in U_\upsilon^p$. Suppose that such a υ does *not* split in K. Then $\alpha_T \notin T_\upsilon^p$. In general if U_i denotes the unit group of $(\Omega_i)_\upsilon$, we have $(U_i : U_i^p) = p$, so that the norm map induces an isomorphism $U_{i+1}/U_{i+1}^p \cong U_i/U_i^p$; hence $\alpha \notin U_\upsilon^p$. Since there are infinitely many primes which do not split in K/F, α cannot be a pth power, and therefore $(F(\alpha^{1/p}) : F) = p$.

Now a nonramified υ will split in K/F if and only if it splits in Ω_1/F, for if it splits in K, then the decomposition field contains Ω_1, whence υ also splits in Ω_1/F. Hence if ν splits in Ω_1, then it splits in K and so also in $F(\alpha^{1/p})$; therefore $F(\alpha^{1/p}) = \Omega_1$. This proves our assertion, and extends the representation of the idèle discriminant to arbitrary cyclic p-extensions.

Suppose now that K/F is a noncyclic p-extension. The Galois group G must contain a proper noncyclic subgroup. For suppose a maximal subgroup N is cyclic. Let a be a generator of N and choose b not in N. Then p is the smallest positive integer m such that $b^m \in N$. It follows that G is generated by a and b. The subgroup generated by a^p and b is proper and noncyclic. By a simple induction argument we conclude that G contains a subgroup H of type (p, p).

Let L be the fixed field of H. Then there is a subfield $K \supset T \supset L$ such that $K = T(\mu^{1/p})$ with $\mu \in L$. As before, $d(K/T)$ has a representation of the form $\delta_T^p \beta_T^2 \tau_T^{p-1}$, where each component of τ_T is a power of μ. Since $N_{T/L}(\mu) = \mu^p$, the tower formula gives for each $\omega \in \mathscr{M}_L$ the representation $d(K/L)_\omega \equiv \delta_\omega^p \beta_\omega^2 (\text{mod } U_\omega^2)$, where $\beta_\omega = \varepsilon_\omega \pi_\omega^{\phi'(\omega)} (\phi' = \phi'_{K/L})$. The tower formula applied to $K \supset L \supset F$ then gives a representation of $d(K/F)$ of the form $\delta^p \beta^2 \tau^{p-1}$, with $\beta_\upsilon = \varepsilon_\upsilon \pi_\upsilon^{\phi'(\upsilon)}$ and $\tau_\upsilon = 1$ for all $\upsilon \in \mathscr{M}_F$.

This representation generalizes to arbitrary extensions K/F by applying the tower formula to $K \supset L \supset F$, where L is the fixed field of a p-Sylow subgroup of G. To obtain the theorem, we now take $b_\upsilon = \pi_\upsilon^{\phi(\upsilon)}$ and $\theta = (N_{L/F}(\alpha))^{p-1}$, or $\theta = 1$ depending on whether G_p is cyclic or noncyclic. If G_p is cyclic, then

$$\begin{aligned} \upsilon(c) &\equiv -\psi(\upsilon) \cdot \upsilon(N_{L/F}(\alpha)) \\ &\equiv \frac{(L\colon F)}{e_{L/F}(\upsilon)}(-\psi(\omega) \cdot \omega(\alpha))(\text{mod } p)\ , \end{aligned}$$

where ω extends υ to L. For an exceptional υ, $\omega(\alpha) \equiv 0(\text{mod } p)$. It is therefore clear that

$$\upsilon(c) \equiv 0(\text{mod } p)\ .$$

The proof of the theorem is now complete.

2. Applications.

The purpose of this section is to consider some consequences of Theorem 1.3. We first suppose that $p = 2$. Then there is no restriction on the ground field F, since $\zeta_p = -1$ always belongs to F. Fröhlich [1] defined the *discriminant field* Ω/F of an extension K/F as a quadratic subfield ($\Omega = F$ possible) uniquely characterized by the relation

$$d(K/F) \cdot J_F^2 = d(\Omega/F) \cdot J_F^2\ .$$

Hence $\Omega = F(\theta^{1/2})$. We use the properties of Ω to prove

THEOREM 2.1. *The 2-Sylow groups of the Galois group G of an even degree extension K/F are cyclic if and only if* $d(K/F) \notin J_F^2/U_F^2$.

Proof. Suppose a 2-Sylow subgroup G_2 is cyclic. Then G_2 has a normal 2-complement N so that $G/N \cong G_2$. Let L be the fixed field of N. Then the tower formula yields $d(L/F)J_F^2 = d(\Omega/F)J_F^2$, so that by Fröhlich's characterization, $\Omega \subset L$.

Now $\theta \equiv 1(\mathrm{mod}\, F^2)$ implies that almost all v split in L, whence G_2 cannot be cyclic. The converse, of course, is contained in Theorem 1.3.

REMARK. An independent proof is given in [2]. Also, a proof when G is abelian appears in [6].

We now prove two further results for $p = 2$.

THEOREM 2.2. *If K/F is normal and nonramified, and G contains a noncyclic 2-Sylow group, then $\mathfrak{O}_K$ has an $\mathfrak{O}_F$-integral basis.*

Proof. Immediate from Theorem 2.1 and Theorem 2.5 of [1].

THEOREM 2.3. *If K/F is a Galois extension and $d(K/F) \notin J_F^2/U_F^2$, then G is solvable.*

Proof. Since θ is not a square, the degree $(K\colon F)$ must be even since $(\Omega\colon F) = 2$. Therefore by Theorem 2.1 the 2-Sylow groups are cyclic. Hence any such subgroup G_2 has a normal 2-complement N with $G/N \cong G_2$. Since both N and G_2 are solvable, G is itself solvable.

For the remainder of the section, consider an arbitrary prime $p \geqq 2$. This now imposes a restriction on F. Moreover, if $p > 2$ then θ is not determined, up to a pth power, by $d(K/F)$, as was the case when $p = 2$. Hence the notion of a discriminant field does not extend to an arbitrary prime. Also, the exceptional primes, which play no role in the $p = 2$ theory, are now important. The results for $p > 2$ are therefore not as strong as these obtained for $p = 2$.

However, we have the following generalization of Herbrand's theorem.

THEOREM 2.4. *Assuming the hypotheses of Theorem 1.3, then $\mathfrak{d}_{K/F}$ can be written as a product of ideals in the form $\mathfrak{A}^p\mathfrak{D}(\theta)$, where $\theta \equiv 1(\mathrm{mod}\, \mathfrak{B})$, and $\mathfrak{B}$ is the greatest divisor of $(\zeta_p - 1)^p$, prime to $\mathfrak{d}_{K/F}$; $\mathfrak{D}$ is divisible only by ramified primes and is characterized by the relations*

$$\upsilon(\mathfrak{D}) = \begin{cases} \phi_{K/F}(\upsilon) & \text{if } \upsilon \text{ is exceptional} \\ -\upsilon(\theta) - \dfrac{(L\colon F)}{e_{L/F}(\upsilon)} & \text{if } \upsilon \text{ is ramified, nonexceptional} . \end{cases}$$

Proof. In the representation of Theorem 1.3, let the idèle d be defined by $d_\upsilon = 1$ at all infinite divisors, and $d_\upsilon = \pi_\upsilon^{\phi(\upsilon)}\theta^{\psi(\upsilon)-1}$ at all $\upsilon \in \mathscr{M}_F$. Let $\mathfrak{D}$ be the ideal naturally determined by d; then $\upsilon(\mathfrak{D}) = \phi(\upsilon) + \upsilon(\theta)(\psi(\upsilon) - 1)$. The computations are straightforward, using the congruence relation at the end of the previous section.

Since $\phi \equiv 0$ and $\psi \equiv 1$ when $p = 2$, it is evident that, for $\upsilon \in \mathscr{M}_F$ at least, this result is consistent with Herband's theorem.

If the exceptional divisors are known, b can be determined from $d(K/F)$, for a consequence of the representation theorem is that for an exceptional divisor υ, $\phi_{K/F}(\upsilon) \equiv d(K/F) (\mathrm{mod}\, p)$. In this case, the next result gives a sufficient condition for G_p to be cyclic.

THEOREM 2.4. *Under the hypotheses of Theorem* 1.3, *suppose that*

$$d(K/F) \equiv a_1^p b c_1 (\mathrm{mod}\ U_F^2) ,$$

where b is as determined in Theorem 1.3. *Then G_p is cyclic if $c_1 \notin U_F^2 J_F^p$. If K/F is a cyclic p-extension, then a necessary condition for υ to split in K is that $c_{1\upsilon} \in U_\upsilon^2 F_\upsilon^p$.*

Proof. Let c be determined as in Theorem 1.3. Then $c_1 \equiv c$ (mod $U_F^2 J_F^p$). If G_p is noncyclic, then $c = 1$, whence $c_1 \in U_F^2 J_F^p$. Now if K/F is a cyclic p-extension, then $\theta \in F_\upsilon^p$ if and only if υ splits in K, whence $c_{1\upsilon} \in U_\upsilon^2 F_\upsilon^p$ if υ splits.

The results of this section show how $d(K/F)$ can be used to obtain structural information about the Galois group of K/F, or in the case of cyclic p-extensions, the splitting of primes.

REFERENCES

1. A. Fröhlich, *Discriminants of algebraic number fields*, Math. Zeitschr., **74** (1960), 18–28.
2. V. Gallagher, *The trace-form on Galois field extensions*, pre-print.
3. E. Hecke, *Vorlesungen uber die Theorie der algebraischen Zahlen*, New York, 1948.
4. J. Herbrand, *Une propriété du discriminant des corps algébriques*, Ann. École normale (3), **49** (1932), 105–112.
5. R. Mackenzie and G. Whaples, *Artin-Schreier equations in characteristic zero*, Amer. J. Math., **78** (1956), 473–485.
6. D. Maurer, *Invariants of the trace-form of a number field*, Linear and Multilinear Algebra, **6** (1978), 33–36.
7. J. P. Serre, *Corps Locaux*, Paris, 1968.

Received June 24, 1977 and in revised form March 9, 1979.

CENTER FOR NAVAL ANALYSES
2000 N. BEAUREGARD ST.
ALEXANDRIA, VA 22331