Polynomials over Ring of Integers of Global Fields that have Roots Modulo Every Finite Indexed Subgroup

Bhawesh Mishra

Abstract
A polynomial with coefficients in the ring of integers $\mathcal{O}_K$ of a global field $K$ is called intersective if it has a root modulo every finite-indexed subgroup of $\mathcal{O}_K$. We prove two criteria for a polynomial $f(x) \in \mathcal{O}_K[x]$ to be intersective. One of these criteria is in terms of the Galois group of the splitting field of the polynomial, whereas the second criterion is verifiable entirely in terms of constants which depend upon $K$ and the polynomial $f$. The proofs use the theory of global field extensions and upper bound on the least prime ideal in the Chebotarev density theorem.

Keywords: Intersective Polynomials over Global Fields, Polynomial with Local Roots, Intersective Sets

2020 MSC: 12E10, 12E05, 11S05, 11C08

1. Introduction

1.1. Motivation
Let $q = p^r$ be power of a prime $p$ and $T$ be transcendental over $\mathbb{F}_q$. Let $\mathbb{F}_q(T)$ denote the field of rational functions with constant field $\mathbb{F}_q$ and $\mathbb{F}_q[T]$ denote the ring of polynomials with coefficients in $\mathbb{F}_q$. Recall that an extension $K$ of a field $M$ is said to be separable if for every $\alpha \in K$, the minimal polynomial $p_\alpha$ has distinct roots in the algebraic closure. For the ease of discussion, we will say that $K$ is a global field when $K$ is either of the following:

- An algebraic number field.
- A finite and separable extension of $\mathbb{F}_q(T)$, where $p$ is a prime and $q = p^r$ for some $r \geq 1$.

Let $\mathcal{O}_K$ be the ring of integers of $K$ when $K$ is a number field, whereas let $\mathcal{O}_K$ be the integral closure of the $\mathbb{F}_q[T]$ in $K$ in the function field case. This article is about polynomials $f(x) \in \mathcal{O}_K[x]$ such that for every subgroup $\Gamma$ of $\mathcal{O}_K$ of finite index, there exists $x \in \mathcal{O}_K$ with

$$f(x) \equiv 0 \pmod{\Gamma}. \quad (1.1)$$

Obviously, any $f$ that has a root in $\mathcal{O}_K$ satisfies (1.1) for trivial reasons. The more interesting case is when $f$ satisfies (1.1) but does not have a root in $K$. Each such $f$ constitutes a counterexample to the local-global principle.

Another motivation for studying polynomials $f$ that satisfy (1.1) comes from combinatorial number theory. A set $S \subset \mathcal{O}_K$ is said to be intersective if given any subset $T \subset \mathcal{O}_K$ with positive
upper density, one has \((T - T) \cap S \not\subset [0]\). The upper density of \(S \subset \mathcal{O}_K\) is given by

\[
\overline{d}(S) = \limsup_{N \to \infty} \frac{|S \cap \Phi_N|}{|\Phi_N|},
\]

where the sequence of sets \(\Phi_N\) are defined as:

\[
\Phi_N = \begin{cases} 
\{ \alpha \in \mathcal{O}_K : \text{Norm}(\alpha) \leq N \} & \text{when } K \text{ is a number field} \\
\{ \alpha \in \mathcal{O}_K : \deg(\alpha) \leq N \} & \text{when } K \text{ is a finite separable extension of } \mathbb{F}_q(T). 
\end{cases}
\]

For example, when \(K = \mathbb{Q}\), the sequence \(\Phi_N\) can be taken to be \([-N, N] \cap \mathbb{Z}\) for every \(N \geq 1\). When \(K\) is a finite separable extension of \(\mathbb{F}_q(T)\), the sequence \(\Phi_N\) is the set of divisors of degree \(\leq N\).

A polynomial \(f(x) \in \mathcal{O}_K[x]\) is said to be intersective if \(\{ f(\alpha) : \alpha \in \mathcal{O}_K \}\) is an intersective set. It was shown in [3] that a polynomial \(f(x) \in \mathbb{Z}[x]\) is intersective if and only if \(f\) satisfies (1.1).

A far reaching extension of this result was obtained in [4], a special instance of which implies that for a polynomial \(f(x) \in \mathbb{Z}[x]\) every subset of positive density in \(\mathbb{Z}\) contains arbitrarily long polynomial progressions of the form

\[
a, a+f(n), a+2f(n), \ldots, a+kf(n)
\]

if and only if \(f(x)\) is an intersective polynomial. A polynomial \(f(x) \in \mathcal{O}_K[x]\) is intersective if and only if it satisfies (1.1). This is implied by a very special case of Theorem 1.6 in [5] when \(K\) is a number field, and Theorem 1.15 in [1] gives the analogous result when \(K\) is a finite separable extension of \(\mathbb{F}_q(T)\). The same results in [1] and [5] also imply that intersectivity of polynomial \(f(x) \in \mathcal{O}_K[x]\) is equivalent to the fact that for every \(\alpha \in \mathcal{O}_K\), there exists \(\beta \in \mathcal{O}_K\) such that \(f(\beta) \equiv 0 \pmod{\alpha}\), i.e., \(f(\beta)\) is in the ideal generated by \(\alpha\).

Berend and Bilu, in [3], proved a criterion to decide whether a polynomial \(f(x) \in \mathbb{Z}[x]\) is intersective. In this article, we generalize the results in [3] to polynomials \(f(x) \in \mathcal{O}_K[x]\) when \(K\) is a global field. The methods in this article are generalizations of those in [3] in the settings of number fields and function fields respectively. In the process of proving the main result, we also derive an effective upper bound on the least prime ideal in the Chebotarev density theorem for function fields (see Proposition [2]).

### 1.2. Global Field Extensions and the Artin Symbols

Let \(L\) be a Galois extension of a global field \(K\). We will denote the set of primes in \(\mathcal{O}_K\) by \(\mathbb{P}(K)\). When \(K\) is an extension of \(\mathbb{F}_q(T)\), its field of constants is \(\mathbb{F}_d\) for some \(l \geq 1\). We will denote the set of primes of degree \(n\) by \(\mathbb{P}_n(K)\). Given a prime \(v \in \mathbb{P}(K)\), \(K_v\) will denote the corresponding completion of \(K\) and \(|\cdot|_v\) will denote the corresponding absolute value. If \(v \in \mathbb{P}(K)\) is unramified and \(\beta \in \mathbb{P}(L)\) lies over \(v\) then the Frobenius symbol \((\frac{L/K}{\beta})\) denotes the unique automorphism \(\varphi_v \in \text{Gal}(L/K)\) such that

\[
\varphi_v(\alpha) \equiv \alpha^{|v|} \pmod{\beta} \quad (1.2)
\]

for every \(\alpha \in \mathcal{O}_L\) and \(Nv = [\mathcal{O}_K : v]\).

Let \(L\) be the splitting field of a polynomial \(f(x) \in \mathcal{O}_K[x]\), all of whose irreducible factors are separable, and \(G\) be the Galois group of this extension \(L/K\). Note that when the characteristic of \(K\) is \(p > 0\), an irreducible polynomial \(f(x) \in \mathcal{O}_K[x]\) is not separable if and only if \(f(x) = g(x^p)\)
for some polynomial \(g\) and some integer \(n \geq 1\). Any prime \(p\) in \(O_K\) that does not divide the discriminant of \(f\), is unramified and hence splits as \(p = \beta_1 \beta_2 \cdots \beta_l\) for some primes \(\beta_1, \beta_2, \ldots, \beta_l\) in \(L\). We use the Artin symbol \(\left( \frac{L/K}{\beta_i} \right)\) to denote the set of conjugacy class of automorphisms

\[
\left[ \frac{L/K}{p} \right] = \left\{ \left( \frac{L/K}{\beta_1} \right), \left( \frac{L/K}{\beta_2} \right), \ldots, \left( \frac{L/K}{\beta_l} \right) \right\}.
\]

Let \(M\) be a subfield of \(L\) and \(\mathfrak{p}'\) be a prime in \(M\) that lies above \(p\). Then, for any \(1 \leq i \leq l\) we have

\[
\left( \frac{L/M}{\beta_i} \right) = \left( \frac{L/K}{\beta_i} \right)^{f_{\mathfrak{p}'}}.
\]

where \(f_{\mathfrak{p}'} = [M_{\mathfrak{p}'} : K]\). We also have the natural inclusion of the groups

\[
\Gal(L_{\beta_i}/M_{\mathfrak{p}'}) \leq \Gal(L/M) \leq \Gal(L/K),
\]

which gives that

\[
\left( \frac{L/K}{\beta_i} \right)^m \in \Gal(L/M) \text{ if and only if } f_{\mathfrak{p}'} \mid m. \tag{1.3}
\]

Readers may consult [7, Section 6.2] for more details on Artin Symbols for global field extensions. When \(L\) and \(K\) are number fields, \(d_i\) will denote the absolute discriminant of \(L\) and \(d_{L/K}\) will denote the relative discriminant of the extension \(L/K\). Furthermore, \(N_{L/K}\) will denote the corresponding norm. Given fields \(M_1, M_2\), we denote by \(M_1M_2\) the compositum of \(M_1\) and \(M_2\).

The genus of a separable and finite extension \(M\) of \(\mathbb{F}_q(T)\) is denoted by \(g_M\). The resultant of a polynomial \(f(x) \in O_K[x]\) is the resultant of \(f\) and its derivative \(f'\).

### 1.3. Setup and the Main Result

Let \(f(x) \in O_K[x]\) such that no non-unit divides all the coefficients of \(f\). If some non-unit \(\beta\) does divide every coefficient of \(f(x)\), we can replace \(f(x)\) by \(\frac{1}{\beta}f(x)\). Let \(g_1(x), g_2(x), \ldots, g_m(x)\) be the irreducible factors of \(f(x)\). When \(K\) is an extension of \(\mathbb{F}_q(T)\), we further assume that each of the irreducible factors of \(f\) are separable polynomials.

Let \(L\) be the splitting field of \(f\) over \(K\) and \(G = \Gal(L/K)\) be the Galois group of this extension. For every \(i \in \{1, 2, \ldots, m\}\), let \(a_i\) be a root of \(g_i\) that is fixed. Let \(L_i := K(a_i)\), which is an intermediate field between \(K\) and \(L\), let \(H_i := \Gal(L/L_i) \leq G\), and finally let \(U := \bigcup_{i=1}^m H_i \subseteq G\). For every \(1 \leq i \leq m\), let

\[
g_i(x) = \sum_{j=0}^{n_i} a_{ij}x^j
\]

for some \(a_{0i}, \ldots, a_{ni} \in O_K\). Also, let

- \(q_i\) be the discriminant ideal of the irreducible polynomial \(g_i\), which is non-zero because each of the \(g_i\) is separable.
- \(\tau_i = \text{resultant of } g_i \text{ and } g'_i\),
- \(q = \tau_1 \cdots \tau_m\),
- \(q = \nu_1^{b_1} \cdots \nu_v^{b_v}\) be the unique prime factorization of \(q\) in \(O_K\) and
• Define
\[ \Delta := p_1^{2b_1+1} \cdots p_{\nu}^{2b_{\nu}+1}. \]

• If \( K \) is a number field, define
\[ D := m \prod_{i=1}^{m} (q_i)^{(n_{i_1} \cdots n_{i_m})(1 - \frac{1}{n_i})}. \]

• If \( K \) is extension of \( \mathbb{F}_q(T) \), define
\[ \Delta' := \sum_{j=1}^{\nu} b_j \text{deg}(p_j) \in \mathbb{Z}, \]
\[ D' := \prod_{i=1}^{m} n_i! \]
and
\[ d = [K : \mathbb{F}_q(T)]. \]

Our main result gives two equivalent conditions for the polynomial \( f(x) \) to be intersective.

**Theorem 1.** Let \( K \) be a global field and \( f(x) \in O_K[x] \) be a polynomial such that all of its irreducible factors are separable. Then, the following three statements are equivalent:

1. \( f(x) \) is an intersective polynomial, i.e. \( f \) satisfies (1.1).
2. The congruence \( f(x) \equiv 0 \pmod{\Delta} \) is solvable in \( O_K \) and
\[ \bigcup_{\sigma \in G} \sigma^{-1} U \sigma = G. \]
3. \( f(x) \equiv 0 \pmod{\Delta} \) is solvable in \( O_K \) and
\[ f(x) \equiv 0 \pmod{p} \] is solvable for primes \( p \in O_K \)
with
\[ \begin{cases} \text{deg} (p) \leq [2 \log_q (2\Delta' + 2dD' + 8gKD' + 4)] & \text{if } K \text{ is extension of } \mathbb{F}_q(T) \\ N_{K/\mathbb{Q}}(p) \leq (N_{K/\mathbb{Q}}(D))^{12577} & \text{if } K \text{ is a number field and } L \neq \mathbb{Q}. \end{cases} \]

If \( L = \mathbb{Q} \), then solvability of \( f(x) \equiv 0 \pmod{\Delta} \) is the only condition to check.

Readers may note that the condition (2) in the above theorem involves Galois group of the splitting field. This condition is useful in creating families of examples of polynomials satisfying (1.1), for instance, as in Section 4. On the other hand, the condition (3) is feasible for checking intersectivity of a polynomial since it only involves constants \( \Delta, D, \Delta' \) and \( D' \), all of which can be calculated from the polynomial \( f \) itself.

The rest of this article is organized into three more sections. The second section contains statements and proofs of results that are required to prove Theorem 1. Section 3 contains the proof of Theorem 1. Section 4 contains some examples, consequences and discussions pertaining to the main result.
2. Some Preliminary Results

2.1. Roots Modulo Primes and the Artin Symbol

Proposition 1 gives a necessary and sufficient condition for an irreducible polynomial to have roots in $K_v$ for primes $v$ that do not divide the resultant of the polynomial $f$. Although this proposition can be proved using the decomposition and inertia subgroups of Gal $(L/K)$, we choose to provide a more accessible and elementary proof.

**Proposition 1.** Let $K$ be a global field and $g(x) \in O_K[x]$ be a separable irreducible polynomial. Let $L$ be the splitting field of $g$ and $G$ be the Galois group of $L$ over $K$. Also, let $v \in O_K$ be a prime that does not divide the resultant of the polynomial $g$. Then $g$ has a root modulo $v$ if and only if there exists an automorphism in $[L/K]$ that fixes some root of $g$.

**Proof.** Let $\theta_1, \theta_2, \ldots, \theta_n$ be the distinct roots of $g(x)$ in $L$ and $\beta \in \mathbb{P}(L)$ be a prime that lies above $v$. Assume that $g(\alpha) \equiv 0 \pmod{v}$ for some $\alpha \in O_K$. We will show that the Frobenius automorphism $\varphi_{\beta} \in [L/K]$ fixes one of the roots of $g$. Let us write $\varphi$ for $\varphi_{\beta}$ to avoid too many subscripts.

Since

$$g(\alpha) = \prod_{i=1}^{n}(\alpha - \theta_i) \equiv 0 \pmod{v},$$

we have that $vO_K | (\prod_{i=1}^{n}(\alpha - \theta_i))O_K$, and hence $vO_L | (\prod_{i=1}^{n}(\alpha - \theta_i))O_L$.

Since $\beta$ is a prime above $v$, we also have $\beta O_L | vO_L$, which along with $\beta O_L | (\prod_{i=1}^{n}(\alpha - \theta_i))O_L$ gives $\beta O_L | (\prod_{i=1}^{n}(\alpha - \theta_i))O_L$. Therefore, $\beta O_L | (\alpha - \theta_j)$ for some $j \in \{1, 2, \ldots, n\}$, i.e.,

$$\theta_j \equiv \alpha \pmod{\beta}.$$

The reduction of $\theta_j$ modulo $\beta$ is well-defined because $\beta$ is a prime above $v$, and $v$ is a prime that does not divide the resultant and hence, the leading coefficient of $g$. Since $\alpha \in O_K$, by definition of the Frobenius automorphism we have,

$$\varphi(\alpha) = \alpha \equiv \alpha O_K \pmod{\beta}.$$

Therefore, we have from (2.2) that,

$$\varphi(\theta_j) \equiv \theta_j^{O_K} \equiv \alpha^{O_K} \equiv \alpha \equiv \theta_j \pmod{\beta}$$

and hence

$$\theta_j \equiv \varphi^{-1}(\theta_j) \pmod{\varphi^{-1}(\beta)}.$$  

Using $T := \varphi^{-1} \in G$, (2.1) becomes

$$\theta_j \equiv T(\theta_j) \pmod{T(\beta)).$$

Since $T$ is an automorphism, $T(\theta_j) = \theta_l$ for some $l \in \{1, 2, \ldots, n\}$ and hence we have

$$\theta_j - \theta_l \equiv 0 \pmod{T(\beta))}.$$  

(2.2)

Here, reduction of $(\theta_j - \theta_l)$ modulo $T(\beta)$ is well-defined because $\theta_j$ is equivalent to $\alpha \in O_K \subseteq O_L$ modulo $\beta$ and hence $\theta_l = T(\theta_j)$ is also equivalent to an integral element of $L$. Recall that the resultant $r$ is defined to be

$$a^{2n-1} \prod_{1 \leq r \neq s \leq n} \prod_{\frac{a_{rs}}{5}} (\theta_r - \theta_s),$$
where \( a \) is the leading coefficient of \( g \). Since \( \theta_1, \theta_2, \ldots, \theta_n \) are distinct roots of \( g(x) \), if \( j \neq l \) then from (2.2) we have that
\[
t \equiv 0 \pmod{T(\beta)}, \tag{2.3}
\]
i.e., \( \mathfrak{p}O_L \subseteq T(\beta)O_L \), which implies \( \mathfrak{p}O_K \subseteq \mathfrak{p}O_K \) because \( \beta \), and hence \( T(\beta) \), is a prime above \( \mathfrak{p} \). However, \( \mathfrak{p}O_K \subseteq \mathfrak{p}O_K \) is a contradiction to the fact that \( \mathfrak{p} \) is a prime in \( O_K \) that does not divide the resultant \( r \) of \( g \). Therefore, we must have \( j = l \) and hence \( T(\theta_j) = \varphi^{-1}_\beta(\theta_j) = \theta_j \) i.e. the automorphism \( \varphi_\beta \) in \( \left[ \frac{L/K}{\beta} \right] \) fixes the root \( \theta_j \).

For the other direction, assume that \( \theta \) is a root of \( g(x) \) which is fixed by some Frobenius automorphism \( \varphi_\beta \in \left[ \frac{L/K}{\beta} \right] \), where \( \beta \) is a prime in \( O_L \) dividing \( \mathfrak{p} \). Therefore, we have
\[
\varphi_\beta(\theta) = \theta \equiv \theta^{\mathfrak{p} \mathfrak{p}(\theta)} \pmod{\beta}.
\]
Since \( \theta^{\mathfrak{p} \mathfrak{p}(\theta)} \equiv \theta \pmod{\beta} \) we must have that \( \theta \equiv \alpha \pmod{\beta} \) for some \( \alpha \in O_K \). Since \( \theta \) was a root of \( g \), we have \( g(\alpha) \equiv g(\theta) \equiv 0 \pmod{\beta} \) and hence \( g(\alpha) \equiv 0 \pmod{\mathfrak{p}} \).

2.2. Relating the Absolute Discriminant and the Ideal D in the Number Field Case

We will prove two propositions that relate the ideal \( D \) defined in Theorem 1 to the absolute discriminant \( d \) of the splitting field \( L \) of \( f \), in the case when \( K \) is a number field. The first proposition in this subsection is known but we include the proof for the sake of keeping the presentation largely self-contained. A proof of the second proposition when \( K = \mathbb{Z} \) appears in [3], which we adapt for number fields.

**Proposition 2.** Let \( M_1, M_2, \ldots, M_y \) be finitely many finite algebraic extensions of a number field \( K \) and \( M \) be the composite of these finitely many extensions. Let \( d_1, d_2, \ldots, d_y \) be the relative discriminant of \( M_1, M_2, \ldots, M_y \) respectively and \( d \) be that of \( M \). Then
\[
d \mid \left( \prod_{i=1}^y d_{M/M_i} \right).
\]

**Proof.** We will prove the proposition by induction on \( y \); let \( y = 2 \). Let \( \mathfrak{D}, \mathfrak{D}_1, \mathfrak{D}_2 \) and \( \mathfrak{D}^{(1)} \) respectively denote the relative different of the field extensions \( M/K, M_1/K, M_2/K \) and \( M/M_1 \). Note that the different \( \delta_{L/K}(\alpha) \) of an element \( \alpha \in O_L \) is defined in terms of its minimal polynomial \( m(x) \in O_K[x] \) as
\[
\delta_{L/K}(\alpha) = \begin{cases} m'(\alpha) ; & \text{if } L = K(\alpha) \\ 0 ; & \text{if } L \neq K(\alpha) \end{cases}
\]
We will also use the fact that the different \( \delta_{L/K} \) of a field extension \( L/K \) is the ideal generated by the set of all the element-wise differs \( \{ \delta_{L/K}(\alpha) : \alpha \in O_L \} \) (see [11, pp. 198, Theorem (2.5)])

First, we want to show that \( \mathfrak{D}^{(1)} \mid \mathfrak{D}_2 \), i.e., \( \mathfrak{D}_2 \subseteq \mathfrak{D}^{(1)} \).

Let \( \zeta \in O_{M_2} \) and \( M_2 = K(\zeta) \) without loss of generality (since \( \delta_{M_2/K}(\zeta) = 0 \) otherwise). By definition, we have that \( \delta_{M_2/K}(\zeta) = m'(\zeta) \) where \( m(x) \in O_K[x] \) is the minimal polynomial of \( \zeta \) over \( K \). On the other hand, the minimal polynomial \( p(\zeta) \in O_{M_2}[x] \) of \( \zeta \) over the field \( M_2 \) divides \( m(x) \). Therefore, \( \delta_{M_2/K}(\zeta) \equiv p'(\zeta) \pmod{\mathfrak{D}_2} \) which according to definition of different gives that \( \delta_{M_2/K}(\zeta) \in \mathfrak{D}_{M_2/K} = \mathfrak{D}^{(1)} \). Therefore, we have that \( \mathfrak{D}^{(1)} \mid \mathfrak{D}_2 \).

Now, using the multiplicity of the relative different of the tower of field extension \( M/M_1/K \) (for instance, see [11, pp. 195, proposition 2]) we also have
\[
\mathfrak{D} = \mathfrak{D}^{(1)} \mathfrak{D}_1,
\]
which together with \( \mathcal{D}^{(1)} | \mathcal{D} \) implies that \( \mathcal{D} | \mathcal{D}_1 \mathcal{D}_2 \). Upon applying \( N_{M/K} \) we have that \( d = N_{M/K}(\mathcal{D}) \) divides
\[
N_{M/K}(\mathcal{D}_1 \mathcal{D}_2) = N_{M_1/K}(N_{M/M_1}(\mathcal{D}_1)) \cdot N_{M_2/K}(N_{M/M_2}(\mathcal{D}_2))
\]
Since \( N_{M/M_i}(\mathcal{D}_1) = \mathcal{D}_1^{[M:M_i]} \), we have that \( N_{M/K}(N_{M/M_1}(\mathcal{D}_1)) = d_1^{[M:M_1]} \), which proves the proposition for \( \gamma = 2 \).

In the general case, given any \( \gamma \geq 3 \), let \( \tilde{M} \) be the composite of \( M_1, \ldots, M_{\gamma-1} \). Since \( M \) is the composite of \( \tilde{M} \) and \( M_\gamma \), we have
\[
d | (e^{[M:\tilde{M}]} \cdot d_\gamma^{[M:M_\gamma]}),
\]
where \( e \) is the relative discriminant of \( \tilde{M} \). By inductive assumption, we have that
\[
e | \prod_{i=1}^{\gamma-1} d_i^{[M:M_i]},
\]
which upon using the fact that \( [M : M_i] = [M : \tilde{M}] \cdot [\tilde{M} : M_i] \) proves the proposition. \( \square \)

**Proposition 3.** When \( K \) is a number field, Using the notations defined for Theorem 1, the absolute discriminant \( d_i \) divides \( N_{K/\mathbb{Q}}(D) \).

**Proof.** It suffices to prove that relative discriminant \( d_{L/K} \) of \( L \) divides \( D \) in \( K \); then the result follows by taking norm \( N_{K/\mathbb{Q}} \) to the ensuing divisibility relation. For every \( i \in \{1, 2, \ldots, m\} \):

- Let \( \alpha_i^{(1)} = \alpha_i, \alpha_i^{(2)}, \ldots, \alpha_i^{(n_i)} \) be the \( K \)-conjugates of \( \alpha_i \). Here \( \alpha_i \) is the fixed root of the irreducible factor \( g_i \) of \( f \).

- For every \( j \in \{1, 2, \ldots, n_i\} \), let \( L_i^{(j)} \) be the field \( K(\alpha_i^{(j)}) \). Since each of the \( \alpha_i^{(j)} \) are the roots of the same irreducible polynomial \( g_i \), we have that the relative discriminant of each of the \( L_i^{(j)} \) is equal to the relative discriminant \( d_i \) of \( L_i \).

- Let \( \overline{L_i} = K(\alpha_i^{(1)}, \alpha_i^{(2)}, \ldots, \alpha_i^{(n_i - 1)}, \alpha_i^{(n_i)}) \) be the splitting field of \( g_i \), which is the composite of the fields \( L_i^{(1)}, L_i^{(2)}, \ldots, L_i^{(n_i)} \).

Therefore, the relative discriminant \( \overline{d}_i \) of \( \overline{L_i} \) is such that
\[
\overline{d}_i \big| \prod_{j=1}^{n_i} d_i^{[L_i^{(j)} : L_i]} = d_i^{([\overline{L_i} : \overline{L_i}^{(n_i)}] - [\overline{L_i} : \overline{L_i}^{(n_i - 1)}])} | \overline{d}_i^{([\overline{L_i} : \overline{L_i}^{(n_i - 1)}]-1)!}
\]
(2.4)
The first divisibility is from Proposition 2 and the last divisibility relation in (2.4) is a consequence of the fact that the discriminant \( \delta_i \) of the polynomial \( g_i \) is always divisible by the relative discriminant \( d_i \) of \( L_i = K(\alpha_i) \), which we explain below.
For a fixed $i$, let $n = n_i$ which is the degree of the irreducible factor $g_i$, $a_j = a_{ij}$ and $\alpha = \alpha_i$. Consider the basis $\{\beta_1, \beta_2, \ldots, \beta_n\}$ of $L_i$ over $K$:

\[
\beta_1 = 1 \\
\beta_2 = a_n \alpha \\
\vdots \\
\beta_i = a_n a^{i-1} + a_{n-1} a^{i-2} + \ldots + a_{n-i+1} \alpha \\
\vdots \\
\beta_n = a_n a^{n-1} + a_{n-1} a^{n-2} + \ldots + a_1 \alpha
\]

We claim that $\beta_j$ are integral for every $j = 1, 2, \ldots, n$. Note that we have

\[
\beta_n a_n \alpha^{n-1} + a_{n-1} \alpha^{n-2} + \ldots + a_0 \alpha = -\frac{a_0}{\alpha} - a_1
\]

and for every $1 \leq i \leq (n - 2)$ one has

\[
\beta_{n-i} = a_n a^{n-i-1} a_{n-i} \alpha^{n-i-2} + \ldots + a_{i+2} \alpha \\
= -\frac{a_0}{\alpha^{i+1}} - \frac{a_1}{\alpha} - \ldots - \frac{a_i}{\alpha} - a_{i+1} \\
= \frac{\beta_{n-i+1}}{\alpha} - a_{i+1}
\]

(2.5)

Therefore, we will show that $\beta_{n-i}$ is integral for every $0 \leq i \leq (n - 1)$ by induction. For $i = 0$, note that since $\beta_n = -\frac{a_0}{\alpha} - a_1$ it suffices to prove that $y := \alpha$ is integral. Consider the following series of equivalent statements.

\[
a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_1 \alpha + a_0 = 0 \\
\Leftrightarrow a_n a^{n-1} + a_{n-1} a^{n-2} + \ldots + a_1 + \frac{a_0}{\alpha} = 0 \\
\Leftrightarrow \frac{a_n a_0^{n-1}}{\alpha^{n-1}} + \frac{a_{n-1} a_0^{n-2}}{\alpha^{n-2}} + \ldots + \frac{a_2 a_0}{\alpha} + a_1 + y = 0 \\
\Leftrightarrow y^n + a_1 y^{n-1} + a_2 a_0 y^{n-2} + \ldots + a_{n-1} a_0^{n-2} y + a_n a_0^{n-1} = 0,
\]

which shows that $y$ and hence $\beta_n$ is integral. Now, we assume that $\beta_{n-i+1}$ is integral and show that
\[ z := \frac{\beta_{n+1}}{\alpha} \] is also integral. Again, consider the following series of equivalent statements.

\[ a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_1 \alpha + a_0 = 0 \]
\[ \Leftrightarrow a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_{i+1} \alpha + \left( a_i + \frac{a_{i-1}}{\alpha} + \ldots + \frac{a_0}{\alpha^i} \right) = 0 \]
\[ \Leftrightarrow a_n \left( \frac{\beta_{n+1}}{\alpha} \right)^n + a_{n-1} \left( \frac{\beta_{n+1}}{\alpha} \right)^{n-1} + \ldots + a_{i+1} \left( \frac{\beta_{n+1}}{\alpha} \right)^{n-i} \frac{1}{z} - \beta_{n+i} = 0 \]
\[ \Leftrightarrow a_n \left( \frac{\beta_{n+1}}{\alpha} \right)^{n-i} + a_{n-1} \left( \frac{\beta_{n+1}}{\alpha} \right)^{n-i-1} + \ldots + a_{i+1} \frac{1}{z} - 1 = 0 \]
\[ \Leftrightarrow -z^{n-i} + a_{i+1} \frac{1}{z} \alpha^{n-i-1} + \ldots + a_{n} \left( \frac{\beta_{n+1}}{\alpha} \right)^{n-i-1} = 0, \]

which shows that \( z = \frac{\beta_{n+1}}{\alpha} \) and hence \( \beta_{n+1} = z - a_{i+1} \) is also integral. Since \( \beta_1, \beta_2, \ldots, \beta_n \) are integral in \( L_i \), we have that \( O[\beta_1, \beta_2, \ldots, \beta_n] \subseteq O_{L_i} \). However, we note that \( d(\beta_1, \beta_2, \ldots, \beta_n) = |\text{det}[\beta_j]| = a_n \), where \( \beta_j \) is defined exactly similarly as \( \beta_i \) but with the \( K \)-conjugate \( a^{(j)} \) of \( \alpha \). Therefore, from a well-known relationship between the discriminants of \( O_K \)-submodules (for instance, see [11] pp. 11, Proposition 2.12) we have that

\[ d(\beta_1, \beta_2, \ldots, \beta_n) = q_i = \left[ O_{L_i} : O[\beta_1, \ldots, \beta_n] \right]^2 d_i, \]

i.e., \( d_i \mid q_i \).

On the other hand, the splitting field \( L \) of the polynomial \( f \) is the composite of the splitting fields \( L_1, L_2, \ldots, L_m \) of the irreducible factors \( g_1, g_2, \ldots, g_m \) respectively. Hence if \( d_{L/K} \) is the relative discriminant of \( L \) then, Proposition 4 gives

\[ d_{L/K} \mid \prod_{i=1}^m (\tilde{a}_i)^{\ell_i} \prod_{i=1}^m \left( \tilde{a}_i \right)^{a_1 n_{1i} \ldots n_{mi} - n_i} \] (2.6)

From (2.4) and (2.6), we have that

\[ d_{L/K} \mid \prod_{i=1}^m \left( q_i \right)^{a_i^{(n_i - n_m)}(1 - \frac{1}{g_i})} = D. \]

\[ \square \]

2.3. Least Prime Ideal in the Chebotarev Density Theorem

To show that the condition (3) in Theorem 1 is equivalent to the condition (2), we will employ upper bounds on the prime ideal in the Chebotarev density theorem. The upper bound is well known in the number field case and we use the following version that is taken from [2].

**Proposition 4.** For every finite extension \( K \) of \( \mathbb{Q} \), for every finite Galois extension \( L(\not\equiv \mathbb{Q}) \) of \( K \) and every conjugacy class \( C \) of \( \text{Gal}(L/K) \), there exists a prime ideal \( \mathfrak{p} \) of \( K \) that is unramified in \( L \) such that:

- \( \left[ \frac{L/K}{\mathfrak{p}} \right] = C \) and
Proposition 5. \(N_{K/Q}(p)\) is a rational prime which satisfies
\[N_{K/Q}(p) \leq |d_l|^{12577}.\]

We also need a similar upper bound on the degree of the least prime ideal in the Chebotarev density theorem, when \(K\) is a finite separable extension of \(\mathbb{F}_q(T)\). Such an upper bound should ideally depend only upon the field \(K\) and the given polynomial \(f\). Assume that \(\mathbb{F}_q\) is the integral closure of \(\mathbb{F}_q\) in \(L\), for some \(l \geq 1\). The map
\[\varphi : \mathbb{F}_q \rightarrow \mathbb{F}_q\] given by \(\varphi(x) = x^g\)
is the generator of the \(\text{Gal}(\mathbb{F}_q/\mathbb{F}_q)\). On the other hand, we also have the surjective restriction \(\text{Gal}(L/K) \rightarrow \text{Gal}(\mathbb{F}_q/\mathbb{F}_q)\). Since \(\text{Gal}(\mathbb{F}_q/\mathbb{F}_q)\) is abelian, the image of a conjugacy class \(C \subset \text{Gal}(L/K)\) is a singleton set in \(\text{Gal}(\mathbb{F}_q/\mathbb{F}_q)\). Let \(\varphi_C := \varphi^e \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_q)\) be the image of every element of \(C\) under this restriction map. Given a conjugacy class \(C\) in \(G = \text{Gal}(L/K)\), define
\[\pi_{C,n} := \{p \in \mathbb{P}_q(K) : \left[\frac{L/K}{p}\right] = C\}.
In addition, define \(C_1 = [L : K\mathbb{F}_q]\). We will use the following effective version of the Chebotarev density theorem in function fields (see Proposition 6.4.8).

**Proposition 5.** Let \(C\) be a conjugacy class in \(G = \text{Gal}(L/K)\) and \(n \in \mathbb{N}\). If \(\varphi_C = \varphi^n\), then
\[\left|\pi_{C,n}\right| = \frac{|C|}{C_1} \frac{q^n}{n} < \frac{2|C|}{C_1} \left(\left(C_1 + g_L\right)q^n + C_1(2g_K + 1)q^{n/2} + g_L + C_1d\right),\]
(2.7)

Here, \(d = [K : \mathbb{F}_q(T)]\). On the other hand, if \(\varphi_C \neq \varphi^n\) then \(\pi_{C,n}\) is empty.

Given a Galois extension \(L\) of \(K\), which is a finite separable extension of \(\mathbb{F}_q(T)\), we have \(K \subseteq K\mathbb{F}_q \subseteq L\). Here, \(K\mathbb{F}_q/K\) is a constant field extension and \(L/K\mathbb{F}_q\) is a geometric field extension. To obtain the upper bound on the least prime ideal, we will use the Riemann-Hurwitz theorem (see Proposition 7.16).

**Proposition 6.** Let \(E_1/E_2\) be a finite, separable and geometric extension of functions fields. Then,
\[2g_{E_1} - 2 = [E_2 : E_1](2g_{E_1} - 2) + \deg_{E_1}(D_{E_2/E_1}),\]
(2.8)

where \(D_{E_2/E_1}\) is the different divisor of \(E_2/E_1\).

Now, we are ready to prove an upper bound on the least prime ideal in the Chebotarev density theorem for function fields.

**Proposition 7.** Let \(q\) be a prime power, \(K\) be a finite separable extension of \(\mathbb{F}_q(T)\). Using notations defined in Theorem 1, for any conjugacy class \(C \subset \text{Gal}(L/K)\) with \(\varphi_C = \varphi^n\), there exists an unramified prime \(p\) in \(K\) such that
\[
\begin{align*}
&\left[\frac{L/K}{p}\right] = C \\
&\deg(p) \leq \left\lceil 2 \log_q \left(2\Delta' + 2dD' + 8g_KD' + 4\right) \right\rceil.
\end{align*}
\]
Proof. Equation (2.7) implies that \( \pi_{C,n} \) is positive as soon as \( \frac{2\lvert C \rvert}{C_1 \cdot n} \) is greater than or equal to the RHS of (2.7). Note that the RHS of (2.7) is smaller than

\[
\frac{2\lvert C \rvert}{C_1 \cdot n} \left( 2C_1 + 2g_L + 2C_1g_K + dC_1 \right) q^{\frac{n}{2}}.
\]

Therefore, an upper bound on the smallest \( n \) such that \( \pi_{C,n} > 0 \) is the least \( n \) such that

\[
\frac{\lvert C \rvert q^n}{C_1 \cdot n} \geq \frac{2\lvert C \rvert}{C_1 \cdot n} \left( 2C_1 + 2g_L + 2C_1g_K + dC_1 \right) q^{\frac{n}{2}},
\]

i.e.

\[
n = \lceil 2 \log_q \left( 4C_1 + 4g_L + 4C_1g_K + 2dC_1 \right) \rceil. \tag{2.9}
\]

Consider the tower of field extensions \( K \subseteq \mathbb{KF}_q' \subseteq L \). Since genus does not change in a constant field extension over a perfect field (for instance, using \[12\], Proposition 8.9), we have that the genus of \( \mathbb{KF}_q' \) is equal to genus \( g_K \) of \( K \). On the other hand, using the Riemann-Hurwitz formula (2.8) for the geometric extension \( L/K\mathbb{KF}_q' \) with \( E_2 = L \) and \( E_1 = K\mathbb{KF}_q' \) gives us

\[
2g_L - 2 = (2g_K - 2)C_1 + \deg_{E_2}(D_{E_2/E_1}),
\]

and hence

\[
4g_L = 4g_KC_1 - 4C_1 + 4 + 2\cdot \deg_{E_2}(D_{E_2/E_1}). \tag{2.10}
\]

The degree of the different divisor is \( \sum_{v \in \mathbb{P}(K')} \delta(v) \deg(v) \), where \( \delta(v) \) is the highest power of \( v \) dividing the discriminant and the sum is taken over the primes \( v \) that are ramified. Since the relative discriminant \( q = v_1^{b_1} \cdots v_y^{b_y} \) is the relative norm of the different, the set of primes of \( \mathbb{KF}_q[T] \) that ramify in \( L \) are a subset of \( \{v_1, \ldots, v_y\} \). Therefore,

\[
\deg_{E_2}(D_{E_2/E_1}) \leq \sum_{i=1}^{y} b_i \deg(v_i). \tag{2.11}
\]

Using (2.10) and (2.11), we have that

\[
4g_L \leq 4g_KC_1 - 4C_1 + 4 + 2\cdot \sum_{i=1}^{y} b_i \deg(v_i) = 4g_KC_1 - 4C_1 + 4 + 2\Delta',
\]

which implies that

\[
(4C_1 + 4g_L + 4C_1g_K + 2dC_1) \leq 8g_KC_1 - 2dC_1 + 4 + 2\Delta'. \tag{2.12}
\]

Since the splitting field of the polynomial \( f \) is the compositum of the splitting fields of its individual irreducible factors, we have that \( [L : K] \leq \prod_{i=1}^{y} n_i! \). Therefore,

\[
C_1 = [L : K\mathbb{KF}_q'] \leq [L : K] \leq \prod_{i=1}^{y} n_i! = D'. \tag{2.13}
\]

Using (2.9), (2.12) and (2.13), we have that an upper bound for the degree \( n \) of the prime ideal in the Chebotarev density theorem is given by

\[
\lceil 2 \log_q (2\Delta' + 2dD' + 8g_KD' + 4) \rceil
\]

which proves the proposition. \(\square\)
3. Proof of Theorem 1

We will show that (2) $\implies$ (1) $\implies$ (3) $\implies$ (2), among which the implication (1) $\implies$ (3) follows trivially from definition of an intersective polynomial.

Proof of (2) implies (1).

If a prime $p \in \mathcal{O}_K$ does not divide $q$ then $f$ has a root in $K$, as a consequence of Proposition 1. To see this, we note that $\mathcal{O}_K$ divides $q$.

Therefore, we have $g_{\gamma} \equiv 0 \pmod{p}$, and hence, $h$, has a root modulo $p$.

1. To see this, we note that $\mathcal{O}_K$ divides $q$.

Proof of (2) implies (1).

If $p$ divides $q$ (i.e. $p = \mathcal{O}_K$) then, pick a $\gamma \in \mathcal{O}_K$ such that $f(\gamma) \equiv 0 \pmod{\Delta}$. Since $p = \mathcal{O}_K$, we have $|\gamma|_p = p_i^{-\nu_i}$. Furthermore, since $|\Delta|_p = p_i^{-\nu_i}$, $\mathcal{O}_K$. We will show that (2) $\implies$ (1).

Therefore, Proposition 1 implies that $g_{\gamma}$, and hence, $h$, has a root modulo $p$.

2. For primes $p$ dividing $q$, start by picking a $\gamma \in \mathcal{O}_K$ such that $f(\gamma) \equiv 0 \pmod{\Delta}$. We can see that $\gamma$ is a separable polynomial and hence its derivative is not identically zero. Therefore, $g_{\gamma}$ has a root in $K_p$ by the Hensel’s lemma (for example, see [1, Proposition 3.5.2]). Now the result follows from the standard application of the Chinese Remainder Theorem. □

Proof of (3) implies (2). For primes $p$ dividing $q$, start by picking a $\gamma \in \mathcal{O}_K$ such that $f(\gamma) \equiv 0 \pmod{\Delta}$. We can see that $\gamma$ is a separable polynomial and hence its derivative is not identically zero. Therefore, $g_{\gamma}$ has a root in $K_p$ by the Hensel’s lemma (for example, see [1, Proposition 3.5.2]). Now the result follows from the standard application of the Chinese Remainder Theorem. □

Proof of (3) implies (2). For primes $p$ dividing $q$, start by picking a $\gamma \in \mathcal{O}_K$ such that $f(\gamma) \equiv 0 \pmod{\Delta}$. We can see that $\gamma$ is a separable polynomial and hence its derivative is not identically zero. Therefore, $g_{\gamma}$ has a root in $K_p$ by the Hensel’s lemma (for example, see [1, Proposition 3.5.2]). Now the result follows from the standard application of the Chinese Remainder Theorem. □

We have used above that $|A(\gamma)|_p = |B(\gamma)|_p = 1$ because $A(x), B(x) \in \mathcal{O}_K[x]$ and $\gamma \in \mathcal{O}_K$ and also the fact that $g_{\gamma}$ is a separable polynomial and hence its derivative is not identically zero.

Therefore, $g_{\gamma}^2 = |r_j|_p^2 > |g_{\gamma}|_p$. Then, $g_{\gamma}$ has a root in $K_p$ by the Hensel’s lemma (for example, see [1, Proposition 3.5.2]). Now the result follows from the standard application of the Chinese Remainder Theorem.

Proof of (3) implies (2). For primes $p$ dividing $q$, start by picking a $\gamma \in \mathcal{O}_K$ such that $f(\gamma) \equiv 0 \pmod{\Delta}$. We can see that $\gamma$ is a separable polynomial and hence its derivative is not identically zero. Therefore, $g_{\gamma}^2 = |r_j|_p^2 > |g_{\gamma}|_p$. Then, $g_{\gamma}$ has a root in $K_p$ by the Hensel’s lemma (for example, see [1, Proposition 3.5.2]). Now the result follows from the standard application of the Chinese Remainder Theorem.
because \( d_L \) divides \( N_{K/Q}(D) \) as proved in Proposition 3. Both (a) and (b) together imply that

\[
\left\lfloor \frac{L/K}{p'} \right\rfloor \cap U \neq \emptyset
\]

if and only if

\[
\left\lfloor \frac{L/K}{p'} \right\rfloor \cap U \neq \emptyset
\]

for \( p' \) satisfying (3.1). In other words, \( f \) has a root in \( K \) if and only if \( f \) has a root in \( K_{p'} \) satisfying (3.1). By assumption of (3), along with Proposition 3, we have that the set of \( \left\lfloor \frac{L/K}{p} \right\rfloor \) as \( p' \) runs through

\[
N_{K/Q}(p') \leq |N_{K/Q}(D)|^{12577}
\]

is all of \( G \). In other words, every conjugacy class in \( G \) intersects \( U \) and hence \( \cup_{\sigma \in G} (\sigma^{-1} U \sigma) = G \). When \( L = Q \), \( f \) splits into linear factors and all the roots of \( f \) are rational. Therefore, the Galois group only contains identity, which fixes the root of every linear polynomial. Therefore, the Galois-theoretic condition in (2) is trivially satisfied.

In the case when \( K \) is an extension of \( F_q(T) \), the proof follows from exactly the same argument; except using the bound on the degree of least prime ideal as given in Proposition 7. \( \square \)

4. Corollaries, Examples and Discussion.

**Corollary 1.** Let \( f(x) \in O_K[x] \) be a polynomial with separable irreducible factors. If \( f \) is irreducible and of degree \( \geq 2 \), then \( f \) cannot be intersective. On the other hand, if \( f \) is intersective but does not have a root in \( K \), then degree of \( f \) must be at least 5.

**Proof.** We will use the notation defined before Theorem 1. Assume that \( f \) is irreducible and of degree \( \geq 2 \). From irreducibility of \( f \), we have \( U = H_1 \) and since \( \deg (f) > 1 \), we also have \( G \neq U \). Since \( U = H_1 \) is a proper subgroup of \( G \), we have that \( G/U = \{g_1 U, g_2 U, \ldots, g_k U\} \) for \( k = \frac{|G|}{|U|} \geq 2 \). Therefore we have,

\[
|\bigcup_{\sigma \in G} \sigma^{-1} U \sigma| = \left| \bigcup_{i=1}^{k} g_i^{-1} U g_i \right| < k|U| - (k - 1) = |G| - (k - 1) < |G|
\]

because \( k \geq 2 \). Therefore, we have \( G \neq \bigcup_{\sigma \in G} g^{-1} U g \) and hence Theorem 1 implies that \( f \) cannot have a root modulo every ideal of \( O_K \).

Now, assume that \( \deg (f) \leq 4 \) and that \( f \) has no roots in \( K \). We will prove that \( f \) cannot have root modulo every ideal in \( O_K \). Since \( f \) satisfies (1.1), \( f \) must be reducible by Corollary 1. The reducibility of \( f \), along with the fact that \( f \) has no roots in \( K \), implies that

\[
f(x) = \begin{cases} 
g_1(x)g_2(x) & \text{or} \\
g_1(x)^2 & \text{or} \\
g_1(x) & \text{,}
\end{cases}
\]

where \( g_1 \) and \( g_2 \) are irreducible quadratic polynomials in \( O_K[x] \). In the first case, the splitting field \( L \) of \( f \) has degree 4 over \( K \), whereas the splitting field of \( L \) has degree 2 in the latter two cases.
We first deal with the case when the splitting field has degree 4. Let \( \alpha_i, \beta_i \) be roots of \( g_i \), for \( i = 1, 2 \). Then the splitting field of \( f \) is \( L = K(\alpha_1, \alpha_2) \) and the Galois group of splitting field of \( f \) is \( G = \{e, \sigma_1, \sigma_2, \sigma_1\sigma_2\} \). Here, \( e \) is the identity map and
\[
\sigma_i(\alpha_i) = \beta_i \quad \text{and} \quad \sigma_i(\beta_i) = \alpha_i \quad \text{and} \quad \sigma_i \text{ fixes the roots of the other quadratic factor.}
\]
In other words, \( G \) is isomorphic to the Klein 4-group. Then, in the notation of Theorem 1 we have,
\[
H_1 = \mathrm{Gal}(L/K(\alpha_1)) = \{e, \sigma_2\} \quad \text{and} \quad H_2 = \mathrm{Gal}(L/K(\alpha_2)) = \{e, \sigma_1\}.
\]
Therefore, \( U = H_1 \cup H_2 = \{e, \sigma_1, \sigma_2\} \) and hence \( \cup_{g \in G} g^{-1}Ug = U \neq G \) i.e. \( f \) does not satisfy condition (2) of Theorem 1. Therefore, \( f \) cannot be intersective.

Now we deal with the case when splitting field \( L \) of \( f \) has degree 2 over \( K \). In this case, let \( \alpha \) be the root of only irreducible quadratic factor \( g_1 \). The splitting field is \( L = K(\alpha) \) with \( [L : K] = 2 \) and the Galois group \( G = \mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \) is generated by \( \sigma(\alpha) = -\alpha \). In the notation of Theorem 1, the only element of \( \mathrm{Gal}(L/K) \) that fixes the root \( \alpha \) is the identity element, i.e., \( U = \{e\} \). Therefore,
\[
\{e\} = \bigcup_{\sigma \in \mathbb{Z}} (\sigma^{-1}U\sigma) \neq G
\]
and hence \( f \) cannot be intersective. \( \square \)

### 4.1. An Example.

In this subsection, we will use Theorem 1 to construct a family of examples of intersective polynomials. Let \( q \) be a power of some odd prime, \( K = \mathbb{F}_q(T) \) and let
\[
f(x) = (x^2 - \theta_1)(x^2 - \theta_2)(x^2 - \theta_3) \in \mathcal{O}_K[x],
\]
where \( \theta_1 \) and \( \theta_2 \) are primes in \( \mathcal{O}_K = \mathbb{F}_q[T] \) that are non-associates. Recall that we require \( q \) to be odd here to ensure that the irreducible factors of \( f \) are all separable. To use the notations defined for Theorem 1 we denote the irreducible factors of \( f \) as:
\[
g_1(x) = (x^2 - \theta_1), \quad g_2(x) = (x^2 - \theta_2), \quad g_3(x) = (x^2 - \theta_1\theta_2).
\]
Since none of the \( \theta_i \) can be square in \( \mathcal{O}_K \), the splitting field of the polynomial \( f \) is
\[
L = K(\sqrt[4]{\theta_1}, \sqrt[4]{\theta_2}).
\]
Fix the roots \( \alpha_1 = \sqrt{\theta_1}, \alpha_2 = \sqrt{\theta_2}, \alpha_3 = \sqrt{\theta_1\theta_2} \) of \( g_1, g_2 \) and \( g_3 \) respectively. Note that the Galois group of this extension is given by
\[
G = \{e, \sigma_1, \sigma_2, \sigma_1\sigma_2\}.
\]
Here \( e \) is the identity map and for every \( i, j \in \{1, 2\} \)
\[
\sigma_i(\sqrt[4]{\theta_j}) = \begin{cases} -\sqrt[4]{\theta_j} & \text{if } i = j \\ \sqrt[4]{\theta_j} & \text{if } i \neq j. \end{cases}
\]
So, \( G \) is isomorphic to the Klein four-group, where each non-identity element has order 2. As in Theorem 1, let \( H_i \) be the subgroup of \( G \) that fixes the root \( \alpha_i \) of \( g_i \). Then,
• \( H_1 = \text{Gal}(L/K(\sqrt{\alpha})) = \{e, \sigma_2\} \leq G \),
• \( H_2 = \text{Gal}(L/K(\sqrt{\beta})) = \{e, \sigma_1\} \leq G \),
• \( H_3 = \text{Gal}(L/K(\sqrt{\gamma})) = \{e, \sigma_1 \sigma_2\} \leq G \).

Therefore,
\[
\bigcup_{\sigma \in G} (\sigma^{-1}U(\sigma)) = U = H_1 \cup H_2 \cup H_3 \cup H_4 = \{e, \sigma_1, \sigma_2, \sigma_1 \sigma_2\} = G.
\]

In addition, we also have that \( q = q_1 \cdot q_2 \cdot q_3 \) where \( q_1, q_2 \) and \( q_3 \) are ideals generated by \( \theta_1, \theta_2 \) and \( \theta_1 \theta_2 \) in \( \mathbb{F}_q[T] \) (since \( q \) is odd). Therefore, \( q = (\theta_1^2, \theta_2^2) \) and hence \( \Delta = (\theta_1^2, \theta_2^2) \). Since \( \theta_1 \) and \( \theta_2 \) are non-associates, using the Chinese Remainder Theorem and (2) of Theorem 1, we have that \( f(x) \) is intersective if and only if \( f(x) \equiv 0 \pmod{(\theta_i^2)} \) is solvable for \( i = 1, 2 \).

In fact, a similar argument also gives the same result when the above polynomial \( f(x) \) has coefficients over the ring of integers of a number field. Hence, we have the following corollary, where \( \langle \chi \rangle \) is used to denote the ideal \( xO_K \).

**Corollary 2.** Let \( K \) either be a number field or \( \mathbb{F}_q(T) \) for an integer \( q \) that is a power of an odd prime. Let \( \theta_1 \) and \( \theta_2 \) be non-associate primes in \( O_K \). Then the polynomial
\[
f(x) = (x^2 - \theta_1)(x^2 - \theta_2)(x^2 - \theta_1 \theta_2) \in O_K[x]
\]
is intersective if and only if \( \theta_1 \) is a square modulo \( (\theta_2^2) \) and \( \theta_2 \) is a square modulo \( (\theta_1^2) \).

**Proof.** From the explanation in [11] we have that \( f(x) \) is intersective if and only if \( f(x) \equiv 0 \pmod{(\theta_i^2)} \) is solvable for \( i = 1, 2 \). It suffices to show that \( f(x) \equiv 0 \pmod{(\theta_i^2)} \) is solvable if and only if \( \theta_2 \) is a square modulo \( (\theta_1^2) \). Analogously, the same fact will hold when the roles of \( \theta_1 \) and \( \theta_2 \) is reversed.

Now, we will show that neither \( \theta_1 \) nor \( \theta_2 \) can be a square modulo \( (\theta_1^2) \). In fact, we will only show that \( \theta_1 \theta_2 \) cannot be a square modulo \( (\theta_1^2) \). An exactly analogous proof, with \( \theta_1 \theta_2 \) replaced by \( \theta_1 \), that \( \theta_1 \) is not a square modulo \( (\theta_1^2) \).

Assume that \( y^2 \equiv \theta_1 \theta_2 \pmod{(\theta_1^2)} \) for some \( y \in O_K \), i.e., \( y^2 - \theta_1 \theta_2 \in (\theta_1^2) \subseteq (\theta_1) \). Since, \( y^2 - \theta_1 \theta_2 \in (\theta_1) \), we have that \( (\theta_1) \mid (y^2 - \theta_1 \theta_2) \) which implies that \( (\theta_1) \mid (\gamma^2) \) and hence \( (\theta_1) \mid (\gamma^2) \). However, \( (\theta_1^2) \mid (\gamma^2) \) along with \( y^2 - \theta_1 \theta_2 \in (\theta_1^2) \) gives that \( (\theta_1^2) \mid (\theta_1 \theta_2) \). This is a contradiction because \( \theta_1 \) and \( \theta_2 \) are non-associates. Therefore, the corollary is established.

### 4.2. Optimality of the Upper Bound in Theorem 1

The Proposition 6 and hence upper bound in (3) of Theorem 1, can be improved in the case when \( K \) is a number field, under the Generalized Riemann Hypothesis (GRH) for the Dedekind zeta function
\[
\zeta_K(s) = \sum_{I \in O_K} \frac{1}{N_{K/Q}(I)}.
\]

For example, assuming validity of the GRH for \( \zeta_L(s) \), the upper bound in Proposition 6, can be replaced by \( C(\log |d_L|)^2 \) for some constant \( C \) (see comments on Corollary 1.2 in [10], pp. 461–462]). Furthermore, it was demonstrated in [13] that this is the best possible bound for a general \( L \). Therefore, under GRH we can replace the upper bound in (3) of Theorem 1 by
\[
N_K/Q(p) \leq C(\log |N_K/Q(D)|)^2
\]
in the number field case. The upper bound in Proposition 4 admits significant asymptotic improvements (for large enough $d_L$) (see [8] and [13]). However, due to our interest in Theorem 1 for a general polynomial, we cannot use those results.

Acknowledgement

The author would like to thank Dr. Ofir Gorodetsky for an illuminating email conversation regarding the Chebotarev density theorem in global function fields.

References

[1] Ackelsberg, E. and Bergelson, V. (2021). A dynamical approach to bracket polynomials in finite characteristic and applications. Preprint https://drive.google.com/file/d/1jqHe1YqOBbr_0iIdDWUYUimbIjdMt3d8/view
[2] Ahn, J-H. and Kwon, S-H. (2019). An explicit upper bound for the least prime ideal in the Chebotarev density theorem. Ann. Inst. Fourier (Grenoble). 69 (3). 1411–1458.
[3] Berend, D. and Bilu, Y. (1996). Polynomials with Roots Modulo Every Integer. Proc. Amer. Math. Soc. 124 (6). 1663–1671.
[4] Bergelson, V., Leibman, A. and Lesigne, E. (2008). Intersective Polynomials and Polynomial Szemeredi Theorem. Adv. Math. 219. 369–388.
[5] Bergelson, V. and Robertson, D. (2016). Polynomial Multiple Recurrence Over Rings of Integers. Ergodic Theory Dynam. Systems. 36 (5). 1354–1378.
[6] Fiori, A. (2019). Lower Bounds for the Least Prime in Chebotarev. Algebra Number Theory. 13 (9). 2199–2203.
[7] Fried, M. D. and Jarden, M. Field Arithmetic, 2nd Ed. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics. vol. 11. Springer-Verlag, Berlin. 2005.
[8] Kadiri, H., Ng, N. and Wong, P-J. (2019). The Least Prime Ideal in the Chebotarev Density Theorem. Proc. Amer. Math. Soc. 147 (6). 2289–2303.
[9] Kamae, T. and Mendés-France, M. (1978). Van der Corput’s Difference Theorem. Israel J. Math. 31 (3-4). 335–342.
[10] Lagarias, J.C. and Odlyzko, A. M. (1977). Effective Versions of the Chebotarev Density Theorem. Algebraic Number Fields: L-functions and Galois properties (Proc. Sympos. Univ. Durham, Durham, 1975). Academic Press, London, 409–464.
[11] Neukrich, J. Algebraic Number Theory. (Translated from German by Norbert Schappacher). A Series of Comprehensive Studies in Mathematics Springer-Verlag, New York. 1999.
[12] Rosen, M. Number Theory in Function Fields. Graduate Texts in Mathematics. Springer-Verlag, New York. 2002.
[13] Zaman, A. (2017). Bounding the Least Prime Ideal in the Chebotarev Density Theorem. Funct. Approx. Comment. Math. 57 (1). 115–142.