On the Finiteness of a Special Family of Polynomials

Xiaohan Ye

Abstract. In this paper, we study a family of polynomials with the property that $f(x)$ is a factor of $f(x^m)$ for some integer $m > 1$. We prove that there is a finite number of such polynomials over $\mathbb{Q}$ with fixed degree and find a connection between these polynomials and cyclotomic polynomials.

1. Introduction

In this paper, we explore a family of polynomials with the property that $f(x)$ is a factor of $f(x^m)$ for a some positive integer $m > 1$ (we call such polynomials FPP polynomials, see §2.1 below). The initial spark of this project comes from a problem in the admission test of the Ross Program in 2019. The problem asks for a list of all monic polynomials with degree less than or equal to 4 that satisfy $f(x) \mid f(x^2)$.

However, our general situation is more profound, interesting and, of course, more difficult. For a given m, we discover that the number of such polynomials over $\mathbb{C}$ with degree less than or equal to a given n is finite. But surprisingly, if we only consider polynomials with rational coefficients, we can prove a stronger finiteness theorem without fixing the power m.

Theorem 1.1. *There is a finite number of FPP polynomials over $\mathbb{Q}$ with degrees less than a certain value.*

To prove those results, we make a connection to graph theory. For any FPP polynomial with complex coefficients, we can associate it with a graph. Using this graph representation, we reach the conclusion that the roots of such polynomials are all roots of unity. This result helps us prove the finiteness of F_mPP polynomials over $\mathbb{C}$ with any given m and degree n.

To prove Theorem 1.1, we use the facts that the degree of the minimal polynomial of any root of f must be bounded by the degree of f and that the minimal polynomial of a root of unity has a known degree. Then, we find a connection between such polynomials and cyclotomic polynomials. We also find some interesting results in number theory that comes along as by-products of our exploration of this family of polynomials (see Corollary 4.1.3 and Corollary 4.4.2 in Section 4).

2. Preliminary

2.1. Basic Definitions.

We start by giving several basic definitions.

Definition 1. Let K be any field, and $K[x]$ the ring of polynomials over K. For any polynomial $f(x) \in K[x]$, we say $f(x)$ is of factor-power property, or FPP (we can also call $f(x)$ a FPP polynomial), if $f(x)$ is monic and there exists some positive integer $m > 1$ such that

$$f(x) \mid f(x^m).$$

If we want to specify the power m, we say $f(x)$ is of factor-m-power property, or F_mPP.

Definition 2. A F_mPP/FPP polynomial $f(x)$ is defined to be F-reducible if it can be expressed as the product of some lower-degree F_mPP/FPP polynomials. Otherwise, it is defined to be F-irreducible.

Definition 3. Given a positive integer n, we define the collection of FPP polynomials, $F_m(K)_n$, $F_m(n,K)$, $F(K)_n$ and $F(n,K)$ as follows:

$$F_m(K)_n = \{f \in F_mPP(K) \mid deg(f) = n\}$$
$$F_m(n,K) = \{f \in F_mPP(K) \mid deg(f) \leq n\}$$
$$F(K)_n = \{f \in FPP(K) \mid deg(f) = n\}.$$
$$F(n,K) = \{f \in FPP(K) \mid deg(f) \leq n\}.$$

With those definitions, we can prove some direct consequences:

Proposition 2.2. *$f(x) = x$ and $f(x) = x - 1$ are F_mPP polynomials for any positive integer m.*

This is obviously true since $x \mid x^m$ and $x - 1 \mid (x-1)^m$ for any positive integer m.

Proposition 2.3. *If a FPP/F_mPP polynomial $f(x)$ is F-irreducible then $f(x) = x$ or $x \nmid f(x)$.*

Proof: If $f(x) \neq x$ and $x \mid f(x)$, suppose $f(x) = g(x) \cdot x^k$, where k is a positive integer and $x \nmid g(x)$. Because $f(x)$ is FPP/F_mPP, we know that $f(x) \mid f(x^m)$. It follows that $g(x) \cdot x^k \mid g(x^m) \cdot x^{km}$. Since $g(x) \nmid x^{km}$, we know that $g(x) \mid g(x^m)$. Therefore, $g(x)$ is also a FPP/F_mPP polynomial. Hence, for $f(x)$ to be F-irreducible, $f(x) = x$ or $x \nmid f(x)$, which proves the proposition. □

Proposition 2.4. *$|F(n, \mathbb{C})|$ is infinite.*

Proof: Consider the polynomial $f(x) = x - \zeta_m$, where ζ_m is a m^{th} root of unity. We know that $\zeta_m^m = 1$, and it follows that $\zeta_m^{m+1} = \zeta_m$. Then we can infer that $f(x)$ is a $F_{m+1}PP$ polynomial, that is, $x - \zeta_m \mid x^{m+1} - \zeta_m$. This is because if $x - \zeta_m = 0$, then $x^{m+1} - \zeta_m$ is also 0. Therefore, however big m is, the polynomial $x - \zeta_m$ is always a FPP polynomial with complex coefficients. Hence, there is an infinite number of FPP polynomials over $\mathbb{C}$ with degrees less than or equal to n. □

2.5. Algebraic Number Theory.

Now we go through some algebraic number theory that will be used later in our paper.

Algebraic fields are fields whose elements are all algebraic numbers, where an algebraic number is a root of a non-zero polynomial with rational coefficients. A field extension K/F is algebraic if every element in K is algebraic over F, that is, if every element in K is a root of a non-zero polynomial with coefficients in F. All finite field extensions are algebraic.

These concepts then lead to the definition of number fields, which are finite field extensions of $\mathbb{Q}$, the field of rational numbers. In this paper, we will mainly use one specific type of number field—the cyclotomic field, which is a number field obtained by adjoining a complex primitive root of unity to $\mathbb{Q}$. A primitive n^{th} root of unity ζ_n is a root of unity for n that is not a root of unity for some k smaller than n. That is, if $z = \zeta_n$, then $z^n = 1$ and $z^k \neq 1$ for $k = 1, 2, 3, \cdots, n-1$.

The degree of the cyclotomic field extension $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where $\varphi(n)$ is Euler's totient function. Also, a cyclotomic field is the splitting field of the cyclotomic polynomial whose zeros are precisely the primitive n^{th} roots of unity. A cyclotomic polynomial has integer coefficients and is irreducible over $\mathbb{Q}$ (i.e. cannot be written as the product of two positive-degree polynomials with rational coefficients).

There is a well-known connection between number field extensions and irreducible polynomials over $\mathbb{Q}$, which is established by the notion of minimal polynomial. Let α be any algebraic number over F. The minimal polynomial of α over F is the monic polynomial of least degree among all polynomials in $F[x]$ having α as a root.

Recall that if $f(x) \in F[x]$ is irreducible, then $F[x]/(f(x))$ is a field. More specifically, if $f(x)$ is the minimal polynomial of α over F, we have: $F(\alpha) = F[X]/(f(x))$. Using this property, we can determine a field by the minimal polynomial of its generator. Let K/F be a finite algebraic field extension, $f(x)$ the minimal polynomial of α, an element of K. If α is a generator of K over F, then $K = F(\alpha) = F[X]/(f(x))$.

3. Connection to Graph Theory

Now we set up a correspondence between the set of all F-irreducible F_mPP polynomials with complex coefficients and a set of directed graphs with certain properties. We exclude the case $f(x) = x$ here. Notice that if $f(x) \neq x$ then $x \nmid f(x)$, otherwise $f(x)$ will be F-reducible.

Case 1: $f(x)$ is an F-irreducible F_mPP polynomial without multiple roots.

Suppose $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are distinct non-zero complex numbers. We construct a directed graph $G_f := (V_f, E_f)$ according to $f(x)$ in the following way. First we let the vertices of G_f be $\alpha_1, \alpha_2, \cdots, \alpha_n$. Apparently, $|V_f| = n$. Then, we draw a directed edge from α_i to α_j if and only if $(x-\alpha_i) \mid (x^m - \alpha_j)$ $(1 \leq i, j \leq n)$, i.e. ${\alpha_i}^m = \alpha_j$.

Proposition 3.1. *G_f has the properties:*

1. *For all i, there is one and only one arrow that starts from α_i.*
2. *There is one and only one directed cycle in every component of G_f.*
3. *G_f is weakly connected (i.e. G_f only has one component).*

Proof of property 1:

We first prove that every vertex must be the source of some arrow. Because $f(x) \mid f(x^m)$, we know that $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \mid (x^m-\alpha_1)(x^m-\alpha_2)\cdots(x^m-\alpha_n)$, and $(x-\alpha_i) \mid (x^m-\alpha_1)(x^m-\alpha_2)\cdots(x^m-\alpha_n)$, where $i \in \{1, 2, \cdots, n\}$. Because $(x-\alpha_i)$ is irreducible, it follows that there exists $j \in \{1, 2, \cdots, n\}$ such that $(x-\alpha_i) \mid (x^m-\alpha_j)$. Therefore, every vertex is the source of some arrow.

Then, we prove that there could only be one arrow that starts from a vertex. Suppose there are two or more arrows that start from α_i, and two of the targets of these arrows are α_j and α_k. From our construction of G_f, we have $\alpha_j = \alpha_i^m$ and $\alpha_k = \alpha_i^m$, so $\alpha_j = \alpha_k$. Since the vertices in G_f all represent distinct numbers, we know that α_j and α_k are the same vertex. Therefore, the arrows that start from α_i are the same arrow. Hence, there is one and only one arrow that starts from any vertex in G_f. □

Proof of property 2:

Let C be a component of G_f. If C is an isolated vertex, we know that there is only one arrow in C and that arrow forms a loop, so property 2 is true in this case.

If C contains two or more vertices, we first prove that there is at least one directed cycle in C.

Pick an arbitrary directed path p in C. Suppose the last vertex of the path is α_l. Consider all the vertices along the path except α_l. Given property 1, which is obviously true by our definition of G_f, we know that every vertex along the path except α_l is already the starting point of an arrow. Therefore, these vertices could only be the targets of some other arrows in C. In other words, there could only be incoming arrows pointing to the path other than the path that leads to α_l. Consider the incoming arrows (if there is any) and the paths they form. By the same logic, the starting points of those incoming arrows can only be the targets of other arrows. It follows that every incoming path is a directed path and has the same direction as p, which means that there is a directed path from every vertex in C to α_l. On the other hand, α_l itself is the source of one and only one arrow. The arrow (α_l, α_k) will always form a directed cycle with the directed path from α_k to α_l. Therefore, there is at least one directed cycle in every component.

Then, we prove that there is at most one directed cycle in C.

Suppose there are two or more directed cycles in the component C. Consider directed cycles c_1 and c_2. Notice that every vertex in c_1 and c_2 is already the source of one arrow. If c_1 and c_2 are in the same component, there must be a directed path from some vertex α_1 in c_1 to some vertex α_2 in c_2. Consider the first and the last arrow of this path. We know that one of them is the source of two or more arrows, which contradicts property 1.

Therefore, there is one and only one directed cycle in every component of G_f. □

Proof of property 3:

We prove that if G_f is composed of multiple components, then $f(x)$ is F-reducible.

Let C be a connected component of G_f that consists of the set of vertices $\{\alpha_l, \alpha_{l+1}, \cdots, \alpha_{l+k}\}$, where $\{l, l+1, \cdots, l+k\} \subset \{1, 2, \cdots, n\}$. By the construction of G_f, we know that for all i, there exists a j such that $(x-\alpha_i) \mid (x^m - \alpha_j)$, where $i, j \in \{l, l+1, \cdots, l+k\}$. This means $g(x) = (x-\alpha_l)(x-\alpha_{l+1})\cdots(x-\alpha_{l+k})$ is also a F_mPP polynomial. Similarly, every component of G_f represents a F_mPP polynomial. Because $f(x)$ is the product of all the polynomials corresponding to the components of G_f, we know that $f(x)$ is F-reducible. Therefore, if $f(x)$ is F-irreducible, G_f only has one component, i.e. it is weakly connected. □

Case 2: $f(x)$ is a F_mPP polynomial that has multiple roots. We claim that such polynomials must be F-reducible.

Suppose $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are complex numbers that are not necessarily distinct. Assume $f(x)$ is F-irreducible, and we know that $\alpha_1, \alpha_2, \cdots, \alpha_n$ are all non-zero roots. We can still construct a slightly modified version of the graph (V_f, E_f).

We let the vertices of G_f be $\alpha_1, \alpha_2, \cdots, \alpha_n$. Apparently, $|V_f| = n$. We draw a directed edge from α_i to α_j if and only if $(x-\alpha_i) \mid (x^m - \alpha_j)$ $(1 \le i, j \le n)$, i.e. ${\alpha_i}^m = \alpha_j$. We stipulate that every vertex can only be the source of one arrow.

To avoid the complexity that comes with multiple roots, we add the following three rules.

1) If α_l is a multiple root and $\alpha_l^m = \alpha_l$, we draw an arrow from α_l to itself to form a loop.

2) Suppose α_l is a multiple root with the multiplicity of k. $\alpha_l = \alpha_{l+1} = \cdots = \alpha_{l+k-1}$. Let $\alpha_l^m = \alpha_r$. Without loss of generality, we first draw an arrow from α_l to α_r. Let a_0 be the arrow that starts from α_{l+1}. If α_r is not a multiple root, then the target of a_0 is also α_r. This means $(x-\alpha_l)^2 \mid (x^m - \alpha_r)$. However, the polynomial $x^m - \alpha_r$ has no multiple root since $\alpha_r \neq 0$. Hence, α_r is also a multiple root of $f(x)$. We stipulate that the target of a_0 is not α_r, but α_{r+1}, which is a vertex that equals α_r numerically. Using the same method, we know that the multiplicity of α_r is greater than or equal to k. We can guarantee that all the arrows starting from multiple roots end at different vertices.

3) Suppose both $\alpha_{s_1} = \alpha_{s_2} = \cdots = \alpha_{s_p}$ and $\alpha_{r_1} = \alpha_{r_2} = \cdots = \alpha_{r_q}$ are multiple roots of $f(x)$ and $\alpha_{r_i}^m = \alpha_{s_i}$, where $i \in \{1, 2, \cdots, q\}$. Since there are multiple options for drawing arrows from α_{r_i} to α_{s_i}, we stipulate that if there is a directed path from α_{s_j} to α_{r_j} for some $j \in \{1, 2, \cdots, q\}$, we draw an arrow from α_{r_j} to α_{s_j}. In other words, we want to form a cycle as soon as possible.

PROPOSITION 3.2. *G_f has the properties:*

(1) *For all i, there is one and only one arrow that starts from α_i.*
(2) *There is one and only one directed cycle in every component of G_f.*
(3) *G_f has multiple components.*

Proof of property 2:

We have proved that if α_l has the multiplicity of k and there is an arrow from α_l to α_r, then the multiplicity of α_r is greater than or equal to k. Without loss of generality, assume there is a directed path from α_1 to α_r with vertex sequence $(\alpha_1, \alpha_2, \alpha_3 \cdots, \alpha_r)$. If the multiplicity of α_2 is greater than that of α_1, there must be another path with vertex sequence $(\alpha_2, \alpha_3, \cdots, \alpha_r)$. If we go on with this process, we get multiple paths that end at distinct vertices that all represent α_r.

Consider the arrows that start from α_r. If those arrows end at α_i where $1 \leq i \leq r$, they form cycles with the paths from α_i to α_r, and we know that $\alpha_i, \alpha_{i+1}, \cdots, \alpha_r$ (all the vertices in the cycle) have the same multiplicity. Since the paths from α_j to α_r $(1 \leq j \leq r)$ are all disconnected with each other, it follows that there is one and only one cycle in every component. In other words, property 2 still holds true here. □

Proof of property 3:

We know from the proof of property 2 that the paths from α_j to α_r $(1 \leq j \leq r)$ are all disconnected with each other, which means there are multiple components in G_f. □

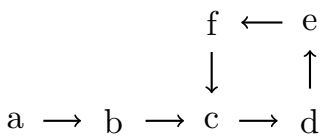
Since every component in G_f represents a F_mPP polynomial and the product of those polynomials is exactly $f(x)$, it follows that $f(x)$ is F-reducible. Hence, this case should not be taken into consideration.

Here are two examples of G_f:

EXAMPLE 3.2.1. *The graph on the left corresponds to the F_2PP polynomial $f(x) = (x^2 - 1)^2$.*

Since $f(x) = (x^2 - 1)^2$ has multiple roots, the construction of G_f involves the use of all three rules mentioned above. According to Rule 1, we draw a self-loop from 1 to itself instead of an arrow from 1 to the other 1. The second rule ensures that the graph on the right is not a possible alternative. Rule 3 has the same effect as Rule 1 in this case because making a self-loop is the fastest way to form a cycle.

EXAMPLE 3.2.2. *The graph below corresponds to the F_3PP polynomial $f(x) = (x-a)(x-b)(x-c)(x-d)(x-e)(x-f)$, where $a = e^{i\frac{1}{360}\pi}$, $b = e^{i\frac{1}{120}\pi}$, $c = e^{i\frac{1}{40}\pi}$, $d = e^{i\frac{3}{40}\pi}$, $e = e^{i\frac{9}{40}\pi}$, $f = e^{i\frac{27}{40}\pi}$.*



4. The Finiteness of FPP Polynomials

THEOREM 4.1. *$|F_m(n, \mathbb{C})|$ is finite.*

Proof: To prove this theorem, we only have to prove that the number of F-irreducible n-degree F_mPP polynomials is finite. Assume $f(x)$ is such an F-irreducible n-degree F_mPP polynomial and $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, where $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{C}$. As in Section 3, we exclude the case where $f(x) = x$ and make the same assumption that $\alpha_1, \alpha_2, \cdots, \alpha_n$ are all non-zero roots. Notice that if any of $\alpha_1, \alpha_2, \cdots, \alpha_n$ is zero, the only possible case is where $f(x) = x$, otherwise $f(x)$ will be F-reducible.

LEMMA 4.1.1. *$\alpha_1, \alpha_2, \cdots, \alpha_n$ are all roots of unity and their powers as roots of unity are less than or equal to $m^n - 1$.*

Proof of Lemma 4.1.1: We construct a graph G_f that corresponds to $f(x)$. According to property 2 from the last section, there is one and only one directed cycle in G_f.

First, we consider the vertices in a cycle. Suppose the sequence of arrows (α_i, α_{i+1}), $(\alpha_{i+1}, \alpha_{i+2})$, $\cdots$, $(\alpha_{i+k-1}, \alpha_{i+k})$, (α_{i+k}, α_i) form a directed cycle. By definition of G_f, we know that $\alpha_{i+k} = \alpha_{i+k-1}^m = \alpha_{i+k-2}^{m^2} = \cdots = \alpha_i^{m^k}$ and

$\alpha_{i+k}^m = \alpha_i$. Hence, $\alpha_i^{m^{k+1}} = \alpha_i$, and α_i is a t^{th} root of unity where

$$t = m^{k+1} - 1.$$

Because α_i can be selected arbitrarily, we know that every vertex in the cycle is a t^{th} root of unity. Therefore, every number in a cycle is a root of unity.

Then, we look at the vertices that are not in a cycle. According to property 2, these vertices are all connected to the vertices in a cycle. Consider a directed path p that connects a vertex not in a cycle with a vertex in a cycle. Given property 1, we know that p is directed toward the cycle. Let α_j be an arbitrary vertex on p, and α_i the endpoint of the path. α_i is in the cycle, so α_i is a root of unity. Meanwhile, $\alpha_j^{m^r} = \alpha_i$ for some positive integer r, so α_j is also a root of unity. Thus, every vertex not in a cycle is also a root of unity.

Suppose the length of the directed cycle in G_f is s. From the proof above, we know that the vertices in that cycle are all $(m^s - 1)^{th}$ root of unity, and vertices not in the cycle are roots of unity with powers less than or equal to $m^{n-s} \cdot (m^s - 1) = m^n - m^{n-s}$ since the length of p is less than or equal to $n - s$. Therefore, the powers of $\alpha_1, \alpha_2, \cdots, \alpha_n$ as roots of unity have an upper bound $m^n - 1$, which completes the proof of Lemma 4.1.1. □

We know that for a F-irreducible $f(x)$, G_f contains one directed cycle. Because the length of that cycle is less than or equal to n, the powers of $\alpha_1, \alpha_2, \cdots, \alpha_n$ as roots of unity are less than or equal to $m^n - 1$. Since the powers of $\alpha_1, \alpha_2, \cdots, \alpha_n$ as roots of unity have an upper bound, there is a finite number of ways to choose $\alpha_1, \alpha_2, \cdots, \alpha_n$ and to construct $f(x)$. In other words, the number of monic F-irreducible n-degree F_mPP polynomials is finite.

Because n is given, we know that the number of F-irreducible F_mPP polynomials with degrees less than or equal to n is also finite. On the other hand, since every F-reducible polynomial is the product of F-irreducible polynomials of smaller degrees, we know that the number of F-reducible F_mPP polynomials with degrees less than or equal to n is also finite. Therefore, the number of all F_mPP polynomials with degrees less than or equal to n is finite, i.e. $|F_m(n, \mathbb{C})|$ is finite. □

Corollary 4.1.2. *$|F_m(n, \mathbb{Q})|$ is finite.*

This is obviously true because $F_m(n, \mathbb{Q}) \subset F_m(n, \mathbb{C})$.

Corollary 4.1.3. *For any given positive integers m and n, $n \mid \varphi(m^n - 1)$.*

This result comes from the computation of the number of F_mPP polynomials with a given degree n over $\mathbb{C}$. For given positive integers m and n, we want

to calculate the number of F_mPP polynomials with degree n. Suppose $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ is a F_mPP polynomial. To start, we consider the case where $\alpha_1, \alpha_2, \cdots \alpha_n$ are in the same cycle. It follows that $\alpha_1, \alpha_2, \cdots \alpha_n$ are all $(m^n-1)^{th}$ roots of unity. To simplify the problem, we let $\alpha_1, \alpha_2, \cdots \alpha_n$ be primitive $(m^n-1)^{th}$ roots of unity. (If they are non-primitive roots of unity, the length of the cycle might be less than n.) We know that there are $\varphi(m^n-1)$ ways to choose an α_i, where $1 \leq i \leq n$. Once α_i is selected, the whole cycle is determined. Notice that choosing α_i^m, or $\alpha_i^{m^2}, \cdots$, or $\alpha_i^{m^{n-1}}$ will bring us the same cycle. To remove the duplicates, we divide the total number $\varphi(m^n-1)$ by n to get the final answer. Since we can construct this cycle for any given m and n, we know that n divides $\varphi(m^n-1)$.

COROLLARY 4.1.4. *Let $f(x)$ be a F-irreducible F_mPP polynomial with degree n. If the roots of $f(x)$ form a cycle of length n in G_f and $n = \varphi(m^n-1)$, then $f(x)$ is a $(m^n-1)^{th}$ cyclotomic polynomial.*

Suppose $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$. We know that α_i is a $(m^n-1)^{th}$ root of unity for all $i \in \{1, 2, \cdots, n\}$. If α_i is a non-primitive $(m^n-1)^{th}$ root of unity, we assume that α_i is a primitive k^{th} root of unity. We know that $k \mid m^n-1$. It follows that $(k, m) = 1$. Thus, $\alpha_i^m, \alpha_i^{m^2}, \cdots, \alpha_i^{m^{n-1}}$ are all primitive k^{th} roots of unity. On the other hand, $k \mid m^n-1$ indicates that $\varphi(k) \mid \varphi(m^n-1) = n$. Because there are n elements in the set $\{\alpha_i, \alpha_i^m, \alpha_i^{m^2}, \cdots, \alpha_i^{m^{n-1}}\}$ and there are only $\varphi(k)$ primitive k^{th} roots of unity to choose from, we know that there must be repeats in the set, which contradicts our assumption that $f(x)$ is F-irreducible. Therefore, α_i is a primitive $(m^n-1)^{th}$ root of unity, and $\alpha_1, \alpha_2, \cdots, \alpha_n$ are precisely the n primitive $(m^n-1)^{th}$ roots of unity. It follows that $f(x)$ is a $(m^n-1)^{th}$ cyclotomic polynomial.

Now we explore F_mPP polynomials over $\mathbb{Q}$. Because being a F_mPP polynomial with rational coefficients is a stricter restriction, we want to prove a stronger theorem on the finiteness of such polynomials with a fixed degree and varying m.

THEOREM 4.2. *$|F(n, \mathbb{Q})|$ is finite.*

Proof: Assume $f(x) \in \mathbb{Q}[x]$ is an F-irreducible n-degree FPP polynomial and $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, where $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{C}$. Suppose $f(x) \mid f(x^m)$, where m is a positive integer. We pick a root α_t and let the minimal polynomial of α_t over $\mathbb{Q}$ be $p(x)$. $p(x) \mid f(x)$, so the degree of $p(x)$ is less than or equal to that of $f(x)$, that is, $deg(p(x)) \leq deg(f(x)) = n$. We then construct a quotient ring: $K = \mathbb{Q}[x]/(p(x))$. It follows that $[K : \mathbb{Q}] = deg(p(x))$. Because $p(x)$ is the minimal polynomial of α_t over $\mathbb{Q}$, we have $\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}(\alpha_t)$. Thus, $[\mathbb{Q}(\alpha_t) : \mathbb{Q}] = [K : \mathbb{Q}] = deg(p(x)) \leq n$.

On the other hand, we know that according to Lemma 4.1.1, $\alpha_1, \alpha_2, \cdots, \alpha_n$ are all roots of unity, so they are all primitive roots of unity for some powers. This means $\mathbb{Q}(\alpha_t)$ is a cyclotomic field. Suppose α_t is a primitive k^{th} root of unity and we have: $[\mathbb{Q}(\alpha_t) : \mathbb{Q}] = \varphi(k)$. Therefore, $\varphi(k) \leq n$. We now prove that k has an upper bound that only depends on the value of n.

Suppose the prime factorization of k is $k = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = \prod_{i=1}^{r} p_i^{a_i}$, where $p_1, p_2, \cdots, p_r$ are distinct prime numbers. We know that $n \geq \varphi(k) = k(1 - \frac{1}{p_1})(1-\frac{1}{p_2}) \cdots (1-\frac{1}{p_r}) = \prod_{i=1}^{r} p_i^{a_i-1}(p_i-1)$. It follows that $p_i \leq n+1$. Meanwhile, we have: $k \cdot \prod_{i=1}^{r}(p_i - 1) = \prod_{i=1}^{r} p_i^{a_i}(p_i - 1) \leq n \cdot \prod_{i=1}^{r} p_i$. Hence, we know that $k \leq n \cdot \prod_{i=1}^{r} \frac{p_i}{p_i - 1} \leq n \cdot \prod_{p_i \leq n+1} \frac{p_i}{p_i - 1} < n \cdot 2^n$. This indicates that k has an upper bound that only depends on the value of n. Suppose $k \leq k_0$. To construct $f(x)$ of degree n, we just need to select n primitive roots of unity with powers less than or equal to k_0 as the roots of $f(x)$, and then check whether the coefficients of $f(x)$ are rational.

Because there is a finite number of ways of choosing each root of $f(x)$ and the degree of $f(x)$ has an upper bound n, we know that the number of such FPP polynomials in $\mathbb{Q}[x]$ is finite, i.e. $|F(n, \mathbb{Q})|$ is finite. □

Corollary 4.2.1. *There exists a positive integer M such that for any m, $F_m PP(n, \mathbb{Q}) \subset \bigcup_{i=1}^{M} F_i PP(n, \mathbb{Q})$.*

The proof of this corollary is self-explanatory since we have already proved that regardless of the value of m, the number of FPP polynomials with rational coefficients is finite.

Theorem 4.3. $F(n, \mathbb{Q}) = F(n, \mathbb{Z})$

Proof: Let $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ be a FPP polynomial with rational coefficients. First we consider the case where $x \nmid f(x)$. $\alpha_1, \alpha_2, \cdots, \alpha_n$ are all non-zero roots in this case. Suppose $p_i(x)$ is the minimal polynomial of α_i, where $1 \leq i \leq n$. We know that $p_i(x) \mid f(x)$. Let $p(x) := \prod_i p_i(x)$ where the product runs over all distinct $p_i(x)$, so $p(x) \mid f(x)$. Meanwhile, since the roots of $p(x)$ cover all α_i's, we have $f(x) \mid p(x)$. Thus, $f(x) = p(x)$. This means $f(x)$ is a product of cyclotomic polynomials. Since cyclotomic polynomials have integer coefficients, we know that $f(x)$ must have integer coefficients. If

$x \mid f(x)$, we know that $f(x)$ is either in the form of x^k or it is a product of x^k and cyclotomic polynomials. In this case, $f(x)$ also has integer coefficients. □

THEOREM 4.4. *$f(x) \in \mathbb{Q}[x]$ has FPP if and only if it is a product of x^k and cyclotomic polynomials.*

Proof: The claim that $f(x) \in \mathbb{Q}[x]$ has FPP only if it is a product of x^k and cyclotomic polynomials results directly from the proof of Theorem 4.3. We only need to prove that every cyclotomic polynomial is FPP. Suppose $\Phi_k(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$ is a cyclotomic polynomial and its roots are the primitive k^{th} roots of unity. We know that $\beta_i^k = 1$ for any $i \in \{1, 2, \cdots, n\}$, which means $\beta_i^{k+1} = \beta_i$. Hence, $x - \beta_i \mid x^{k+1} - \beta_i$. It follows that $\Phi_k(x)$ is a $F_{k+1}PP$ polynomial and is thus FPP. Therefore, If $f(x)$ is a product of x^k and cyclotomic polynomials, it must be a FPP polynomial. □

COROLLARY 4.4.1. *If $\Phi_k(x)$ is a cyclotomic polynomial, its roots are all in the same cycle in G_{Φ_k}.*

This is obviously true since all the roots are primitive k^{th} roots of unity.

COROLLARY 4.4.2. *If $\Phi_k(x)$ is a cyclotomic polynomial with degree n, then $n = \varphi(k)$. (i.e. The converse of Corollary 4.1.4 is also true.)*

We know that G_{Φ_k} is a cycle of length n. Since the number of primitive k^{th} roots of unity is $\varphi(k)$, we know that $n = \varphi(k)$.

From Theorem 4.3 and 4.4, we can reach the conclusion that a F-irreducible FPP polynomial with integer coefficients is a cyclotomic polynomial. Since there is a known number of cyclotomic polynomials given an upper bound on its degree, we can calculate the number of FPP polynomials with integer coefficients and a given degree.

REFERENCES

[1] N. Biggs, E. Lloyd, R. Wilson *Graph Theory*, 1736-1936, Oxford University Press (1986)

[2] K. Ireland, M. Rosen *A Classical Introduction to Modern Number Theory* , in Graduate Texts in Mathematics, Volume 84, Springer (1998)

[3] P. Morandi *Field and Galois Theory*, in Graduate Texts in Mathematics, Volume 167, Springer (1996)

[4] Qiu Wei Sheng *Abstract Algebra*, 2nd Edition, Higher Education Press (2015)