Notes on Intersective Polynomials

Thesis

Presented in Partial Fulfillment of the Requirements for the Degree
Master of Science in the Graduate School of The Ohio State
University

By

Ethan Gegner, B.S.

Graduate Program in Mathematics

The Ohio State University

2018

Master’s Examination Committee:

Alexander Leibman, Advisor
Christopher Miller
Abstract

A polynomial $f(x)$ with integer coefficients is called *intersective* if for every $n \in \mathbb{N}$, there exists $a \in \mathbb{Z}$ such that

$$f(a) \equiv 0 \pmod{n}$$

We show that if $p$ is prime and $n, m$ are coprime integers such that every prime divisor of $mn$ is not congruent to 1 modulo $p$, and at least one of $n, m, mn, \ldots, mn^{p-1}$ is a $p$th residue modulo $p^2$, then

$$F(x) = (x^p - n) \prod_{k=0}^{p-1} (x^p - mn^k)$$

is intersective. In addition, we apply a result from [5] to prove that if $n$ is an integer greater than 4 and not divisible by 4, then there exists an intersective polynomial of degree $n$ which has no proper intersective factors.
Acknowledgments

I would like to express my deep gratitude to my advisor Alexander Leibman for taking me as an advisee, for his guidance, and for his many significant insights which contributed to the success of this thesis. It has truly been a great pleasure to work with him.

I would also like to thank Christopher Miller, who took the time to serve on my thesis committee and review my work.
Vita

2016 ........................................B.S. Mathematics,
        Taylor University
2017-present  ...........................Graduate Teaching Associate,
        The Ohio State University

Publications

Research Publications


Fields of Study

Major Field: Mathematics
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>ii</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>iii</td>
</tr>
<tr>
<td>Vita</td>
<td>iv</td>
</tr>
<tr>
<td>1. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2. Elementary Methods</td>
<td>5</td>
</tr>
<tr>
<td>2.1 Basic Examples</td>
<td>5</td>
</tr>
<tr>
<td>2.2 A General Class</td>
<td>9</td>
</tr>
<tr>
<td>2.3 2-Intersecting Quadratics</td>
<td>13</td>
</tr>
<tr>
<td>3. Intersective polynomials and Galois Theory</td>
<td>15</td>
</tr>
<tr>
<td>3.1 A Theorem of Berend and Bilu</td>
<td>15</td>
</tr>
<tr>
<td>3.2 Normal Covers</td>
<td>17</td>
</tr>
<tr>
<td>3.3 Density</td>
<td>22</td>
</tr>
<tr>
<td>Bibliography</td>
<td>25</td>
</tr>
</tbody>
</table>
A polynomial \( f(x) \) with integer coefficients is called \textit{intersective} if for every \( n \in \mathbb{N} \), there exists \( a \in \mathbb{Z} \) such that
\[
f(a) \equiv 0 \pmod{n}
\] (1.1)

We denote the set of all intersective polynomials by \( \mathcal{I} \). If \( f \in \mathbb{Z}[x] \) has a root \( a \in \mathbb{Z} \), then (1.1) holds for all \( n \), so \( f \) is intersective. If \( f \in \mathbb{Z}[x] \) has a rational root \( r/s \) (where \( r, s \) are coprime integers), then \( f \) is “nearly” intersective, in the sense that \( f \) has a solution modulo \( n \) for every \( n \) coprime to \( s \). It is therefore easy to find intersective polynomials by taking products of polynomials with rational roots. Such a polynomial is said to be \textit{trivially intersective}.

Berend and Bilu ([1]) gave a method (Theorem 3.1) by which it may be determined whether any given integer polynomial is intersective. Their theorem relies on Galois Theory. The problem of finding intersective polynomials is motivated by some problems in ergodic Ramsey theory (see [1], [2]). Elementary methods are given in [7] for determining whether certain polynomials of small degree are intersective, but in general such elementary methods are very limited in scope.

As Sonn remarks in [6], there remain few explicit examples of intersective polynomials in the literature. Two kinds of intersective polynomials are of particular interest: those of small degree and those which have a small number of irreducible
factors. The classic example is \( f(x) = (x^3 - 19)(x^2 + x + 1) \), which—as we shall see—is minimal by both counts (excluding linear polynomials).

We will present a new class of intersective polynomials. In particular, we will show that if \( p \) is prime and \( n, m \) are coprime integers such that every prime divisor of \( mn \) is not congruent to 1 modulo \( p \), and at least one of \( n, m, mn, \ldots, mn^{p-1} \) is a \( p \)th residue modulo \( p^2 \), then

\[
F(x) = (x^p - n) \prod_{k=0}^{p-1} (x^p - mn^k)
\]

is intersective.

Some general results are known. For \( f \in \mathbb{Z}[x] \), we define \( G(f) = \text{Gal}(K/\mathbb{Q}) \), where \( K \) is the splitting field of \( f \) over \( \mathbb{Q} \). It is proved in [5] that for \( m > 1 \), and for any finite solvable group \( G \) which is the union of the conjugates of \( m \) proper subgroups of \( G \) (with the intersection of all conjugates being trivial), there exists an intersective polynomial \( f \) such that \( G(f) = G \). Brandl ([3]) proved that if \( f \in \mathcal{I} \) is the product of two irreducible (over \( \mathbb{Q} \)) monic integer polynomials \( f_1, f_2 \) with roots \( \alpha_1, \alpha_2 \), respectively, and if \( K/\mathbb{Q}(\alpha_i) \) is cyclic for \( i = 1, 2 \), then \( G(f) \) is solvable.

**Definition 1.1.** For \( n \in \mathbb{N} \), we say that \( f \) is \( n \)-intersective if for every \( k \in \mathbb{N} \), there is some \( a \in \mathbb{Z} \) such that \( f(a) \equiv 0 \) (mod \( n^k \)). The set of \( n \)-intersective polynomials is denoted by \( \mathcal{I}_n \). For all \( k \in \mathbb{N} \), we denote the set of all intersective polynomials which are the product of exactly \( k \) irreducible (over \( \mathbb{Q} \)) polynomials in \( \mathbb{Z}[x] \) by \( \mathcal{J}_k \).

In particular, \( \mathcal{J}_1 \) is the set of all irreducible (over \( \mathbb{Q} \)) intersective polynomials. We shall soon see that \( \mathcal{J}_1 \) is precisely the set of all linear polynomials which have an integer root.
We say that a polynomial \( f \in \mathcal{I} \) is \textit{minimally intersective} if \( f \) has no proper intersective factors. If \( f \in \mathcal{I} \) is minimally intersective and \( g \in \mathbb{Z}[x] \setminus \mathcal{I} \), then \( fg \in \mathcal{I} \) is irreducible in \( \mathcal{I} \), but not minimally intersective. Thus, every minimally intersective polynomial is irreducible in \( \mathcal{I} \), but the converse is not true. For example, \( x(x^2 - 2) \) is intersective and irreducible in \( \mathcal{I} \) (\( x^2 - 2 \) has no root modulo 4), but not minimally intersective, since \( x \) itself is intersective.

We shall use \( \mathbb{P} \) to denote the set of prime numbers. For \( r, m \in \mathbb{Z} \), we define

\[
\mathcal{P}_{m,r} = \{ p \in \mathbb{P} : p \equiv r \pmod{m} \}
\]

For \( f \in \mathbb{Z}[x] \), we define

\[
\mathbf{p}(f) = \{ p \in \mathbb{P} : f \in \mathcal{I}_p \}
\]

Let us make a few observations. First, \( f \in \mathcal{I}_p \) if and only if \( p \in \mathbf{p}(f) \). If \( f, g \in \mathbb{Z}[x] \) and \( g \) divides \( f \), then \( \mathbf{p}(g) \subseteq \mathbf{p}(f) \). Finally, note that if \( f_1, f_2 \in \mathbb{Z}[x] \), then \( \mathbf{p}(f_1f_2) = \mathbf{p}(f_1) \cup \mathbf{p}(f_2) \).

We shall now show that the problem of finding intersective polynomials is a special case of determining \( \mathbf{p}(f) \). Fix \( n \in \mathbb{N} \), and let \( p_1^{e_1} \cdots p_k^{e_k} \) be the prime factorization of \( n \), with the \( p_i \) distinct. Let \( f \in \mathbb{Z}[x] \), and suppose that \( f \in \mathcal{I}_{p_i} \) for \( 1 \leq i \leq k \). Then for every \( 1 \leq i \leq k \), there is some \( a_i \) such that \( p_i^{e_i} \mid f(a_i) \). By the Chinese Remainder Theorem, there exists \( b \in \mathbb{Z} \) such that \( b \equiv a_i \pmod{p_i^{e_i}} \) for all \( 1 \leq i \leq k \). Then

\[
f(s) \equiv f(a_i) \equiv 0 \pmod{p_i^{e_i}}
\]

for \( 1 \leq i \leq k \), whence \( f(s) \equiv 0 \pmod{n} \). Thus, \( f \in \mathcal{I}_n \). Since \( \mathcal{I}_{p_i} \subset \mathcal{I}_n \) for all \( 1 \leq i \leq k \), this shows that

\[
\mathcal{I}_n = \bigcap_{p \in \mathbb{P}} \mathcal{I}_p \quad \text{(1.2)}
\]

3
By equation (1.2), it follows that

$$\mathcal{I} = \bigcap_{n=1}^{\infty} \mathcal{I}_n = \bigcap_{p \in \mathbb{P}} \mathcal{I}_p$$

Thus, \( \mathcal{I} = \{ f \in \mathbb{Z}[x] : p(f) = \mathbb{P} \} \).
Chapter 2: Elementary Methods

Here we shall discuss elementary methods pertaining to the intersectivity of certain polynomials. Some elementary techniques are discussed in [7]. For example, criteria are given to determine if a polynomial \( f \in \mathbb{Z}[x] \) of degree less than 4 is \( p \)-intersective for a fixed odd prime \( p \). We shall present some of the results in [7]. Additionally, we shall give a number of interesting examples of intersective polynomials not given in [7], including an entirely new class of intersective polynomials.

2.1 Basic Examples

We begin with some simple observations. Given an intersective polynomial \( f \), there are a number of straightforward ways to produce new intersective polynomials from \( f \). Any multiple of an intersective polynomial is intersective. If \( f \in \mathbb{Z}[x] \) and \( m \in \mathbb{Z} \), then \( f(x) \in \mathcal{I} \) if and only if \( f(x + m) \in \mathcal{I} \). If \( f \in \mathbb{Z}[x] \) with \( f(0) = 0 \), and \( g \in \mathcal{I} \), then \( f \circ g \in \mathcal{I} \). If \( f, g \in \mathbb{Z}[x] \) with \( g \notin \mathcal{I} \), then \( g \circ f \notin \mathcal{I} \). If \( f(x) = h_1(x)h_2(x) \in \mathcal{I} \) and \( h_1 \in \mathcal{I}_p \) for some prime \( p \), then \( h_1(x)h_2(p^kx) \in \mathcal{I} \) for all \( k \in \mathbb{N} \).

**Example 2.1.** Let \( h(x) = x^4 + 2x^3 + 4x^2 + 3x + 3 \). We claim that \( h \notin \mathcal{I} \). To see this, simply note that that \( h = f \circ f \), where \( f = x^2 + x + 1 \) is not intersective by Corollary 3.2.
Thus, given any polynomial \( f \in \mathcal{I} \), we can generate new intersective polynomials with ease; similarly, if \( f \notin \mathcal{I} \), we can immediately obtain many more non-intersective polynomials. The real problem, then, is finding intersective polynomials to start with. It is to this task we now turn.

The basis for many of the elementary results is known as Hensel’s Lemma.

**Lemma 2.2** (Hensel). Let \( f \in \mathbb{Z}[x] \), let \( p \) be prime, and let \( k \in \mathbb{N} \). If \( a \in \mathbb{Z} \) such that \( p^k | f(a) \) and \( p \nmid f'(a) \), then there is a unique \( t \) modulo \( p \) such that \( p^{k+1} | f(a + tp^k) \).

**Proof.** Write \( f(x) = \sum_{r=0}^{m} b_r x^r \). By hypothesis, there exists \( s \in \mathbb{Z} \) such that \( f(a) = sp^k \).

Since \( p \nmid f'(a) \), \( f'(a) \) has an inverse \( z \) in \( \mathbb{Z}_p^* \). Let \( t \in \{0, \ldots, p-1\} \). Then

\[
f(a + tp^k) = \sum_{r=0}^{m} b_r (a + tp^k)^r
\]

\[
\equiv \sum_{r=0}^{m} b_r \sum_{j=0}^{r} \left( \begin{array}{c} r \\ j \end{array} \right) a^j t^{r-j} (p^k)^{r-j}
\]

\[
\equiv \sum_{r=0}^{m} b_r \left( \left( \begin{array}{c} r \\ r \end{array} \right) a^r + \left( \begin{array}{c} r \\ r-1 \end{array} \right) a^{r-1} t p^k \right)
\]

\[
\equiv \sum_{r=0}^{m} b_r a^{r-1} (a + rtp^k)
\]

\[
\equiv f(a) + t p^k f'(a)
\]

\[
\equiv p^k \left( s + tf'(a) \right) \pmod{p^{k+1}}
\]

Thus, \( f(a + tp^k) \equiv 0 \pmod{p^{k+1}} \) if and only if \( t \equiv -sz \pmod{p} \).

As an immediate corollary, we obtain a result which will prove to be quite useful.

**Corollary 2.3.** Let \( f \in \mathbb{Z}[x] \), and let \( p \) be prime. If there exists \( a \in \mathbb{Z} \) such that \( p | f(a) \) and \( p \nmid f'(a) \), then \( f \in \mathcal{I}_p \).

**Example 2.4.** Let \( f(x) = x^2 + x + 1 \). Since \( f \) has no root modulo 2, \( f \) is not intersective. However, \( f(2) = 7 \) and \( f'(2) = 5 \), so by Corollary 2.3, \( f \in \mathcal{I}_7 \).
The following result is proved in [7], but with the addition of several unnecessary hypotheses. Here we state and prove the more general result.

**Theorem 2.5.** Let $p$ be prime, let $r \in \mathbb{Z}$ such that $p \nmid r$, let $m \in \mathbb{N} \cup \{0\}$, and let $f(x) = x^p - rp^m$. Then $f \in \mathcal{I}_p$ if and only if $p|m$ and there exists $a \in \mathbb{Z}$ such that $a^p - r \equiv 0 \pmod{p^2}$.

**Proof.** Suppose $f \in \mathcal{I}_p$. Then by definition $f$ has a root $a$ modulo $p^{m+1}$. There exist $s \in \mathbb{Z}$ and $t \in \mathbb{N} \cup \{0\}$ such that $a = sp^t$. Since $p^{m+1} | (sp^tp^t - rp^m)$, it follows that $p^m | p^{pt}$ and $\min(p^{m+1}, p^{pt}) | p^m$; the former implies $m \leq pt$, and the latter implies $pt < m + 1$. Thus, $m = pt$.

Since $f \in \mathcal{I}_p$, $f$ has a root $b$ modulo $p^{pt+2}$. Thus, $p^{pt+2} | (b^p - rp^{pt})$, whence $p^t | b$.

Thus, there exists $u \in \mathbb{Z}$ such that $b = up^t$. Then

$$p^{pt+2} | (up^tp^t - rp^{pt}) = p^{pt}(u^p - r)$$

so that $u^p - r \equiv 0 \pmod{p^2}$.

Conversely, suppose that $p|m$ and $a^2 - r \equiv 0 \pmod{p^2}$ for some $a \in \mathbb{Z}$. We shall show by induction that for each $k \geq 2$, there exists $a_k \in \mathbb{Z}$ such that $a_k^p - r \equiv 0 \pmod{p^k}$. Fix $k$, and assume that $a_k^p - r \equiv 0$ for some $a_k \in \mathbb{Z}$. If $a_k^p - r \equiv 0 \pmod{p^{k+1}}$, then take $a_{k+1} = a_k$. Suppose $a_k^p - r \not\equiv 0 \pmod{p^{k+1}}$. Then there exists $z \in \mathbb{Z}$ such that $p \nmid z$ and $a_k^p - r = zp^k$. Since $(r, p) = 1$, we must have $(a_k, p) = 1$. Thus, there exists $w \in \mathbb{Z}$ such
that $p | (z + wa_k^{p-1})$. Put $a_{k+1} = a_k + p^{k-1}w$. Then
\begin{align*}
a_{k+1}^p - r &= (a_k + wp^{k-1})^p \\
&= a_k^p - r + \sum_{i=0}^{p-1} \binom{p}{i} a_k^i w^{p-i} p^{(k-1)(p-i)} \\
&
\equiv zp^k + \left( \frac{p}{p-1} \right) a_k^{p-1} wp^{k-1} \\
&
\equiv p^k (z + a_k^{p-1}w) \\
&
\equiv 0 \pmod{p^{k+1}}
\end{align*}

This completes the inductive step.

To complete the proof, note that since $p | m$, there exists $c \in \mathbb{N} \cup \{0\}$ such that $m = cp$. Thus, for all $k \geq 2$,
\begin{align*}
(p^ca_k)^p - rp^m &= p^m (a_k^p - r) \equiv 0 \pmod{p^k}
\end{align*}
In particular, $f$ has an integer root modulo $p^k$ for all $k \in \mathbb{N}$.

**Example 2.6.** Let $p$ and $q$ be odd primes such that each is a quadratic residue modulo the other. Let $f(x) = (x^2 - p)(x^2 - q)(x^2 - pq)$. We claim that $f$ is intersective. Since $p$ is a quadratic residue mod $q$, the polynomial $g(x) = x^2 - p$ has a root $\alpha$ in $\mathbb{Z}_q$. Since $g'(\alpha) = 2\alpha$ is not divisible by $q$, by Hensel’s Lemma it follows that $g \in \mathcal{I}_q$. Thus, $f \in \mathcal{I}_q$. By the same argument, $f \in \mathcal{I}_p$.

If $p \not\equiv 1 \pmod{4}$ and $q \not\equiv 1 \pmod{4}$, then $p \equiv 3 \equiv q \pmod{4}$, whence $pq \equiv 1 \pmod{4}$. Thus, at least one of $p, q, pq$ is congruent to 1 modulo $2^2$. Consequently, at least one of $(x^2 - p), (x^2 - q), (x^2 - pq)$ has a root in $\mathbb{Z}_4$. By Theorem 2.5, $f \in \mathcal{I}_2$.

Let $r$ be a prime not equal to 2, $p, q$. If both $p$ and $q$ are quadratic non-residues of $r$, then $pq$ is a quadratic residue of $r$. In particular, there is some $c \in \{p, q, pq\}$ such that $h(x) = x^2 - c$ has a root $\beta$ modulo $r$. Since $h'(\beta) = 2\beta \not\equiv 0 \pmod{r}$, by Hensel’s Lemma it follows that $r \in \mathcal{p}(h) \subset \mathcal{p}(f)$. This proves that $f \in \mathcal{I}$.  

8
The following two propositions are proven in [7].

**Proposition 2.7.** Let \( q > 3 \) be prime, and let \( r \) be an integer such that \( kq + r \) for all \( k \in \mathbb{N} \). Let \( f(x) = x^q - r \). Suppose \( p \) is a prime such that \( p \not\equiv q \pmod{q} \), and \( p \not\mid r \). Then \( f \in \mathcal{I}_p \).

**Proposition 2.8.** Let \( p \) be prime. Let \( f(x) = \sum_{k=0}^{p} x^k \). Then \( p(f) = \mathcal{P}_{p,1} \).

**Example 2.9.** Let

\[
f(x) = (x^5 - 31)(x^4 + x^3 + x^2 + x + 1)
\]

We claim that \( f \) is intersective. Let \( g(x) = x^4 + x^3 + x^2 + x + 1 \). Then by Proposition 2.8, \( p(g) = \mathcal{P}_{5,1} \). By Proposition 2.7, \( \mathcal{P} \setminus \mathcal{P}_{5,1} \subset p(x^5 - 31) \) (observe that \( 31 \in \mathcal{P}_{5,1} \)). Thus, \( f(x) \in \mathcal{I} \).

### 2.2 A General Class

For a set \( M \), \( \mathcal{P}(M) \) shall denote the power set of \( M \). For any prime \( q \), let \( \alpha_q \) be a primitive root modulo \( q \), and define \( \varphi_q : \mathbb{Z}_q^* \to \mathbb{Z}_{q-1} \) by \( \varphi_q(\alpha_q^k) = k \). Fix \( q \). Then for any \( k_1, k_2 \in \mathbb{Z} \),

\[
\varphi_q(\alpha_q^{k_1} \alpha_q^{k_2}) = \varphi_q(\alpha_q^{k_1+k_2}) = k_1 + k_2 = \varphi_q(\alpha_q^{k_1}) + \varphi_q(\alpha_q^{k_2})
\]

so \( \varphi_q \) is a group homomorphism. Since \( \ker(\varphi_q) = 1 \), \( \varphi_q \) is injective. Since \( |\mathbb{Z}_q^*| = q - 1 = |\mathbb{Z}_{q-1}| \), \( \varphi_q \) must also be surjective. Thus, \( \varphi_q \) is an isomorphism.

**Lemma 2.10.** Let \( p \) be prime. Let \( a_1, \ldots, a_\ell \in \mathbb{Z} \) such that \( a_i \not\equiv 0,1 \pmod{p} \) for all \( 1 \leq i \leq \ell \), and suppose that \( \mathcal{F} \subset \mathcal{P}(\{1, \ldots, \ell\}) \) such that

1. there exist \( R_1, R_2 \in \mathcal{F} \) such that \( \prod_{i \in R_1} a_i \) and \( \prod_{i \in R_2} a_i \) are relatively prime
2. for every prime \( q \) such that \( q \equiv 1 \pmod{p} \), there exists \( S_q \in \mathcal{F} \) such that
\[
p \mid \sum_{i \in S_q} \varphi_q(a_i)
\]
Let
\[
f(x) = \prod_{T \in \mathcal{F}} \left( x^p - \prod_{i \in T} a_i \right)
\]
Then \( \mathbb{P} \setminus \{ p \} \subset \mathfrak{p}(f) \).

Proof. Let \( q \) be a prime not equal to \( p \). Let \( \alpha = \alpha_q, \varphi = \varphi_q \).

First suppose that \( q \not\equiv 1 \pmod{p} \). Then \( p \) is invertible in \( \mathbb{Z}_{q-1}^* \). Moreover, by condition (1), there exists \( k \in \{1, 2\} \) such that \( q \mid \prod_{i \in R_k} a_i \). Let \( n = \prod_{i \in R_k} a_i \). Then there exists \( a \in \mathbb{Z}_q^* \) such that \( p \varphi(a) = \varphi(n) \). Since \( \varphi \) is an isomorphism, \( a^p \equiv n \pmod{q} \). Let \( g(x) = x^p - n \). We have shown that \( g(a) \equiv 0 \pmod{q} \). Since \( g'(a) = pa^{p-1} \) is not divisible by \( q \), it follows by Corollary 2.3 that \( q \in \mathfrak{p}(g) \subset \mathfrak{p}(f) \).

Now suppose \( q \equiv 1 \pmod{p} \). Let \( H = \{ m^p : m \in \mathbb{Z}_q^* \} \). Then
\[
\varphi(H) = \{ p\varphi(a^k) : 1 \leq k \leq q - 1 \} = \{ pk \mod(q-1) : 1 \leq k \leq q - 1 \}
\]
Let \( b = \prod_{i \in S_q} a_i \). By hypothesis (2), it follows that
\[
\varphi(b) = \sum_{i \in S_q} \varphi(a_i) \in \varphi(H)
\]
whence \( b \in H \). In particular, the polynomial \( h(x) = x^p - b \) has a root \( r \) in \( \mathbb{Z}_q^* \). Moreover, since \( h'(r) = pr^{p-1} \) is not divisible by \( q \), it follows by Corollary 2.3 that \( q \in \mathfrak{p}(h) \subset \mathfrak{p}(f) \).

Since \( q \) was arbitrary, the result follows. \( \square \)

While the previous lemma is certainly interesting, it may at first glance appear that the second hypothesis is unreasonably difficult to satisfy, therefore limiting the application of the lemma. However, we shall now present a class of polynomials to which the lemma may be applied with satisfying results.
**Theorem 2.11.** Let $p$ be prime, and let $n, m$ be coprime integers such that every prime divisor of $mn$ is not congruent to 0 or 1 modulo $p$. Let

$$f(x) = (x^p - n) \prod_{k=0}^{p-1} (x^p - mn^k)$$

Then $\mathbb{P} \setminus \{p\} \subset p(f)$.

**Proof.** Let $a_1 = m$, and for $2 \leq i \leq p + 1$, let $a_i = n$. Let $T_{p+1} = \{p+1\}$, and for $1 \leq i \leq p$, define $T_i = \{j \in \mathbb{N} : 1 \leq j \leq i\}$. Let $\mathcal{F} = \{T_1, \ldots, T_{p+1}\}$, and for $1 \leq i \leq p + 1$, let $b_i = \prod_{j \in T_i} a_j$. Then

$$f(x) = \prod_{i=1}^{p+1} (x^p - b_i) = \prod_{T \in \mathcal{F}} \left( x^p - \prod_{i \in T} a_i \right)$$

Since $(b_1, b_{p+1}) = (m, n) = 1$, $\mathcal{F}$ satisfies hypothesis (1) of Lemma 2.10.

Now, let $q$ be a prime such that $q \equiv 1 \pmod{p}$. Let $\varphi = \varphi_q$. If $p \not| \varphi(n) = \sum_{i \in T_{p+1}} a_i$, then there exists $0 \leq t \leq p - 1$ such that

$$p \mid (\varphi(m) + t \varphi(n)) = \sum_{i \in T_{p+1}} \varphi(a_i)$$

Thus, $\mathcal{F}$ satisfies hypothesis (2) of Lemma 2.10. By Lemma 2.10, it follows that $\mathbb{P} \setminus \{p\} \subset p(f)$.

**Example 2.12.** Let $m, n$ be coprime integers such that every prime divisor of $mn$ is congruent to 2 modulo 3. Let

$$f(x) = (x^3 - n)(x^3 - m)(x^3 - mn)(x^3 - mn^2)$$

We claim that $f(x)$ is intersective. By Theorem 2.11, $\mathbb{P} \setminus \{3\} \in p(f)$, so it remains to prove $f \in \mathcal{I}_3$.

For $k \in \mathbb{Z}$, let $\overline{k}$ be the residue class of $k$ modulo 9. By hypothesis, $\overline{m}, \overline{m} \in \{2, 5, 8\}$. Let

$$A = \{\overline{m}, \overline{m}, \overline{mn}, \overline{mn^2}\}$$

We claim that $f(x)$ is intersective. By Theorem 2.11, $\mathbb{P} \setminus \{3\} \in p(f)$, so it remains to prove $f \in \mathcal{I}_3$.
We claim that $A \cap \{1, 8\} \neq \emptyset$. This is immediate if $\bar{n} = 8$ or $\bar{m} = 8$. If $\bar{n} = \bar{m} = 2$, then $\bar{mn}^2 = 8$. If $\bar{n} = \bar{m} = 5$, then $\bar{mn}^2 = 8$. Finally, if $\{\bar{n}, \bar{m}\} = \{2, 5\}$, then $\bar{mn} = 1$. This proves $A \cap \{1, 8\} \neq \emptyset$. One can check by simple calculation that the cubic residues mod 9 are 0, 1, 8. Thus, $x^3 - a$ has a root in $\mathbb{Z}_9$ for some $a \in A$. By Theorem 2.5, it follows that $f \in \mathcal{I}_3$.

**Corollary 2.13.** Let $p, m, n, f$ be as in Theorem 2.11. Let $r \in \mathbb{N}$ be coprime to $p$, let $a \in \{1, \ldots, p-1\}$, and let $h(x) = (x^r - a)f(x)$. If $a$ is an $r$th residue mod $p$, then $h \in \mathcal{I}$.

**Proof.** Assume $a$ is an $r$th residue mod $p$. Let $g(x) = x^r - a$. Then $g$ has a root $b$ in $\mathbb{Z}_p$, and $p \nmid r^{b-1} = g'(b)$. By Hensel’s Lemma, $p \in p(g)$, and hence $p \in p(h)$. By Theorem 2.11, $\mathbb{P} \setminus \{p\} \subset p(f) \subset p(h)$, so this proves that $h \in \mathcal{I}$. □

**Corollary 2.14.** Let $p, m, n, f$ be as in Theorem 2.11. If at least one of $n, m, mn, \ldots, mn^{p-1}$ is a $p$th residue modulo $p^2$, then $f$ is intersective.

**Proof.** By Theorem 2.11, $f \in \mathcal{I}_p$, so we have only to show that $p \in p(f)$. By hypothesis, there exists some factor $x^p - a$ of $f$ which has a root mod $p^2$. By Theorem 2.5, it follows that $p \in p(x^p - a)$, whence $p \in p(f)$. □

**Remark 2.15.** Let $p, m, n, f$ be as in Theorem 2.11. Let $H = \{a^2 : \mathbb{Z}_{p^2}^*\}$. It is known that $\mathbb{Z}_{p^2}^*$ is cyclic of order $p(p-1)$. Thus, $H$ is a subgroup of $\mathbb{Z}_{p^2}^*$ of index $p-1$. Now suppose that $n$ generates $\mathbb{Z}_{p^2}^*/H$. Then $mn^k \in H$ for some $0 \leq k \leq p-1$. In particular, the hypotheses of Corollary 2.14 are satisfied, so $f \in \mathcal{I}$.

**Example 2.16.** Let $p = 5, n = 2, m = 7$. Since $2^5 \equiv 7 \pmod{5^2}$, $m$ is a $p$th residue modulo $p^2$. By Theorem 2.11, it follows that

$$(x^5 - 2)(x^5 - 7)(x^5 - 14)(x^5 - 28)(x^5 - 56)$$

is intersective.
2.3 2-Intersecting Quadratics

We conclude this section with some brief remarks pertaining to quadratic polynomials. In particular, consider a general quadratic polynomial $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ which is irreducible over $\mathbb{Z}$. We wish to determine if $f \in \mathcal{I}_2$. Define the parity function

$$\text{par} : \mathbb{Z} \to \{0, 1\}$$

by

$$\text{par}(n) = \begin{cases} 0 & : 2 | n \\ 1 & : 2 \nmid n \end{cases}$$

For a three-tuple $(x, y, z) \in \mathbb{Z}^3$, define $\text{par}(x, y, z) = (\text{par}(x), \text{par}(y), \text{par}(z))$. Soule showed ([7]) the following: if $\text{par}(a, b, c) \in \begin{cases} (1, 1, 1), (0, 0, 1) \\ (1, 1, 0), (0, 1, 1), (0, 1, 0) \end{cases}$ then $f \notin \mathcal{I}_2$; if $\text{par}(a, b, c) \in \begin{cases} (1, 1, 0), (0, 1, 1), (0, 1, 0) \end{cases}$ then $f \in \mathcal{I}_2$.

Determining whether $f$ is 2-intersecting remains an open problem for $\text{par}(a, b, c) = (1, 0, 1)$ if $b$ is divisible by 4.

**Theorem 2.17.** Let $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$. Suppose $a, c$ are odd and $4 | b$. Then $f$ is 2-intersecting if and only if there exists $s \in \mathbb{Z}$ such that $f(s) \equiv 0 \pmod{8}$.

**Proof.** If no such $s$ exists, then $f$ is not 2-intersecting by definition.

Now suppose that $s \in \mathbb{Z}$ such that $f(s) \equiv 0 \pmod{8}$. Define $s_1 = s_2 = s_3 = s$. Write $b = 4k$. We will prove by induction that for every $n \in \mathbb{N}$, there exists an odd integer
such that

\[ f(s_n) \equiv 0 \pmod{2^n} \quad (2.1) \]

By hypothesis, equation (2.1) holds for \( n = 1, 2, 3 \). Moreover, \( s = s_1 = s_2 = s_3 \) is odd. Now, assume (2.1) holds for some \( n = m \geq 3 \), and that \( s_m \) is odd. If \( 2^{m+1} | f(s_m) \), then (2.1) holds with \( s_{m+1} = s_m, n = m + 1 \). So assume \( 2^{m+1} \nmid f(s_m) \). Then there exists an odd integer \( j \) such that \( f(s_m) = 2^m j \). Let \( t = 2^{m-1} \), \( s_{m+1} = s_m + t \). Then \( s_{m+1} \) is odd, and

\[
\begin{align*}
 f(s_{m+1}) &= f(s_m + t) \\
 &= f(s_m) + 2asnt + at^2 + bt \\
 &= 2^m j + (2as_m + at + 4k)t \\
 &= 2^m (j + as_m + 2^{m-2}a + 2k) \\
 &\equiv 0 \pmod{2^{m+1}} 
\end{align*}
\]

since \( j + as_m \) is even. By induction, it follows that there is an integer solution to (2.1) for all \( n \in \mathbb{N} \). \( \square \)
Chapter 3: Intersective polynomials and Galois Theory

In Chapter 2 we considered a number of results derived using elementary methods. At a more general level, there is an interesting relationship between intersective polynomials and Galois theory. It is to this relationship that we now turn.

3.1 A Theorem of Berend and Bilu

We shall begin by presenting the most significant theoretical result on intersective polynomials. This theorem was proved in [1] by D. Berend and Y. Bilu, and provides a method for determining whether any given integer polynomial is intersective.

Before stating the theorem, let us introduce some notation. Let $G$ be a group, and let $H \leq G$. For $g \in G$, we define $H^g = g^{-1}Hg$. We shall denote $\bigcup_{g \in G} H^g$ by $H^G$. Let $f \in \mathbb{Z}[x]$. Then there exists $k \in \mathbb{N}$ and $f_1, \ldots, f_k \in \mathbb{Z}[x]$ such that each $f_i$ is irreducible over $\mathbb{Q}$, and

$$f(x) = f_1(x) \cdots f_k(x)$$

Let $K$ be the splitting field of $f(x)$ over $\mathbb{Q}$. Since $K$ is the splitting field of $f$, $K/\mathbb{Q}$ is normal, and hence Galois. We define $G(f) = \text{Gal}(K/\mathbb{Q})$. For $1 \leq i \leq k$, let $\alpha_i$ be a root of $f_i$, and let

$$H_i = \text{Gal}(K/\mathbb{Q}(\alpha_i))$$

(3.1)
By the Fundamental Theorem of Galois Theory, it follows that

\[ |G: H_i| = [\mathbb{Q}(\alpha_i) : \mathbb{Q}] = \deg f_i \quad (3.2) \]

We define \( U(f) = \bigcup_{i=1}^{k} H_i \).

For each \( 1 \leq i \leq k \), let \( \Delta_i \) be the discriminant of \( h_i \), and let \( a_i \) be the leading coefficient of \( h_i \). Let \( D = \prod_{i=1}^{k} a_i \Delta_i \). There exist \( e_1, \ldots, e_r \in \mathbb{N} \) and distinct primes \( p_1, \ldots, p_r \) such that \( D = p_1^{e_1} \cdots p_r^{e_r} \). Finally, define \( \Delta = p_1^{2e_1+1} \cdots p_r^{2e_r+1} \).

**Theorem 3.1.** Let \( f \in \mathbb{Z}[x] \). Then \( f \) is intersective if and only if the following hold:

1. \( \Delta \) divides \( f(a) \) for some \( a \in \mathbb{Z} \)

2. \( \bigcup_{g \in G} g^{-1}U(f)g = G(f) \)

As a corollary to Theorem 3.1, we obtain the fact that every nontrivial intersective polynomial is reducible over \( \mathbb{Q} \).

**Corollary 3.2.** Let \( f \in \mathbb{Z}[x] \). If \( f \) is irreducible over \( \mathbb{Q} \) and \( \deg f > 1 \), then \( f \notin \mathcal{I} \).

**Proof.** Let \( G = G(f) \), and let \( H = H_1 \), where \( H_1 \) is defined as in equation (3.1). Since \( f \) is irreducible, \( U(f) = H \), and since \( \deg f > 1 \), \( H \neq G(f) \). Let \( g_1, \ldots, g_k \) be a complete set of coset representatives for \( H \) is \( G \), where \( k = |G|/|H| \). Since \( 1 \in g_i^{-1}Hg_i \) for all \( 1 \leq i \leq k \), it follows that

\[ \left| \bigcup_{g \in G} g^{-1}U(f)g \right| = \left| \bigcup_{i=1}^{k} g_i^{-1}Hg_i \right| \leq k|H| - k < |G| \]

In particular, \( \bigcup_{g \in G} g^{-1}U(f)g \neq G \). By Theorem 3.1, \( f \notin \mathcal{I} \). \( \square \)

**Example 3.3.** Since every cyclotomic polynomial is irreducible over \( \mathbb{Q} \), Corollary 3.2 shows that every cyclotomic polynomial

\[ \Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\text{gcd}(k,n)=1}} \left(x - e^{2\pi ik/n}\right) \]

shows that every cyclotomic polynomial

\[ \Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\text{gcd}(k,n)=1}} \left(x - e^{2\pi ik/n}\right) \]

16
with $n \geq 3$ is not intersective. In particular, the polynomials

$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$

are not intersective.

From Theorem 3.1 we may also observe that every intersective polynomial without rational roots has degree at least 5. Indeed, suppose that $f \in \mathcal{I}$ has degree less than 5 and no rational roots. By Corollary 3.2, $f$ is reducible over $\mathbb{Q}$, and since $f$ has no rational roots, $f$ must be the product of two irreducible quadratics, say $f = h_1 h_2$. Let $H_1, H_2$ be defined as in (3.1). Then $H_1 \cong H_2 \cong \mathbb{Z}_2$. Thus, either $G(f) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ or $G(f) \cong \mathbb{Z}_2$. But neither $\mathbb{Z}_2 \times \mathbb{Z}_2$ nor $\mathbb{Z}_2$ is the union of the conjugates of any two of its proper subgroups, contradicting Theorem 3.1.

Conversely, intersective polynomials of degree 5 exist; for example, Berend and Bilu show that $(x^3 - 19)(x^2 + x + 1)$ is intersective in [1].

### 3.2 Normal Covers

**Definition 3.4.** For $k \in \mathbb{N}$, we define

$$R_k = \{f_1 \cdots f_k : f_1, \ldots, f_k \in \mathbb{Z}[x] \text{ such that } f_i \text{ is irreducible over } \mathbb{Q} \text{ for } i = 1, \ldots, k\}$$

Let $G$ be a noncyclic finite group. Then for all $g \in G$, $(g)$ is a proper subgroup of $G$, and $\bigcup_{g \in G} (g) = G$. Thus, we may introduce the following definitions.

**Definition 3.5.** Let $G$ be a finite group. If $G$ is cyclic, we define $\sigma(G) = \infty$. If $G$ is not cyclic, then we define $\sigma(G)$ to be the smallest integer $k$ such that there exist proper subgroups $H_1, \ldots, H_k$ of $G$ such that $G = \bigcup_{i=1}^{k} H_i$; the number $\sigma(G)$ is called the *covering number* of $G$. 

17
If \( G \) is cyclic, we define \( \gamma(G) = \infty \). If \( G \) is not cyclic, then we define \( \gamma(G) \) to be the smallest integer \( k \) such that there exist proper subgroups \( H_1, \ldots, H_k \) of \( G \) such that \( G = \bigcup_{g \in G} \bigcup_{i=1}^{k} H_i^g \); the number \( \gamma(G) \) is called the normal covering number of \( G \).

Remark 3.6. For every group \( G \), \( \sigma(G) \geq \gamma(G) \geq 2 \). If \( G_1, G_2 \) are groups, then \( \gamma(G_1 \times G_2) = \min \{ \gamma(G_1), \gamma(G_2) \} \). If \( G \) is abelian, then \( \gamma(G) = \sigma(G) \).

Lemma 3.7. Let \( G \) be abelian and noncyclic, and let \( p \) be the smallest prime dividing \( |G| \). Then \( \gamma(G) = p + 1 \).

Proof. By the Fundamental Theorem of Finite Abelian Groups, there exist primes \( p_1, \ldots, p_n \) (not necessarily distinct) and positive integers \( e_1, \ldots, e_n \) such that \( G \cong \prod_{i=1}^{n} \mathbb{Z}_{p_i^{e_i}} \). Thus,
\[
\gamma(G) = \min_{1 \leq i \leq n} \left( \gamma\left( \mathbb{Z}_{p_i^{e_i}} \right) \right) = \min_{1 \leq i \leq n} (p_i) + 1 \tag*{\square}
\]

Corollary 3.8. Let \( f \in R_2 \). If \( G(f) \) is abelian, then \( f \not\in \mathcal{I} \).

Proof. Let \( H_1, H_2 \) be defined as in equation (3.1). Then \( U(f) = H_1 \cup H_2 \). Let \( G = G(f) \). Then by Theorem 3.1,
\[
G = \bigcup_{g \in G} g^{-1}U(f)g = \bigcup_{g \in G} U(f) = \bigcup_{i=1}^{k} H_i
\]
which is clearly impossible if \( k = 1 \), since \( H_1 \neq G \). If \( k = 2 \), then \( 1 \in H_1 \cap H_2 \) and \( |G : H_i| \geq 2 \) for \( i = 1, 2 \), whence \( |G| = |H_1 \cup H_2| \leq 2(|G|/2) - 1 = |G| - 1 \), contradiction. \( \square \)

The following theorem is proved in [4].

Theorem 3.9. Let \( G \) be a finite group such that \( \gamma(G) = 2 \). If \( \gamma(G/N) > 2 \) for every nontrivial normal subgroup \( N \) of \( G \), then \( G \) has a unique minimal normal subgroup.
Corollary 3.10. Let \( f \in R_2 \), and let \( G = G(f) \). If \( \gamma(G/N) > 2 \) for every nontrivial \( N \triangleleft G \), and \( G \) contains two distinct minimal normal subgroups, then \( f \notin \mathcal{I} \).

Proof. By Theorem 3.9, \( \gamma(G) \geq 3 \), so that \( G \neq \bigcup_{g \in G} g^{-1}U(f)g \). Thus, \( f \notin \mathcal{I} \) by Theorem 3.1. \( \Box \)

From Theorem 3.1 we see that if \( f \) is intersective, then \( G(f) \) is covered by the union of all the conjugates of the proper subgroups of \( G \). The following theorem (proved in [5]) is a partial converse to this implication.

Theorem 3.11. Let \( G \) be a finite solvable group, and suppose \( H_1, \ldots, H_m \) are subgroups of \( G \) such that

\[
\bigcup_{i=1}^{m} \bigcap_{g \in G} g^{-1}H_ig = G \quad (3.3)
\]

\[
\bigcap_{i=1}^{m} \bigcup_{g \in G} g^{-1}H_ig = \{1\} \quad (3.4)
\]

Then there exist nonlinear polynomials \( f_1, \ldots, f_m \in \mathbb{Z}[x] \) which are irreducible over \( \mathbb{Q} \), and \( \alpha_1, \ldots, \alpha_m \in \mathbb{C} \) such that \( f_1 \cdots f_m \in \mathcal{I} \), \( G(f_1 \cdots f_m) = G \), and for \( 1 \leq i \leq m \), \( f_i(\alpha_i) = 0 \) and \( H_i = \text{Gal}(K/\mathbb{Q}(\alpha_i)) \), where \( K \) is the splitting field of \( f_1 \cdots f_m \) over \( \mathbb{Q} \).

Let \( p \) be prime, and suppose that \( q \) is prime such that \( q \equiv 1 \) (mod \( p \)). Let \( G = \mathbb{Z}_p \times \mathbb{Z}_q \). Let \( H_1 = \mathbb{Z}_p \times \{0\} \leq G \), \( H_2 = \{0\} \times \mathbb{Z}_q \leq G \). Then \( H_1 \triangleleft G \), and \( H_2 \) is not normal in \( G \). The subgroup \( H_1 \) acts on \( H_2 \) by conjugation; the stabilizer of this action is a subgroup of \( H_1 \), and since the action is nontrivial, the stabilizer must be \( \{1\} \). Thus, for all \( a, b \in H_1 \), we have \( a^{-1}H_2a \neq b^{-1}H_2b \), and since \( q \) is prime, it follows that \( a^{-1}H_2a \cap b^{-1}H_2b = \{1\} \). Moreover, since \( H_1 \cap a^{-1}H_2a = \{1\} \) for all \( a \in G \), we have

\[
|\mathbb{Z}_p^G \cup \mathbb{Z}_q^G| = p + p(q - 1) = pq = |G|
\]

19
This shows that $G, H_1, H_2$ satisfy the hypotheses of Theorem 3.11. Thus, there exist nonlinear irreducible polynomials $f_1, f_2 \in \mathbb{Z}[x]$ with roots $\alpha_1, \alpha_2$, respectively, such that $G(f_1f_2) = G$, $f_1f_2 \in \mathcal{I}$, and $H_i = \text{Gal}(K/\mathbb{Q}(\alpha_i))$ for $i = 1, 2$, where $K$ is the splitting field of $f_1f_2$ over $\mathbb{Q}$. By equation 3.2, we have

$$\deg(f_1f_2) = \deg(f_1) + \deg(f_2) = |G : H_1| + |G : H_2| = p + q$$

Moreover, since $f_1, f_2$ are irreducible and nonlinear, $f_1, f_2 \notin \mathcal{I}$ by Corollary 3.2, so $f_1f_2$ is minimally intersective.

With some additional conditions on the subgroups $H_i$ in Theorem 3.11, we can ensure that the resulting polynomial $f_1 \cdots f_m$ is minimally intersective, as we now show.

**Corollary 3.12.** Let $G, H_1, \ldots, H_m$ be as in Theorem 3.11. Suppose in addition that

$$\bigcap_{1 \leq i \leq m} H_i = \{1\} \quad (3.5)$$

$$\bigcup_{1 \leq i \leq m} H_i^G \neq G \quad (3.6)$$

for all $1 \leq j \leq m$. Then there exist nonlinear polynomials $f_1, \ldots, f_m \in \mathbb{Z}[x]$ which are irreducible over $\mathbb{Q}$, and $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ such that $f_1 \cdots f_m$ is minimally intersective, $G(f_1 \cdots f_m) = G$, and for $1 \leq i \leq m$, $f_i(\alpha_i) = 0$ and $H_i = \text{Gal}(K/\mathbb{Q}(\alpha_i))$, where $K$ is the splitting field of $f_1 \cdots f_m$ over $\mathbb{Q}$.

**Proof.** Let $f_1, \ldots, f_m$, $\alpha_1, \ldots, \alpha_m$, and $K$ be as in the statement of Theorem 3.11. We claim that $f_1 \cdots f_m$ is minimally intersective. Suppose otherwise. Since each $f_i$ is irreducible over $\mathbb{Q}$, there exists some $1 \leq j \leq m$ such that $g = \prod_{i \neq j} f_i$ is intersective. Let $K'$ be the splitting field of $g$ over $\mathbb{Q}$. By the Fundamental Theorem of Galois Theory,

$$[K : K'] = \left| \bigcap_{1 \leq i \leq m} H_i : \{1\} \right| = 1$$

20
Thus, $K' = K$, whence $G(g) = G(f_1 \cdots f_m) = G$. By Theorem 3.1, it follows that

$$\bigcup_{1 \leq i \leq m \atop i \neq j} H_i^G = G$$

contradicting (3.6). \qed

**Example 3.13.** Consider the group

$$G = D_n = \langle r, s : r^n = s^2 = rsrs = 1 \rangle$$

the dihedral group of order $2n$. The group $D_n$ is solvable for all $n \in \mathbb{N}$.

Suppose $n$ is even. Let $H_1 = \langle r \rangle$, $H_2 = \langle s \rangle$, $H_3 = \langle sr \rangle$. One can check that

$$H_1^G = H_1$$

$$H_2^G = \{1\} \cup \{sr^{2k} : 0 \leq k \leq n/2 - 1\}$$

$$H_3^G = \{1\} \cup \{sr^{2k+1} : 0 \leq k \leq n/2 - 1\}$$

Thus,

$$H_1^G \cup H_2^G \cup H_3^G = G$$

$$(\bigcap_{g \in G} H_1^g) \cap (\bigcap_{g \in G} H_2^g) \cap (\bigcap_{g \in G} H_3^g) = \{1\}$$

and for $j = 1, 2, 3$,

$$\bigcap_{1 \leq i \leq 3 \atop i \neq j} H_i = \{1\}$$

$$\bigcup_{1 \leq i \leq 3 \atop i \neq j} H_i^G = G$$

By Corollary 3.12, there exist nonlinear irreducible polynomials $f_1, f_2, f_3 \in \mathbb{Z}[x]$ such that $f_1 f_2 f_3$ is minimally intersective and $\text{Gal}(f_1 f_2 f_3) = G$. Moreover, by equation 3.2,

$$\deg(f_1 f_2 f_3) = |G : H_1| + |G : H_2| + |G : H_3| = 2 + n + n = 2(n + 1)$$

21
Example 3.14. As in the previous example, let

\[ G = D_n = \langle r, s : r^n = s^2 = rsr = 1 \rangle \]

Now, however, assume \( n \) is odd. Then

\[ \langle r \rangle^G = \langle r \rangle \]
\[ \langle s \rangle^G = \{1\} \cup \{sr^k : 0 \leq k \leq n - 1\} \]

Thus,

\[ \langle r \rangle^G \cup \langle s \rangle^G = G \]
\[ \left( \bigcap_{g \in G} \langle r \rangle^g \right) \cap \left( \bigcap_{g \in G} \langle s \rangle^g \right) = \{1\} \]

By Theorem 3.11, it follows that there exist nonlinear irreducible polynomials \( f_1, f_2 \in \mathbb{Z}[x] \) such that \( \text{Gal}(f_1f_2) = G \), and

\[ \deg(f_1f_2) = |G : \langle r \rangle| + |G : \langle s \rangle| = n + 2 \]

By Corollary 3.2, \( f_1, f_2 \notin \mathcal{I} \), so \( f_1f_2 \) is minimally intersective.

As an immediate consequence of Examples 3.13 and 3.14, we obtain the following theorem.

**Theorem 3.15.** Let \( n \) be an integer greater than 4. If \( 4 \nmid n \), then there exists a minimally intersective polynomial \( f \) with \( \deg(f) = n \).

### 3.3 Density

For \( n \in \mathbb{N} \), we shall use \( \pi(n) \) to denote the number of primes less than or equal to \( n \).
Definition 3.16. Let $S \subset \mathbb{P}$. For $n \in \mathbb{N}$, we define $\rho(S,n) = |S \cap \{1,\ldots,n\}|$. The density $d(S)$ of the set $S$ is given by

$$d(S) = \lim_{n \to \infty} \frac{\rho(S,n)}{\pi(n)}$$

Definition 3.17. Let $f \in \mathbb{Z}[x]$. Then we shall denote the set of all primes $p$ such that $f(x) \equiv 0 \pmod{p}$ has a solution by $s(f)$.

Note that $p(f) \subset s(f)$ for all $f \in \mathbb{Z}[x]$, and $f \in \mathcal{I}$ implies that $1 = d(p(f)) = d(s(f))$.

The following theorem is proved in [1].

Theorem 3.18. Let $f \in \mathbb{Z}[x]$. Let $G = G(f), U = U(f)$. Then

$$d(s(f)) = \frac{1}{|G|} \left| \bigcup_{g \in G} g^{-1}Ug \right|$$

Example 3.19. Let $f \in \mathbb{Z}[x]$. Suppose that $f$ is irreducible over $\mathbb{Q}$, and $G(f) = D_n$, where $n$ is even. Let $\alpha$ be a root of $f$. Let $K$ be the splitting field of $f$ over $\mathbb{Q}$, let $G = G(f)$, and let $H = \text{Gal}(K/\mathbb{Q}(\alpha))$. Then $|G : H| = \deg f = n$, so $|H| = 2n/n = 2$.

Thus, there is some $0 \leq k \leq n - 1$ such that $H = \{1, sr^k\}$. Since

$$s^{-1}(sr^m)s = r^m s = sr^{-m} = sr^{n-m}$$

$$r^{-1}(sr^m)r = sr^{m+2}$$

for any $m \in \{0,\ldots,n-1\}$, it follows that

$$\{1, sr^k\}^G = \{1\} \cup \left\{sr^{k+2j} : 0 \leq j \leq \frac{n}{2} - 1 \right\}$$

Since $U(f) = H$, by Theorem 3.18 we have

$$d(p(f)) \leq d(s(f)) = \frac{|\{1, sr^k\}^G|}{|D_n|} = \frac{n/2 + 1}{2n} = \frac{1}{4} + \frac{1}{2n} \quad (3.7)$$

23
Now, suppose that \( f_1, f_2, f_3 \in \mathbb{Z}[x] \) are irreducible over \( \mathbb{Q} \) and there exist even integers \( n_1, n_2, n_3 \) such that \( G(f_i) = D_{n_i} \) for \( i = 1, 2, 3 \). Then by equation (3.7),

\[
d(p(f_1f_2)) \leq \sum_{i=1}^{2} d(p(f_i)) \leq \frac{1}{2} + \frac{1}{2n_1} + \frac{1}{2n_2}
\]
\[
d(p(f_1f_2f_3)) \leq \sum_{i=1}^{3} d(p(f_i)) \leq \frac{3}{4} + \frac{1}{2n_1} + \frac{1}{2n_2} + \frac{1}{2n_3}
\]

Thus, if \( n_1 \) and \( n_2 \) are both larger than 2, then

\[
d(p(f_1f_2)) \leq \frac{1}{2} + \frac{1}{6} + \frac{1}{6} < 1
\]

so that \( f_1f_2 \notin \mathcal{I} \). Similarly, if \( n_1, n_2, n_3 \) are all greater than 6, then

\[
d(p(f_1f_2f_3)) \leq \frac{3}{4} + \frac{1}{14} + \frac{1}{14} + \frac{1}{14} < 1
\]

so that \( f_1f_2f_3 \notin \mathcal{I} \).
Bibliography


