ARITHMETIC PROPERTIES OF THE IDÈLE DISCRIMINANT

DONALD EUGENE MAURER
ARITHMETIC PROPERTIES OF THE IDELE DISCRIMINANT

Donald Maurer

A theorem of Hecke asserts that the discriminant \( b_{K/F} \) of an extension of algebraic number fields \( K/F \) is a square 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 \( b_{K/F} \) can be written in the form \( \Psi(\theta) \), \( \theta \in F \); where (i) \( \theta \equiv 1 \) (mod \( \mathfrak{B} \)), \( \mathfrak{B} \) is the greatest divisor of 4 which is prime to \( b_{K/F} \), and (ii) \( \theta > 0 \) at each real prime \( \nu \) except when \( K \cong F \) is a direct sum of copies of the complex field and \( (K:F) \equiv 2 \) (mod 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 \( \mathfrak{M}_F \) denote the finite prime divisors of \( F \). The ring of integers in \( F \) will be denoted by \( \mathcal{O} \) (or \( \mathcal{O}_F \)), and for each \( \nu \in \mathfrak{M}_F \), \( \mathcal{O}_\nu \) will be the integers of the completion \( F_\nu \). Also, for \( \alpha \in F_\nu \), we write \( \nu(\alpha) \) for the order of \( \alpha \), so that if the prime ideal \( \mathfrak{P}_\nu \) of \( \mathcal{O}_\nu \) is generated by \( \pi_\nu \), then \( \nu(\pi_\nu) = 1 \). If \( x \) is an idèle with \( \nu \)-component \( x_\nu \), then we shall write \( x = (x_\nu) \), and \( \nu(x) = \nu(x_\nu) \). If \( \alpha \in F^* \) then, unless otherwise stated, \( (\alpha) \) will denote the principal idèle defined by \( \alpha = \alpha \). The idèle group \( J_F \) contains, as a subgroup, the unit idèles \( U_F \) consisting of those \( x \) such that \( x_\nu \in U_\nu \), the unit group in \( F_\nu \), for all \( \nu \). The idèle discriminant \( d(K/F') \) defined in [1] is an element of \( J_F/U_F^* \). 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 \( \zeta_p \), a primitive \( p \)-th 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 \( \alpha \equiv 1 \) (mod \( \mathfrak{B} \)), where \( \mathfrak{B} \) is the greatest divisor of \( (\zeta_p - 1)^p \) which is relatively prime to the discriminant \( b_{K/F} \). Moreover, \( \nu \) splits in \( K \) if and only if \( \alpha \in F_\nu^* \).
Proof. For each \( \nu \in \mathcal{M}_F \), let \( K_\nu = K \otimes_F F_\nu \); then \( K_\nu \) is algebra-isomorphic to a direct product \( \prod_{\omega/\nu} K_\omega \) of local field extensions \( K_\omega/F_\nu \). Similarly, if we let \( (\mathcal{O}_K)_\nu = \mathcal{O}_K \otimes \mathcal{O}_\nu \), then \( (\mathcal{O}_K)_\nu = \prod_{\omega/\nu} \mathcal{O}_\omega \). Let \( \mathcal{P} \) be the set of all \( \nu \) which divide \( p \) (i.e., \( \nu(p) > 0 \)) but do not divide \( \nu_{K/F} \). Then for each \( \nu \in \mathcal{P} \), \( K_\nu \) is nonramified, and so \( K_\nu \) has a normal \( \mathcal{O}_\nu \)-integral basis \( \{ x_\nu^g \}_{g \in G} \). By the strong approximation theorem, it is then possible to find a normal \( F \)-basis \( \{ x_\nu^g \}_{g \in G} \) of \( K_\nu \) which is an \( \mathcal{O}_\nu \)-integral basis of \( (\mathcal{O}_K)_\nu \) at each \( \nu \in \mathcal{P} \). Moreover, we may also assume that \( \sum_{g \in G} x_\nu^g = 1 \).

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

\[
\theta_\chi = 1 + \sum_{g \neq 1} (\chi(g) - 1) x_\nu^g .
\]

But in the field \( Q_p \) of the \( p \)th roots of unity over the rational field we can write

\[
\chi(g) - 1 = c_\chi(\zeta_p - 1) \quad (c_\chi \text{ integral in } Q_p).
\]

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

We continue to suppose that \( K/F \) is a cyclic \( p \)-extension. For \( \nu \in \mathcal{M}_F \), let \( G_\nu \) denote the \( \nu \)th ramification group of a localization \( K_{\omega}/F_\nu \). We define the ramification number \( r_\nu \) to be the smallest integer \( n \) such that \( G_\nu^n \) is trivial. Clearly \( r_\nu \) is independent of \( \omega \).

Now \( \nu \) is nonramified, tamely ramified, or wildly ramified according as \( r_\nu = 0 \), \( r_\nu = 1 \) or \( r_\nu > 1 \) respectively. If \( (K:F) = p \), then the ramification numbers \( r_\nu \) give a complete description of ramification, and \( \nu(d(K/F)) = r_\nu(p - 1) \).

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

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

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

\[
\zeta_p = 1 - \gamma \pi_\omega^s .
\]
\[ \zeta_p = \frac{\sigma(\alpha^{1/p})}{\alpha^{1/p}} = \left( \frac{\sigma(\pi_{\omega})}{\pi_{\omega}} \right)^a \frac{\sigma(\epsilon)}{\epsilon}. \]

Since \( \pi_{\omega}^r (r = r_\nu) \) is the highest power of \( \pi_{\omega} \) which divides \( \sigma(\pi_{\omega}) - \pi_{\omega} \), it follows that

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

where \( U_m = 1 + \mathbb{P}_m^n \). Since \((a, p) = 1\), it is also true that

\[ \left( \frac{\sigma(\pi_{\omega})}{\pi_{\omega}} \right)^e \in U_{r-1} - U_r . \]

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

This completes the proof.

It is not possible to say much about \( r_\nu \) when \( \nu(\alpha) \equiv 0 \pmod{p} \).

A slight modification of the previous argument shows that \( r_\nu \leq sp \).

However, if \( n \) is any integer in the range \( 0 < n \leq sp \), then according to [5] or [7], for a \( y \in F_\nu \) with \( \nu(y) = 1 - n \), the roots of

\[ x^p - x - y = 0 \]

generate a cyclic extension of degree \( p \) with \( r_\nu = n \).

Let \( K/F \) be cyclic of degree \( p \), then a divisor \( \nu \in \mathbb{P}_F \) will be called exceptional at \( K/F \) if the congruence \( \nu(\alpha) \cdot x \equiv r_\nu \pmod{p} \) does not have a solution relatively prime to \( p \). That is, \( \nu \) is exceptional if one, but not both, of \( \nu(\alpha) \) or \( r \) is congruent to \( 0 \pmod{p} \). Suppose \( \nu(\alpha) \equiv 0 \pmod{p} \), but \( r_\nu \equiv 0 \pmod{p} \). By Lemma 1.2 \( r_\nu = 0 \), and so \( K/F_\nu \) is nonramified. Since \( \alpha \) is a \( p \)-th power in \( K \), \( p \) must divide \( \nu(\alpha) \), a contradiction. Hence \( \nu \) is exceptional if and only if it is totally ramified, and \( \nu(\alpha) \cdot x \equiv r \pmod{p} \) is not solvable, i.e., \( \nu(\alpha) \equiv 0 \pmod{p} \) but \( r_\nu \not\equiv 0 \pmod{p} \).

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 \( \mathbb{P}_F \). Suppose \( K/F \) is a \( p \)-extension, and let \( T \) be a subfield such that \( (K: T) = p \). We define \( \phi_{K/F}(\nu) = 0 \) unless \( \nu \) is totally ramified in \( K/F \), and \( K/T \) is exceptional at the extension \( \omega \) of \( \nu \) to \( T \). In the latter case, \( \phi_{K/F}(\nu) \) is to be the least positive residue \( \pmod{p} \) 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 \( \nu \) is totally ramified. The tower formula applied to the localization at \( \nu \) gives (since \( \nu \) is totally ramified, we can identify \( \omega \) and \( \nu \) when convenient)

\[ N(d(K_\omega/T_\nu)) \equiv N'(d(K_\omega/T_\nu))(\pmod{p}) , \]
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 $(L: F)\phi_{K/L}(\omega)/e_{L/F}(\nu)$, where $\omega$ extends $\nu$ to $L$, and $e_{L/F}(\nu)$ denotes the ramification index of $\nu$ in $L$. Again, it can be verified that this definition is independent of the choice of either $L$ or $\omega$. If $K/F$ is finite Galois, we say $\nu$ is exceptional at $K/F$ if $\phi_{K/F}(\nu) \neq 0$. This extends the earlier definition.

The function $\psi$ is defined in a similar manner. If $(K: F) = p$, then $\psi_{K/F}(\nu) = 1$ for all exceptional $\nu$. Otherwise $\psi_{K/F}(\nu)$ is the least positive residue (mod $p$), satisfying the congruence $\nu(\alpha) \cdot \psi_{K/F}(\nu) \equiv r_\nu(\nu, \alpha)$, where $K = F(\alpha^{1/3})$. In the general case, if $G_p$ is cyclic, let $T$ be a subfield such that $(K: T) = p$ and define $\psi_{K/F}(\nu) = \psi_{K/T}(\omega)$, where $\omega$ extends $\nu$ to $T$. If $G_p$ is noncyclic, define $\psi_{K/F}(\nu) = 1$ for all $\nu$. The definition is independent of $T$, $\omega$ or $\alpha$. We can now state the main theorem of this section.

**Theorem 1.3.** 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

$$d(K/F) \equiv a^p bc(\nu) \pmod{U_F^\ast}.$$  

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

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

(ii) If $\nu$ is exceptional, $\nu(\theta) \equiv 0(\mod p)$

(iii) If $G_p$ is noncyclic, then $\theta = 1$. Moreover, if $K/F$ is a cyclic $p$-extension, a nonramified $\nu$ prime to $p$ splits in $K/F$ if and only if $\theta \in U_F^\ast$.

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

We do not deal with the infinite components of $d(K/F)$, for when $p = 2$ this is discussed in [1]; and for $p > 2$, $F_\nu = C$ for all infinite $\nu$, whence $d(K/F)$, 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 $(K: F) = p^n$. If $m = 1$, let $K = F(\alpha^{1/p})$, where $\alpha$ 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, \( \gamma, \gamma^2, \ldots, \gamma^{p-1} \) with \( \gamma = \alpha^{1/p} \). Therefore \( d(K/F) \) will have a local representation at \( \nu \) of the form
\[
d(K/F)_\nu \equiv (-1)^{(p-1)/2} p^r \beta \alpha^{p-1} (\mod U_\nu^2),
\]
for some \( \beta \in F_\nu \). Using the relation \( \nu(d(K/F)) = r(p - 1) \), this gives the congruence \( 2 \nu(\beta) \equiv -r + \nu(\alpha)(\mod p) \). Hence there is a function \( \phi'_K/F \) which satisfies the congruence equation \( 2 \phi' \equiv \phi(\mod p) \).

In particular if \( p = 2 \), then \( \phi' = 0 \) and so there are no exceptional primes. Now if \( \nu \) is exceptional, then our result implies that \( \beta_\nu = \varepsilon \pi_\nu^{\phi'(\nu)} \) for some unit \( \varepsilon_\nu \). On the other hand, if \( \nu \) is nonexceptional, then \( \nu(\alpha) \cdot \psi(\nu) = \nu(\alpha) (\mod p) \). Therefore in the above representation for \( d(K/F)_\nu \) we can replace \( \alpha \) by \( \alpha^{\psi(\nu)} \).

Thus we obtain the global idèle representation
\[
d(K/F) \equiv \delta^p \beta^p \tau^{p-1} (\mod U_p^2),
\]
where each component of \( \beta \) is given by \( \beta_\nu = \varepsilon \pi_\nu^{\phi'(\nu)} \), and \( \tau_\nu = \alpha^{\psi(\nu)} \). Moreover, for all nonramified \( \nu \), \( \alpha \in U_\nu^p \) if and only if \( \nu \) 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 \( d(K/T) \equiv \delta^p \beta^p \tau^{p-1} (\mod U_p^2) \). The tower formula gives \( d(K/F) \equiv \delta^p \beta^p \tau^{p-1} (\mod U_p^2) \), where \( \beta = N_{T/F}(\beta_T) \) and \( \tau = N_{T/F}(\tau_T) \). By a straightforward computation, \( \beta_\nu = \varepsilon \pi_\nu^{\phi'(\nu)} (\phi' = \phi'_K/F) \). Similarly, if we define \( \alpha = N_{T/F}(\alpha_T) \), then \( \tau_\nu = \alpha^{\psi(\nu)} (\psi = \psi_{K/F}) \).

Suppose that \( \nu \) divides \( p \) but not \( b_{K/F} \). Then an extension \( \omega \) of \( \nu \) to \( T \) also divides \( p \) but not \( b_{K/T} \); therefore in \( \mathcal{O}_\omega \), \( \alpha_T = 1 + h_\omega(\zeta_p - 1)^p \). Since \( T/F \) is normal, we have
\[
N_{\alpha_T}(\alpha_T) = \prod (1 + \sigma(h_\omega)(\zeta_p - 1)^p),
\]
where \( \sigma \) runs through the elements of the Galois group of \( T_\omega/F_\nu \). Hence it follows that \( \alpha = 1 + h_\omega(\zeta_p - 1)^p \) is in \( \mathcal{O}_\omega \).

Now we must show that if \( \nu \) is nonramified in \( K \), and prime to \( p \), then \( \nu \) splits if and only if \( \alpha \in U_\nu^p \). Suppose that such a \( \nu \) does not split in \( K \). Then \( \alpha_T \notin T_\nu^p \). In general if \( U_t \) denotes the unit group of \( (\Omega_t)_t \), we have \( (U_t; U_t^p) = p \), so that the norm map induces an isomorphism \( U_{t+1}/U_t^p_{t+1} \cong U_t/U_t^p \); hence \( \alpha \notin U_\nu^p \). Since there are infinitely many primes which do not split in \( K/F \), \( \alpha \) cannot be a \( p \)-th power, and therefore \( (F(\alpha^{1/p}); F) = p \).

Now a nonramified \( \nu \) will split in \( K/F \) if and only if it splits
in $\Omega_i/F$, for if it splits in $K$, then the decomposition field contains $\Omega_i$, whence $\nu$ also splits in $\Omega_i/F$. Hence if $\nu$ splits in $\Omega_i$, then it splits in $K$ and so also in $F(\alpha^{1/p})$; therefore $F(\alpha^{1/p}) = \Omega_i$. 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 $b^n \in N$. 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 $\delta^p_\nu \beta_\nu \tau_\nu^{-1}$, where each component of $\tau_\nu$ is a power of $\mu$. Since $N_{L/F}(\mu) = \mu^p$, the tower formula gives for each $\omega \in \mathcal{M}_L$ the representation $d(K/L)_\omega = \delta^\omega_\nu \beta_\omega \varepsilon^{G_\nu}(U_\omega)$, where $\beta_\omega = \varepsilon_\omega \tau_\omega^{p(\omega)}(\beta' = \phi_{K/L})$. The tower formula applied to $K \supset L \supset F$ then gives a representation of $d(K/F)$ of the form $\delta^p \beta^p \tau^{-1}$, with $\beta_\nu = \varepsilon \tau_\nu^{p(\omega)}$ and $\tau_\nu = 1$ for all $\nu \in \mathcal{M}_F$.

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 $b_\nu = \tau_\nu^{p(\omega)}$ and $\theta = (N_{L/F}(\alpha))^{p-1}$, or $\theta = 1$ depending on whether $G_\nu$ is cyclic or noncyclic. If $G_\nu$ is cyclic, then

$$
\nu(c) \equiv -\psi(\nu) \cdot \nu(N_{L/F}(\alpha)) \\
\equiv \frac{(L: F)(-\psi(\nu) \cdot \omega(\alpha)) \mod p}{e_{L/F}(\nu)},
$$

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

$$
\nu(c) \equiv 0 \mod p.
$$

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 $\zeta_2 = -1$ always belongs to $F$. Fröhlich [1] defined the discriminant field $\Omega/F$ of an extension $K/F$ as a quadratic subfield ($\Omega = F$ possible) uniquely characterized by the relation

$$
\tau(K/F) \cdot J_\nu^2 = \tau(\Omega/F) \cdot J_\nu^2.
$$
Hence $\Omega = F(\theta^{1/2})$. We use the properties of $\Omega$ 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 $d(K/F) \in J^2_{\Omega}/U^2_{\Omega}$.

**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 $d(L/F) J^2_{\Omega} = d(\Omega/F) J^2_{\Omega}$, so that by Fröhlich's characterization, $\Omega \subset L$.

Now $\theta \equiv 1(\text{mod } F^2)$ implies that almost all $\nu$ 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 $\Omega$ has an $D$-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 $d(K/F) \in J^2_{\Omega}/U^2_{\Omega}$, then $G$ is solvable.

**Proof.** Since $\theta$ is not a square, the degree $(K: F)$ must be even since $(\Omega: F) = 2$. 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 $p \geq 2$. This now imposes a restriction on $F$. Moreover, if $p > 2$ then $\theta$ is not determined, up to a $p$th 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 $d_{K/F}$ can be written as a product of ideals in the form $\mathcal{U}^r \mathcal{D}(\theta)$, where $\theta \equiv 1(\text{mod } \mathfrak{B})$, and $\mathfrak{B}$ is the greatest divisor of $(\zeta_p - 1)^p$, prime to $d_{K/F}$; $\mathcal{D}$ is divisible only by ramified primes and is characterized by the relations
\[ \nu(\mathfrak{D}) = \begin{cases} \phi_{K/F}(\nu) & \text{if } \nu \text{ is exceptional} \\ -\nu(\theta) - \frac{(L: F)}{e_{L/F}(\nu)} & \text{if } \nu \text{ is ramified, nonexceptional} \end{cases} \]

**Proof.** In the representation of Theorem 1.3, let the idèle \( d \) be defined by \( d_\nu = 1 \) at all infinite divisors, and \( d_\nu = \pi_\nu^{\phi(\nu)} \theta^{\psi(\nu) - 1} \) at all \( \nu \in \mathbb{N}_\nu \). Let \( \mathfrak{D} \) be the ideal naturally determined by \( d \); then \( \nu(\mathfrak{D}) = \phi(\nu) + \nu(\theta)(\psi(\nu) - 1) \). 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 \( \nu \in \mathbb{N}_\nu \) at least, this result is consistent with Herbrand'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 \( \nu \), \( \phi_{K/F}(\nu) \equiv d(K/F)(\text{mod } p) \). 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

\[ d(K/F) \equiv a^\nu b c_\nu (\text{mod } U^\nu_p) \]

where \( b \) is as determined in Theorem 1.3. Then \( G_p \) is cyclic if \( c_\nu \in U^\nu_p J_p^\nu \). If \( K/F \) is a cyclic \( p \)-extension, then a necessary condition for \( \nu \) to split in \( K \) is that \( c_\nu \in U^\nu_p F^\nu_p \).

**Proof.** Let \( c \) be determined as in Theorem 1.3. Then \( c_\nu \equiv c (\text{mod } U^\nu_p J_p^\nu) \). If \( G_p \) is noncyclic, then \( c = 1 \), whence \( c_\nu \in U^\nu_p J_p^\nu \). Now if \( K/F \) is a cyclic \( p \)-extension, then \( \theta \in F^\nu_p \) if and only if \( \nu \) splits in \( K \), whence \( c_\nu \in U^\nu_p F^\nu_p \) if \( \nu \) 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**

2. V. Gallagher, The trace-form on Galois field extensions, pre-print.
Charles A. Akemann and Steve Wright, *Compact and weakly compact derivations of C*-algebras* .................................................. 253
Dwight Richard Bean, Andrzej Ehrenfeucht and George Frank McNulty, *Avoidable patterns in strings of symbols* .............................. 261
Kenneth Alexander Brown and John William Lawrence, *Injective hulls of group rings* .......................................................... 323
Jacob Burbea, *The Schwarzian derivative and the Poincaré metric* ............. 345
Stefan Andrus Burr, *On the completeness of sequences of perturbed polynomial values* ......................................................... 355
Peter H. Chang, *On the characterizations of the breakdown points of quasilinear wave equations* .............................................. 361
Joseph Nicholas Fadyn, *The projectivity of Ext(T, A) as a module over E(T)* ............................................................................ 383
Donald Eugene Maurer, *Arithmetic properties of the idèle discriminant* .... 393
Stuart Rankin, Clive Reis and Gabriel Thierrin, *Right subdirectly irreducible semigroups* .......................................................... 403
David Lee Rector, *Homotopy theory of rigid profinite spaces. I* ............... 413
Raymond Moos Redheffer and Wolfgang V. Walter, *Comparison theorems for parabolic functional inequalities* ................................ 447
H. M. (Hari Mohan) Srivastava, *Some generalizations of Carlitz’s theorem* ........................................................................... 471
James Alan Wood, *Unbounded multipliers on commutative Banach algebras* .................................................................................. 479
T. Yoshimoto, *Vector-valued ergodic theorems for operators satisfying norm conditions* ............................................................. 485
Jerry Searcy and B. Andreas Troesch, *Correction to: “A cyclic inequality and a related eigenvalue problem”* ............................. 501
Leslie Wilson, *Corrections to: “Nonopenness of the set of Thom-Boardman maps”* ................................................................. 501