ON SPLITTING TYPES, DISCRIMINANT BOUNDS, AND CONCLUSIVE TESTS FOR THE GALOIS GROUP

FÜSUN AKMAN

Abstract. Using the action of the Galois group of a normal extension of number fields, we generalize and symmetrize various fundamental statements in algebra and algebraic number theory concerning splitting types of prime ideals, factorization types of polynomials modulo primes, and cycle types of the Galois groups of polynomials. One remarkable example is the removal of all artificial constraints from the Kummer-Dedekind Theorem that relates splitting and factorization patterns. Finally, we present an elementary proof that the discriminant of the splitting field of a monic irreducible polynomial with integer coefficients has a computable upper bound in terms of the coefficients. This result, combined with one of Lagarias et al., shows that tests of polynomials for the cycle types of the Galois group are conclusive. In particular, the Galois groups of monic irreducible cubics, quartics, and quintics with integer coefficients can be completely determined in finitely many steps (though not necessarily in one’s lifetime).

1. Introduction and Main Results

1.1. Galois group action in number theory. In an earlier article [1], we described a new graph invariant of finite groups. This invariant provides a complete characterization of the splitting types of unramified prime ideals in normal number field extensions entirely in terms of the Galois group, and is conjectured to distinguish finite groups. In particular, we presented the generalization of an under-utilized theorem of Lagarias [5], which depicts a one-to-one correspondence between the divisions (Abteilung) of the Galois group and splitting types:

Theorem 1.1 (Generalized Lagarias Theorem). Let $L/k$ be a normal extension of number fields, $G = \text{Gal}(L/k)$ be the Galois group, $p_1, p_2$ be primes of $k$ unramified in $L$, and $\phi_1, \phi_2$ be any two Frobenius automorphisms in $G$ associated with $p_1$ and $p_2$ respectively. Then $\phi_1$ and $\phi_2$ are in the same division.
of $G$ (i.e. the cyclic decomposition groups $< \phi_1 >$ and $< \phi_2 >$ are conjugates) if and only if the splitting types of $p_1$ and $p_2$ are the same throughout the intermediate fields of the extension $L/k$.

The elegance of the classification of splitting types above suggests that the study of prime decompositions in number fields is best conducted in normal field extensions. If $L/K/k$ is a normal extension with intermediate field $K$, then the action of the Galois group $G = \text{Gal}(L/k)$ on the subgroup $H$ fixing $K$, and on the cyclic decomposition group $D = < \phi >$ of an unramified prime $p$ of $k$, gives rise to double cosets $H \backslash G / D$. Thus, many proofs are simply reduced to counting arguments. It is well known that $G/D$ corresponds to the $L$-primes above $p$, and that the $H$-orbits of $G/D$ correspond to the $K$-primes above $p$. Similarly, $H \backslash G$ represents all roots (in $L$) of an irreducible polynomial $c(x)$ generating the extension $K/k$ (whose splitting field is $L$), and each $D$-orbit of $H \backslash G$ comprises those roots that correspond to one irreducible factor of $c(x)$ modulo $p$ (to be denoted by $\bar{c}(x)$ hereafter). The matching of the irreducible factors of $\bar{c}(x)$ with the $K$-primes above $p$ (with some restrictions) is known as the Kummer-Dedekind Theorem.

1.2. Generalization of the Kummer-Dedekind Theorem. We will state and prove the most general version of this celebrated Theorem, lifting all constraints on the rings of algebraic integers and prime ideals. We denote by $\mathfrak{O}_F$ the ring of algebraic integers in a number field $F$. In the proof, the field extension in question is embedded into the splitting field of $c(x)$ in order to use the action of the Galois group.

**Theorem 1.2 (Generalized Kummer-Dedekind Theorem).** Let $K/k$ be an extension of number fields, $K = k[\alpha]$ with $\alpha \in \mathfrak{O}_K$, and $c \in \mathfrak{O}_K[x]$ be the irreducible polynomial of $\alpha$ over $k$. Suppose that for some prime ideal $p$ of $k$, the factorization of $\bar{c} \in (\mathfrak{O}_k/p)[x]$ is given by

$$\bar{c} = \bar{c}_1^{e_1} \cdots \bar{c}_s^{e_s}$$

($\bar{c}_i$ distinct and irreducible, $c_i \in \mathfrak{O}_K[x]$ monic, $\deg(c_i) = f_i$), and that $p$ splits in $\mathfrak{O}_K$ as

$$p\mathfrak{O}_K = P_1^{e(P_1|p)} \cdots P_r^{e(P_r|p)},$$

where the $P_i$ are distinct $K$-primes. Then the following hold for some ordering of the factors $\bar{c}_i$ and the primes $P_i$:

(i) $r = s$,
(ii) $e(P_i|p) = e_i$ for all $i = 1, \ldots, r$,
(iii) $f(P_i|p) = f_i$ for all $i = 1, \ldots, r$.

**Remark 1.3.** The generalized Kummer-Dedekind Theorem is completely free of any special assumptions on the field extension $K/k$ and the prime $p$. We do not need the customary additional hypothesis, namely that $\mathfrak{O}_K = \mathfrak{O}_k[\alpha]$, or that the characteristic of the residue field of $p$ does not divide $[\mathfrak{O}_K : \mathfrak{O}_k[\alpha]]$. 

Apparently, either one of these hypotheses is assumed only to prove that the prime $P_i$ is of the form $(p, c_i(\alpha))$ (see, for example, Marcus [7]).

1.3. Necessary and sufficient conditions for normality of subextensions. The following criterion, commonly stated only in one direction, was used to prove Part (3) of Theorem 4.1 in [1]. We will provide a detailed proof in this paper.

**Proposition 1.4.** An extension $K/k$ of number fields is normal (equivalently, for any finite normal extension $L$ of $k$ that has $K$ as a subfield, the subgroup $H$ of the Galois group $G = \text{Gal}(L/k)$ that fixes $K$ is normal in $G$) IF AND ONLY IF for any unramified prime $p$ of $k$ which splits into $r$ primes $P_1, \ldots, P_r$ in $K$, the residual degrees $f(P_i|_p)$ are equal for all $i$.

An immediate corollary of Theorem 1.2 is the mirror image of Proposition 1.4, namely,

**Proposition 1.5.** Let $k$, $K = k(\alpha)$, $c = \text{irr}(\alpha, k)$ be as in Theorem 1.2. Then the extension $K/k$ is normal IF AND ONLY IF every factorization of $c$ modulo unramified primes of $k$ (equivalently, every factorization with no multiple factors) results in factors of equal degree.

1.4. Equivalence of factorization, splitting, and cycle types. The new version of the Kummer-Dedekind Theorem shows the symmetric relationship of splitting types and factorization types, with no additional conditions on the number field extension or on the prime $p$. There exists a similar relationship between the factorization types of an irreducible polynomial in $\mathbb{Z}[x]$ modulo integer primes and the cycle types of its Galois group, which has been used as an asymmetric (and not necessarily conclusive) test for the Galois group: for example, see Section 8.10 of van der Waerden [10]. Namely, if $c(x) \in \mathbb{Z}[x]$ is irreducible, then the factorization types of $c(x)$ modulo an integer prime $p$ must occur as cycle types in the Galois group of the polynomial. This result is then extended only to those rings of algebraic integers which are unique factorization domains. We will prove the following unconditional and symmetric result instead:

**Theorem 1.6** (Equivalence Theorem). Let $k$ and $K = k[\alpha]$ be number fields, where $\alpha$ is an algebraic integer, and $c(x)$ be the irreducible polynomial -of degree $n$- of $\alpha$ over $k$. Also let $G$ be the Galois group of the splitting field $L$ of $c$ over $k$ and $p$ denote a generic prime of $k$ unramified in $L$. Then there exists a one-to-one correspondence -given by lengths of cycles, degrees of irreducible factors, and inertial degrees of primes respectively- among the following finite sets:

1. Cycle types of $G$, viewed as a transitive subgroup of $S_n$ which permutes the roots of $c(x)$;
2. Factorization types of $c(x)$ modulo base primes $p$ unramified in $L$;
Splitting types of such primes in \( K \).

1.5. Upper discriminant bound for the splitting field and conclusive tests for cycle types. Tchebotarev Density Theorem (see [7]) states that there are infinitely many unramified \( k \)-primes with Frobenius automorphism as any given element of the Galois group of \( L/k \). When testing a monic irreducible polynomial \( c(x) \) with algebraic integer coefficients, we would like to know that we have checked at least one prime corresponding to every possible (unramified) splitting type so that the cycle type of the Galois group \( G \) of \( c(x) \) is completely determined. If \( G \) is the only transitive subgroup of \( S_n \) with the given order and cycle type up to isomorphism, then the test will also determine \( G \).

Lagarias et al. [6] give an upper bound for the size of primes to be tried as a power of the absolute value of the discriminant of the splitting field (see Theorem 8.1 below), which is a priori unknown. In Section 8 of this article, we will prove the following theorem:

**Theorem 1.7.** Let \( c(x) \) be a monic irreducible polynomial of degree \( n \) with integer coefficients. Then there exists a computable upper bound for the discriminant of the splitting field of \( c(x) \) depending only on \( n \) and the coefficients of \( c(x) \).

Thus, tests computing cycle types are conclusive; we shall deem a test or computation conclusive if it yields the desired result in a pre-determined, finite number of steps. The problem of computational complexity will not be considered. We will state the explicit tests for monic irreducible cubics, quartics, and quintics with algebraic integer coefficients.

1.6. Conclusive test for the Galois group of a cubic polynomial.

**Theorem 1.8** (Test for Galois group of a cubic). Let \( k \) be a number field, and \( c \) be a monic irreducible polynomial of degree three in \( \mathfrak{O}_k[x] \). Then the only possibilities for the Galois group \( G \) of \( c \) are \( A_3 \) and \( S_3 \). The finitely many factorization types of \( c \) into non-repeating irreducible factors modulo base primes determine \( G \) as follows:

- \( G = A_3 \) if and only if the factorization types are \( \{1,1,1\} \) and \( \{3\} \).
- \( G = S_3 \) if and only if the factorization types are \( \{1,1,1\} \), \( \{1,2\} \), and \( \{3\} \).

1.7. Conclusive test for the Galois group of a quartic polynomial.

For an historical account of tests for the Galois group of quartic polynomials, see Kappe and Warren [4]; Hungerford [3] (p.373) has a test in terms of the resolvent cubic. Some versions of the following result have appeared in the literature, but our theorem is very general and free of restrictions.

**Theorem 1.9** (Test for Galois group of a quartic). Let \( k \) be a number field, and \( c \) be a monic irreducible polynomial of degree four in \( \mathfrak{O}_k[x] \). Then the only possibilities for the Galois group \( G \) of \( c \) are \( \mathbb{Z}_4 \), \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \), the dihedral group...
The finitely many factorization types of $c$ into non-repeating irreducible factors modulo base primes determine $G$ as follows:

- $G = \mathbb{Z}_4$ if and only if the factorization types are $\{1, 1, 1, 1\}$, $\{2, 2\}$, and $\{4\}$.
- $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ if and only if the factorization types are $\{1, 1, 1, 1\}$ and $\{2, 2\}$.
- $G = D_4$ if and only if the factorization types are $\{1, 1, 1, 1\}$, $\{1, 1, 2\}$, $\{2, 2\}$, and $\{4\}$.
- $G = A_4$ if and only if the factorization types are $\{1, 1, 1, 1\}$, $\{1, 3\}$, and $\{2, 2\}$.
- $G = S_4$ if and only if the factorization types are $\{1, 1, 1, 1\}$, $\{1, 1, 2\}$, $\{1, 3\}$, $\{2, 2\}$, and $\{4\}$.

1.8. **Conclusive test for the Galois group of a quintic polynomial.**

All transitive subgroups of $S_5$, as well as the cycle types of their elements, are described in Schwarz et al. [8] (p.369).

**Theorem 1.10** (Test for Galois group of a quintic). Let $k$ be a number field, and $c$ be a monic irreducible polynomial of degree five in $\mathcal{O}_k[x]$. Then the only possibilities for the Galois group $G$ of $c$ are $\mathbb{Z}_5$, $D_5$, $\text{Hol}(\mathbb{Z}_5)$, $A_5$, and $S_5$. The finitely many factorization types of $c$ into non-repeating irreducible factors modulo base primes determine $G$ as follows:

- $G = \mathbb{Z}_5$ if and only if the factorization types are $\{1, 1, 1, 1, 1\}$ and $\{5\}$.
- $G = \text{Hol}(\mathbb{Z}_5)$ if and only if the factorization types are $\{1, 1, 1, 1, 1\}$, $\{1, 2, 2\}$, $\{1, 4\}$, and $\{5\}$.
- $G = D_5$ if and only if the factorization types are $\{1, 1, 1, 1, 1\}$, $\{1, 2, 2\}$, and $\{5\}$.
- $G = A_5$ if and only if the factorization types are $\{1, 1, 1, 1, 1\}$, $\{1, 2, 2\}$, $\{1, 1, 3\}$, and $\{5\}$.
- $G = S_5$ if and only if the factorization types are $\{1, 1, 1, 1, 1\}$, $\{1, 1, 1, 2\}$, $\{1, 2, 2\}$, $\{1, 1, 3\}$, $\{2, 3\}$, $\{1, 4\}$, and $\{5\}$.

2. **Proof of Generalized Lagarias Theorem 1.1**

The following short proof of Theorem 1.1 first appeared in [1]:

**Proof.** The following are equivalent:

(i) $\phi_1 > 0$ and $\phi_2 > 0$ are conjugates in $G$;
(ii) $G/ \phi_1 > 0$ and $G/ \phi_2 > 0$ are $G$-isomorphic;
(iii) $G/ \phi_1 > 0$ and $G/ \phi_2 > 0$ are $H$-isomorphic for all $H < G$;
(iv) $G/ \phi_1 > 0$ and $G/ \phi_2 > 0$ decompose into the same number and size of orbits under the left action of each $H < G$ (these numbers may vary with $H$);
(v) $H \setminus G$ decomposes into the same number and size of orbits under the right actions of $\phi_1 > 0$ and $\phi_2 > 0$ for any $H < G$ (these numbers may vary with $H$);
(vi) $p_1$ and $p_2$ split alike in all intermediate fields $K$.

The relations (i) $\iff$ (ii) $\iff$ (iii) $\Rightarrow$ (iv) are self-evident. For (iv) $\Rightarrow$ (i), take $H = \phi_1 > 0$. The equivalence of (iv) and (v) is an elementary property of...
finite groups, to be proven in Lemma 3.2. The final equivalence (v) \iff (vi) is a well-known result, which we will state below as Proposition 3.5, and generalize in Proposition 3.7. □

3. DOUBLE COSETS AND NUMBER THEORY

3.1. Double cosets of finite groups. Let \( G \) be a finite group with arbitrary subgroups \( H, D, D_1, \) and \( D_2 \). The collection \( H \backslash G \backslash D \) of double cosets of \( H \) and \( D \) in \( G \) consists of disjoint sets \( HgD = \{hgd : h \in H, d \in D\} \) which exhaust \( G \), because each \( HgD \) is an equivalence class of the equivalence relation

\[ g_1 \sim g_2 \text{ iff } g_1 = hgd \text{ for some } h \in H, d \in D. \]

In particular, if \( g' \in HgD \), then \( HgD = Hg'D \). Unlike ordinary left or right cosets, double cosets may have different numbers of elements. These numbers are given by the formula

\[ |HgD| = |HgDg^{-1}| = \frac{|H| |gDg^{-1}|}{|H \cap gDg^{-1}|} = \frac{|H| |D|}{|H \cap gDg^{-1}|}, \]

which will also follow from Lemma 3.3. It is also possible to obtain double cosets as the union of left or right cosets in a certain orbit. Here is an elementary observation:

**Lemma 3.1.** Let \( H \) act on the set of left cosets \( G/D \) on the left and \( D \) act on the set of right cosets \( H \backslash G \) on the right by translation. Suppose \( G/D \) splits into \( r \) \( H \)-orbits with \( a_1, \ldots, a_r \) cosets in each and \( H \backslash G \) splits into \( s \) \( D \)-orbits with \( b_1, \ldots, b_s \) cosets in each. Then the following properties hold:

(i) The union of all cosets in an orbit \( H(gD) \) (resp. \( (Hg)D \)) is exactly the double coset \( HgD \),

(ii) \( r = s \),

(iii) For a certain ordering of both sets of orbits (namely, so that \( (Hg)D \leftrightarrow H(gD) \)), we have \( a_i|H| = b_i|D| \) for all \( i = 1, \ldots, r \).

**Proof.** The union of all cosets in an orbit \( \{gD, h^{-1}gD, \ldots\} \) of \( H \) in \( G/D \) is certainly contained in \( HgD \). Conversely, if \( g' \in HgD \), then \( g' = hgd \in h(gD) \), where the latter is in the same \( H \)-orbit as \( gD \). Parts (ii) and (iii) follow immediately from (i). □

This brings us to the following result, which demonstrates (iv) \iff (v) in the proof of Theorem 1.1:

**Lemma 3.2.** The following are equivalent:

(i) \( G/D_1 \) and \( G/D_2 \) decompose into the same number and size of orbits under the left action of each \( H < G \) (these numbers may vary with \( H \)).

(ii) \( H \backslash G \) decomposes into the same number and size of orbits under the right actions of \( D_1 \) and \( D_2 \) for any \( H < G \) (these numbers may vary with \( H \)).
Proof. Let the notation be as in Lemma 3.1, with a superscript \( (j) \) indicating the group \( D_j \) under consideration \( (j = 1 \) or \( 2) \). First of all, we note that \( r^{(1)} = r^{(2)} \) if (i) holds and \( s^{(1)} = s^{(2)} \) if (ii) holds. Combining this fact with Lemma 3.1 we deduce that in either case all four sets \( H\backslash(G/D_1), H\backslash(G/D_2), (H\backslash G)/D_1, \) and \( (H\backslash G)/D_2 \) are made up of the same number of orbits, say \( r \). Secondly, we must have \( |D_1| = |D_2| \) in either case (take \( H = \langle 1 \rangle \)). We now fix \( H < G \) and show that

\[
(i) \quad a_i^{(1)} = a_i^{(2)} \iff (ii) \quad b_i^{(1)} = b_i^{(2)}
\]

after a possible reordering of orbits. By symmetry, it suffices to prove (i)\( \Rightarrow \) (ii). Choose an ordering of orbits of \( G/D_1 \) and \( G/D_2 \) under \( H \) so that \( a_i^{(1)} = a_i^{(2)} \) holds. The corresponding orbits of \( H\backslash G \) under \( D_1 \) and \( D_2 \) are allowed to have the same representatives from \( G \) by Lemma 3.1, so their orders are fixed as well. Then by using Lemma 3.1 one last time we find that

\[
\begin{align*}
    a_i^{(1)} = a_i^{(2)} & \iff a_i^{(1)}|H| = a_i^{(2)}|H| \forall i \\
    & \iff b_i^{(1)}|D_1| = b_i^{(2)}|D_2| \forall i \\
    & \iff b_i^{(1)} = b_i^{(2)} \forall i.
\end{align*}
\]

Here are two more Lemmas that describe orbits explicitly:

**Lemma 3.3.** Let \( G, H, D \) interact as in Lemma 3.1. Furthermore, let \( g_1, \ldots, g_r \) be such that \( Hg_iD \) are the distinct double cosets of \( G \) with respect to \( H \) and \( D \). Then the \( i \)-th orbit \( (Hg_i)D \) is \( D \)-isomorphic to

\[
D \cap g_i^{-1}Hg_i \backslash D \cong_D H \cap g_iDg_i^{-1} \backslash g_iDg_i^{-1},
\]

and \( H(g_i)D \) is \( H \)-isomorphic to

\[
H/H \cap g_iDg_i^{-1} \cong_H g_i^{-1}Hg_i \cap D \cap g_i^{-1}Hg_i.
\]

**Proof.** The proofs for \( D \)- and \( H \)-orbits are similar, so let us proceed with the first case. Note that

\[
\text{Stab}_D(Hg_i) = D \cap \{g \in G : Hg_i g = H g_i\} = D \cap \{g \in G : g, g g_i^{-1} \in H\} = D \cap \{g \in G : g \in g_i^{-1} H g_i\} = D \cap g_i^{-1} H g_i,
\]

so that

\[
(Hg_i)D \cong_D \text{Stab}_D(Hg_i) / D = D \cap g_i^{-1} H g_i \backslash D,
\]

which is in turn \( D \)-isomorphic to

\[
g_iDg_i^{-1} \cap H \backslash g_iDg_i^{-1},
\]

because \( D \) acts on \( g_iDg_i^{-1} \)-sets via the conjugation isomorphism

\[
\varphi_i : G \to G, \quad x \mapsto g_i x g_i^{-1}.
\]
Lemma 3.4. If $E$ is a normal subgroup of $D$, then every $D$-orbit $(Hg_i)D$ splits into $E$-orbits, each of which is $E$-isomorphic to

$$H \cap g_iEg_i^{-1}\backslash g_iEg_i^{-1}.$$  

Proof. The $E$-orbit of $Hg_i$ itself is isomorphic to $H \cap g_iEg_i^{-1}\backslash g_iEg_i^{-1}$ by the same “conjugation trick”. Let $Hg$ be in the same $D$-orbit as $Hg_i$, so there must be some $d \in D$ such that $Hg_i d = Hg$, hence

$$\text{Stab}_E(Hg) = \text{Stab}_E(Hg_i d) = E \cap (g_i d)^{-1}H(g_i d),$$

and the $E$-orbit of $Hg$ is

$$\text{Stab}_E(Hg) \backslash E \cong_E E \cap (g_i d)^{-1}H(g_i d) \backslash E \cong_E g_i dEg_i^{-1} \cap H \backslash g_i dEg_i^{-1} \cong g_i E g_i^{-1} \cap H \backslash g_i E g_i^{-1}.$$  

The only new ingredient in this calculation is the normality of $E$ in $D$. ⊓⊔

3.2. Double cosets of the Galois group in a normal extension of number fields. The following result is well-known (see [7]).

Proposition 3.5. Let $G$ be the Galois group of a normal extension $L/k$ of number fields, $p$ be a prime in $\mathcal{O}_k$ which is unramified in $\mathcal{O}_L$, $\phi$ be any Frobenius automorphism of $p$ in $G$, $H$ be an arbitrary subgroup of $G$, and $K$ be the subfield of $L$ fixed by $H$. Suppose that the right action of the cyclic subgroup $<\phi>$ of $G$ partitions the set $H \backslash G$ of right cosets of $H$ into $r$ orbits with $f_1, \ldots, f_r$ cosets respectively. Then $p$ splits into $r$ primes $P_i$ in $\mathcal{O}_K$, for which the residual degrees $f(P_i|p)$ are given by the numbers $f_i$.

Our proof of Theorem 1.1 can now be completed by invoking Proposition 3.5, but let us go one step further: we will state and prove a generalization. Let $L/K/k$ be number fields with $L/k$ normal. Denote the Galois group $\text{Gal}(L/k)$ by $G$ and the subgroup fixing $K$ by $H$. Let the splitting of a prime $p$ of $k$ be as shown in Figure 1. Also let $D = D(Q|p)$ with $|D| = e(Q|p)f(Q|p) = ef$ and $E = E(Q|p)$ with $|E| = e(Q|p) = e$. 
Lemma 3.6. Let \( g_i \) be as in Lemma 3.3. Then we have

\[
D_i \overset{\text{def}}{=} D(g_i(Q)|p) = g_i D(Q|p) g_i^{-1} = g_i Dg_i^{-1}
\]

\[
E_i \overset{\text{def}}{=} E(g_i(Q)|p) = g_i E(Q|p) g_i^{-1} = g_i E g_i^{-1}
\]

\[
D_i' \overset{\text{def}}{=} D(g_i(Q)|P_i) = H \cap D(g_i(Q)|p) = H \cap D_i
\]

\[
E_i' \overset{\text{def}}{=} E(g_i(Q)|P_i) = H \cap E(g_i(Q)|p) = H \cap E_i.
\]

Because of the transitive left action of \( G \) on the \( \mathbf{L} \)-primes above \( p \), this set of primes is \( G \)-isomorphic to \( G/\text{Stab}_G(Q) = G/D \). The subgroup \( H \) of \( G \) now acts on the left, and in general \( G/D \) is not \( H \)-transitive. What do we know about the new orbits? Since \( H \) is the Galois group of the normal extension \( \mathbf{L}/\mathbf{K} \), it permutes the \( Q_{ij} \) for fixed \( i \), and an irreducible \( H \)-subset of \( G/D \) corresponds exactly to the \( \mathbf{L} \)-primes \( \{Q_{i1}, \ldots, Q_{ib_i}\} \) above some \( P_i \).

Some counting: under \( H \), we have seen that \( G/D \) breaks into \( r \) irreducible subsets. The “length” \( b_i \) of each is the number of \( \mathbf{L} \)-primes above the matching \( P_i \), i.e.

\[
b_i = \frac{[\mathbf{L} : \mathbf{K}]}{e_i'f_i'} = \frac{|H|}{e_i'f_i'}
\]

In addition, \( D \) acts on \( H \setminus G \) on the right to produce the same number of orbits, namely \( r \) (Lemma 3.1). If the \( i \)-th orbit has \( a_i \) cosets in it, we have

\[
a_i = \frac{b_i |D|}{|H|} = \frac{|D|}{e_i'f_i'} = e_i f_i
\]

by Lemma 3.1 and the above value of \( b_i \). (The direct way of arriving at this number is to consider the orbit of \( Hg_i \) (1 \( \leq \) \( i \) \( \leq \) \( r \)) under \( D \). This orbit is \( D \)-isomorphic to \( D_i' \setminus D_i \) by Lemmas 3.3 and 3.6, thus it has \( e_i f_i' = e_i f_i \) elements.) We have proved the following Proposition, which reduces to Proposition 3.5 for unramified primes:
Proposition 3.7. The right action of $D$ on $H \backslash G$ gives $r$ irreducible $D$-subsets, each corresponding to a prime $P_i$ of $K$ over $p$ and having length $e_i f_i = e(P_i | p)f(P_i | p)$. The one-to-one correspondence is given by

\[ \text{orbit of } Hg_i \leftrightarrow P_i = g_i(Q) \cap \mathcal{O}_K. \]

We can moreover extend this result as follows: $E$, as a subgroup of $D$, acts on $H \backslash G$ to split each $D$-orbit further into $E$-orbits. Let us look at one $D$-orbit, say $(Hg_i)\mathcal{D}$. The $E$-orbit of any $Hg$ in the same $D$-orbit is isomorphic to $E^j \backslash E_i$ by Lemmas 3.4 and 3.6, thus, we have

Proposition 3.8. Let the notation be as in Proposition 3.7. Then $E$ acts on each irreducible $D$-subset of $H \backslash G$ on the right to produce irreducible $E$-sets of length $|E^j \backslash E_i| = e/e'_i = e_i$ each, and there are

\[ \frac{ef_i}{e_i f'_i} = f_i \]

of them.

4. Proof of Generalized Kummer-Dedekind Theorem 1.2

Notation.

$L = \text{spl}(c)$ is the splitting field of $c$ over $k$ in $C$

$G = \text{Gal}(L/k) = \text{Gal}(c)$

$H$ is the subgroup of $G$ fixing $K$ (or fixing $\alpha$)

$Q$ is a fixed prime above $P_1$ in $L$ (see Figure 1, but remember that we are not using the shortcut notation for residual degrees and ramification indices)

$D = D(Q|p)$

$E = E(Q|p)$

$R = \{ \alpha_1 = \alpha, \ldots, \alpha_n \}$ is the set of roots of $c$ in $\mathcal{O}_L$

$n = |R| = \sum e_if_i = [K : k] = [G : H]$

$\bar{R} = \{ \bar{\beta} \in \mathcal{O}_L/Q : \beta \in R \}$, $|\bar{R}| = \sum f_i$

$R_i = \{ \beta \in R : \bar{\beta} \text{ is a root of } \bar{c}_i \}, 1 \leq i \leq s, |R_i| = e_if_i$

$\bar{R}_i = \{ \bar{\beta} \in R_i : |\bar{R}_i| = f_i \}$

$R_i^{(j)} = \{ \beta \in R_i : \bar{\beta} \text{ is the } j\text{-th root of } \bar{c}_i \}$ for some ordering of roots, $1 \leq j \leq f_i$, $|R_i^{(j)}| = e_i$

$\bar{R}_i^{(j)} = \{ \bar{\beta} : \beta \in R_i^{(j)} \}$, $|\bar{R}_i^{(j)}| = 1$

Proof. Step 1. $R$ and $H \backslash G$ are isomorphic transitive $G$-sets under the right action of $G$.

The Galois group $G$ permutes the roots of $c$ transitively, so we have

\[ R \cong G \text{ Stab}_G(\alpha) \backslash G = H \backslash G. \]

The $G$-isomorphism is given by

\[ \beta = \alpha \cdot g = g^{-1}(\alpha) \leftrightarrow Hg. \]
Step 2. \( R_i \) is \( D \)-isomorphic to a \( D \)-orbit of \( H \backslash G \).

For some subgroup \( \Gamma \) of \( \bar{G} = \text{Gal}((\mathcal{D}_L/Q)/((\mathcal{D}_k/p))) \cong E \backslash D \), there is a Galois correspondence between the groups \( 1 < \Gamma < \bar{G} \) and the fields
\[
\mathcal{D}_L/Q \supset F \overset{\text{def}}{=} (\mathcal{D}_k/p)(\bar{R}) = \text{spl}(\bar{e}) \supset \mathcal{D}_k/p.
\]
The group \( \text{Gal}(F/(\mathcal{D}_k/p)) = \text{Gal}(\bar{e}) \) acts on \( \bar{R} \) in such a way that the \( \bar{R}_i \) are transitive. Then \( D \) acts on \( \bar{R} \) via the epimorphism
\[
(4.1) \quad D \to E \backslash D \cong \bar{G} \to \Gamma \backslash \bar{G} \cong \text{Gal}(\bar{e}),
\]
and the \( \bar{R}_i \) are \( D \)-transitive. It follows that \( R_i \), the inverse image of \( \bar{R}_i \) under the surjective \( D \)-map \( R \to \bar{R} \) (mod \( Q \)), is a transitive \( D \)-set. Immediately we obtain the equality \( r = s \). We also deduce that if \( \beta = \alpha \cdot g \in R_i \), then \( e_i f_i = e(P_i|p)f(P_i|p) \) for \( P_i = g(Q) \cap K \), because
\[
R_i \cong_D \text{Stab}(\beta)\backslash D
\]
\[
= D \cap \text{Stab}_G(g^{-1}(\alpha))\backslash D
\]
\[
= D \cap \text{Stab}_G(g^{-1}Hg)\backslash D
\]
\[
= gDg^{-1} \cap H \backslash D
\]
\[
= D(g(k)|P_i)\backslash D(g(Q)|p),
\]
making use of the conjugation trick in Lemma 3.3.

Step 3. \( R_i^{(j)} \) is \( E \)-isomorphic to an \( E \)-orbit of \( H \backslash G \).

As a subgroup of \( D \), \( E \) also acts on \( \bar{R} \), albeit trivially (follow the maps in Equation (4.1)). This means each singleton \( \bar{R}_i^{(j)} \) is an \( E \)-orbit and so is its inverse image, \( R_i^{(j)} \). Repeating the calculation in Step 2 and using Lemma 3.4 this time we find that
\[
R_i^{(j)} \cong_E E(Q_{ij}|P_i)\backslash E(Q_{ij}|p) \quad \forall j,
\]
hence \( e_i = |R_i^{(j)}| = e(P_i|p) \) and \( f_i = f(P_i|p) \).

5. Proof of Proposition 1.4

Proof. The “only if” part is well-known, but we will briefly verify it: recall that the residual degrees are given by the lengths of the orbits of the right action of \( D \) on \( H \backslash G \). By Lemma 3.3 and the normality of \( H \) in \( G \), all \( D \)-orbits are isomorphic to the same \( D \)-set, namely \( D \cap H \backslash D \). To prove the “if” part, we will show that if a subgroup \( H \) of a finite group \( G \) has a conjugate not equal to itself, then there is one unramified prime (hence, infinitely many unramified primes) for which there are at least two different residual degrees. Fix elements \( \phi \) and \( g \) of \( G \) such that \( \phi \in H \) but \( \phi \not\in g^{-1}Hg \). Let \( D \) be the cyclic subgroup of \( G \) generated by \( \phi \), and without loss of generality, designate \( \phi \) to be the representative of its division and use this particular group to construct one of the splitting types. One \( D \)-orbit has length one because \( (H1)D = H1 \), \( D \) being a subgroup of \( H \). But the orbit of \( Hg \) has length greater than one, since
$(Hg)D$ cannot be equal to $Hg$. If it were, we could then say $HgDg^{-1} = H$, or $gDg^{-1} < H$, or equivalently, $< \phi > = D < g^{-1}Hg$.

6. Cycle structure

The Lemma below has an elementary proof, which we omit.

**Lemma 6.1.** Let $G$ be a transitive subgroup of $S_n$, and $\omega$ denote an element of the set $\Omega = \{1, 2, \ldots, n\}$ on which $S_n$ acts. Then all stabilizers

\[ G_\omega = \{ g \in G : g(\omega) = \omega \} \]

form a complete class of conjugate subgroups, and we have

\[ [G : G_\omega] = n \]

for all $\omega \in \Omega$. In particular, if $g_1, g_2, \ldots, g_n$ are any $n$ elements of $G$ with the property $g_i(1) = i$ for all $i \in \Omega$, the set of right cosets of $H = G_1$ is given by

\[ \{Hg_1, Hg_2, \ldots, Hg_n\} \]

**Lemma 6.2.** With the notation of Lemma 6.1, let $\phi$ be an element of $G$ which is the product of $s$ disjoint cycles of lengths $F_1, \ldots, F_s$. On the other hand, assume $H \setminus G$ splits into $r$ orbits of lengths $f_1, \ldots, f_r$ under the right action of the cyclic group $< \phi >$. Then for some ordering of the disjoint cycles and the orbits, we have

(i) $r = s$, and
(ii) $F_i = f_i$ for all $i$.

**Proof.** Let $(j \phi(j) \cdots \phi^{F-1}(j))$ be one of the disjoint cycles in the decomposition of $\phi$. Then the product

\[ g_j \phi = (1 \cdots \cdots (j \phi(j) \cdots) \cdots = (1 \phi(j) \cdots) \cdots \]

shows that $Hg_j \phi = Hg_{\phi(j)}$, and the orbit of $Hg_j$ is the one that corresponds in length to the cycle that $j \in \Omega$ inhabits:

\[ \{Hg_j, Hg_{\phi(j)}, \ldots, Hg_{\phi^{F-1}(j)}\} . \]

7. Proof of the Equivalence Theorem 1.6

**Proof.** Fix $\phi \in G$ with a certain cycle type. Let $\Omega = R = \{\alpha_1 = \alpha, \ldots, \alpha_n\}$ be the set of roots of $c$ in $L$, consistent with the notation of Theorem 1.2. Then $H = G_\alpha$ is the subgroup fixing $k(\alpha)$, so $(H \setminus G)/< \phi >$ produces the cycle type of $\phi$ by Lemma 6.2 and a splitting type for an unramified prime by Proposition 3.7. By Theorem 1.2, this is at the same time a factorization type.
8. Upper bound for the discriminant

Let \( k \) be a number field, \( c(x) \in k[x] \) be the irreducible polynomial for an algebraic integer \( \alpha \not\in k \), and \( K = k[\alpha] \). In this section we will prove the existence of an upper bound for the absolute value of the discriminant of the splitting field \( L \) of \( c(x) \), denoted by \( d_L \), only in terms of \( c(x) \) (Theorem 1.7). Lagarias et al. [6] prove the following theorem:

**Theorem 8.1** (Lagarias, Montgomery, Odlyzko). There is an absolute, effectively computable constant \( A \) such that for every number field \( k \), every normal extension \( L \) of \( k \), and every conjugacy class \( C \) of the Galois group of \( L \) over \( k \), there exists a prime ideal \( p \) of \( k \) which is unramified in \( L \), for which the conjugacy class of Frobenius automorphisms is \( C \), for which \( N_{k/Q}p \) is a rational prime, and which satisfies the bound

\[
N_{k/Q}p \leq 2d_L^A.
\]

(Note: The factor 2 in the bound is there only to take care of the trivial case \( L = k = Q \).)

**Corollary 8.2.** Let the notation be as in the above Theorem. Given any splitting type for primes of \( k \) unramified in \( L \), there exists at least one prime \( p \) of \( k \) with \( N_{k/Q}p \in \mathbb{Z} \) and \( N_{k/Q}p \leq 2d_L^A \) which exhibits this splitting type.

**Proof.** Divisions are unions of conjugacy classes. By Theorem 1.1, every splitting type corresponds to a division of the Galois group. \( \square \)

Taken together with Theorem 1.7, the Corollary clearly shows that tests for cycle types of Galois groups are deterministic. We will now take \( k = Q \) for simplicity. One way to find a discriminant upper bound would be to look for a primitive element \( \beta \) of \( L \) over \( Q \), compute its irreducible polynomial \( h(x) \), and find the discriminant of \( h(x) \) directly. Then we would have

\[
d_L \mid \text{disc}(\beta) = \text{disc}(h) \quad \text{and} \quad d_L \leq |\text{disc}(h)|
\]

(e.g., see Marcus [7], Problem 27, p.45). There exist algorithms to compute the discriminant of a given polynomial with integer coefficients, such as Schwarz et al. [8] (p.368) or the older, recursive algorithm in Brillhart [2].

Instead, we will provide a crude estimate of \( d_L \) in terms of \( c(x) \). We start with an effective version of the Primitive Element Theorem by Thunder and Wolfskill [9]:

**Theorem 8.3** (Thunder and Wolfskill). Let \( \alpha, \delta \) be algebraic integers with \( \alpha \not\in Q \) and \( \delta \not\in Q[\alpha] \). Let \( |Q[\alpha, \delta] : Q| = e \). Then \( Q[\alpha, \delta] = Q[\alpha + z\delta] \) for some \( z \in \mathbb{Z} \) satisfying \( |z| < e^2/2 \).

Now let \( \{\alpha = \alpha_1, \ldots, \alpha_n\} \) be the roots of \( c(x) \).
Corollary 8.4. We have

\[ L = \mathbb{Q}[\beta], \]

where

\[ \beta = \alpha_1 + z_2 \alpha_2 + \cdots + z_n \alpha_n \]

for some integers \( z_i \) with \( 0 \leq |z_i| < (n!)^2/2 \) for \( 2 \leq i \leq n \).

Note that there are \( 2^{[(n!)^2/2 - 1]} + 1 = (\frac{1}{2}n!)^2 \) possibilities for each \( z_i \), and altogether \( (n!)^2 \) possibilities for \( \beta \). We will fix \( z_2, \ldots, z_n \) and find an upper bound for this particular \( \beta \); the estimate will only depend on the upper bound \( (\frac{1}{2}n!)^2 \) of the \( z_i \)'s. The element \( \beta \) lives in \( \mathbb{Z}[\alpha_1, \ldots, \alpha_n] \), which is generated by

\[ \{1, \alpha_1, \ldots, \alpha_{n-1}^i\} \cup \cdots \cup \{1, \alpha_n, \ldots, \alpha_{n-1}^i\} \]

as a ring and by

\[ \{\alpha_1^{i_1} \cdots \alpha_n^{i_n} | 0 \leq i_1, \ldots, i_n \leq n - 1\} \]

as an abelian group. Let

\[ \{\gamma_1, \ldots, \gamma_n\} \]

be some ordering of the latter generating set, and \( \mathbf{G} \) be the \( n \times 1 \) vector with these components. We have

\[ \beta \mathbf{G} = M \mathbf{G} \]

for some \( n \times n \) matrix \( M \) with integer entries, so that \( \beta \) is an eigenvalue of \( M \) and a root of the characteristic polynomial \( k(x) \) of \( M \). The entries of \( M \) come from the bounded integers \( z_i \) and the coefficients of \( c(x) \): if \( c(x) = x^n - c_{n-1} x^{n-1} - \cdots - c_0 \), then \( \alpha_i^n = c_{n-1} \alpha_i^{n-1} + \cdots + c_0 \) for each \( i \). Therefore, there exists a computable upper bound on the coefficients of \( k(x) \).

We have found a monic irreducible polynomial \( k(x) \in \mathbb{Z}[x] \) with \( \beta \) as a root. The irreducible polynomial \( h(x) \in \mathbb{Z}[x] \) of \( \beta \) then divides \( k(x) \) in \( \mathbb{Z}[x] \). The discriminant of \( \beta \) (equivalently, of \( h \)) is given by

\[ \text{disc}(\beta) = \pm N \mathbb{Q}[\beta] h'(\beta) = \pm \prod_{\sigma} \sigma(h'(\beta)) = \pm \prod_{\sigma} h'(\sigma(\beta)) \]

(see Theorem 8 on p.26 of [7]), where \( \sigma \) ranges over the automorphisms of \( L \) fixing \( \mathbb{Q} \).

Lemma 8.5. Let \( k(x), h(x), r(x) \) be polynomials with complex coefficients. If \( k(x) = h(x)r(x) \) then the absolute values of the coefficients and roots of \( h(x) \) and \( r(x) \) have upper bounds which depend only on the coefficients of \( k(x) \).

Proof. Roots of \( h(x) \) and \( r(x) \) are also roots of \( k(x) \), and their size is bounded by an expression in the coefficients of \( k(x) \). The coefficients of \( h \) and \( r \), which are symmetric functions of their roots, are similarly bounded above. \( \square \)
The polynomial $h'(x)$ has coefficients with an upper bound coming from $h(x)$, and the roots $\sigma(\beta)$ of $h(x)$ are again bounded by an expression in the coefficients of $c(x)$ by the construction of $k(x)$ and by the Lemma. This concludes the proof of Theorem 1.7.

**Acknowledgments.** I would like to thank Tom Cusick, Steve Schanuel, and Don Schack (again) for encouraging this project way back when.

**References**

[1] F. Akman, Graph invariants of finite groups via a theorem of Lagarias, *JP Journal of Algebra, Number Theory and Applications* **8(2)** (2007), 227-258.

[2] O.J. Brillhart, On the Euler and Bernoulli polynomials, *J. Reine Angew. Math.* **234** (1969), 45-64.

[3] T.W. Hungerford, *Algebra*, Springer, 1974.

[4] L.-C. Kappe and B. Warren, An elementary test for the Galois group of a quartic polynomial, *The American Mathematical Monthly* **96(2)** (1989), 133-137.

[5] J.C. Lagarias, “Sets of primes determined by systems of polynomial congruences”, *Illinois J. of Math.* **27** (1983), 224-239.

[6] J.C. Lagarias, H.L. Montgomery, and A.M. Odlyzko, “A bound for the least prime ideal in the Chebotarev density theorem”, *Invent. Math.* **54** (1979), 271-296.

[7] D.A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.

[8] A. Schwarz, M. Pohst, and F. Diaz Y Diaz, A table of quintic number fields, *Mathematics of Computation* **63(207)** (1994), 361-376.

[9] J.L. Thunder and J. Wolfskill, Algebraic integers of small discriminant, *Acta Arithmetica* **75** (1996), 375-382.

[10] B.L. van der Waerden, *Algebra* (vol. 1, ed. 7, English translation), Frederick Ungar Publishing Company, New York, 1970.

Department of Mathematics, Illinois State University, Normal, IL 61790-4520

E-mail address: akmanf@ilstu.edu