On G-polynomials with integer coefficients

Ahmed Ayache
Department of Science, College of Science, University of Bahrain
P. O. Box 32038, Kingdom of Bahrain,
aaayache@uob.edu.bh

Abstract: Let $k \geq 2$ be an integer and let $P(X)$ be a monic polynomial of $\mathbb{Z}[X]$ with degree $k-1$. We say that $P(X)$ is a $G-$polynomial if for each $n \in \{1, 2, \ldots, k\}$, $P(X)$ divides $P(X^n)$ in the ring $\mathbb{Z}[X]$ if and only if $\gcd(n, k) = 1$. We present several approaches on finding necessary and sufficient conditions so that $P(X)$ is a $G-$polynomial. Among other interesting results, we show that $A_k(X) := X^{k-1} + X^{k-2} + \cdots X + 1$ is the unique $G-$polynomial of degree $k-1$ if and only if k is a prime number.

2020 AMS Mathematics Subject Classification: 11A05, 11C08, 11R09, 12D05.
Keywords: $G-$polynomials, Cyclotomic polynomials, primes.

1 Introduction

Several authors were interested in polynomials with integer coefficients having all their roots in the unit disc [4], [7]. Other authors focused their study on the divisibility of polynomials with integer coefficients in the ring $\mathbb{Z}[X]$ [3], [8]. Subsequently, some interesting results were settled about polynomials $P(X)$ with integer coefficients that divide $P(X^n)$ for some positive integer n [1], [2]. In this current paper, we continue in the same direction by considering some special kind of polynomials named $G-$polynomials.

For an integer $k \geq 2$, let $A_k(X) := X^{k-1} + X^{k-2} + \cdots X + 1 \in \mathbb{Z}[X]$. It is well-known [2, Theorem 1.4] that for every positive integer n, $A_k(X)$ divides $A_k(X^n)$ in the ring $\mathbb{Z}[X]$ if and only if $\gcd(n, k) = 1$. This result motivates us to set the following definition:

Definition 1 *Let $k \geq 2$ be an integer and let $P(X)$ be a monic polynomial of $\mathbb{Z}[X]$ with degree $k-1$. We say that $P(X)$ is a $G-$polynomial if for each $n \in \{1, 2, \ldots, k\}$, $P(X)$ divides $P(X^n)$ in the ring $\mathbb{Z}[X]$ if and only if* $\gcd(n, k) = 1$.

The reasoning behind the name $G-$polynomials stems from their relationship with the greatest common divisor. One can observe that the equivalence in this definition is essential. Indeed, it may happen that $P(X)$ divides $P(X^n)$ for each $n \in \{1, 2, \ldots, k-1\}$ such that $\gcd(n, k) = 1$, however, $P(X)$ is not a $G-$polynomial. For instance, the polynomial $P(X) = (X-1)(X^2+1)$ of degree

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

3 divides $P(X)$ and $P(X^3)$, and $P(X)$ does not divide $P(X^2)$, however $P(X)$ is not $G-$polynomial because $P(X)$ divides $P(X^4)$.

We denote by $G[k]$ the set of all $G-$polynomials with degree $k-1$. For example, $A_k(X)$ is an element of $G[k]$ whereas the polynomials X^{k-1} and $X^{k-1}-1$ do not belong to $G[k]$. Our goal is to study the set $G[k]$ for any integer $k \geq 2$. Obviously, $X+a$ divides X^2+a if and only if $a=0$ or $a=-1$, so we have

$$G[2] = \{X + a : a \in \mathbb{Z}\backslash\{-1, 0\}\}.$$

Therefore, throughout our study, we impose the condition $k \geq 3$ and we emphisize that any division of polynomials is performed in $\mathbb{Z}[X]$. Our second section concerns Kronecker polynomials. We investigate under which conditions a Kronecker polynomial $P(X)$ divides $P(X^n)$ in $\mathbb{Z}[X]$ for some positive integer n [Theorem 4]. Our third section is devoted to the case where k is a prime number. We show that $G[k] = \{A_k(X)\}$ if and only k is a prime number [Theorem 8]. In the fourth section, we explore the case where k is composite. Several results are established to determine under which conditions a polynomial of $\mathbb{Z}[X]$ is a $G-$polynomial [Theorems 15, 19, 26]. Numerous important consequences are derived [Corollaries 21, 22, 23, 24]. Finally, the fifth section is dedicated to examples to show the scope of our study.

2 Kronecker polynomials

The following characterization collects several facts about Kronecker polynomials. A monic polynomial of $P(X) \in \mathbb{Z}[X]$ with all roots in the unit disc $\{z \in \mathbb{C} : |z| \leq 1\}$ is called a *Kronecker polynomial*. In fact, all the roots of such polynomials have modulus zero or one [4, Theorem 1]. Recall that the a^{th} *cyclotomic polynomial* for a positive integer a, denoted by $\phi_a(X)$ or simply by ϕ_a, is defined by $\phi_a(X) = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n)$, where $\lambda_1, \lambda_2, \ldots, \lambda_n$ are exactly the distinct primitive a^{th} roots of unity. It is shown in [6] that $\phi_a(X)$ is a monic, irreducible polynomial with integer coefficients. Its degree is $\varphi(a)$, where φ is *the Euler's totient function*. Since a cyclotomic polynomial has all its roots in the unit circle $\{z \in \mathbb{C} : |z| = 1\}$, we can then say that any cyclotomic polynomial is a Kronecker polynomial.

Proposition 2 *Let $P(X)$ be a monic polynomial of $\mathbb{Z}[X]$. Then the following conditions are equivalent:*

(i) $P(X)$ is a kronecker polynomial,

(ii) $P(X) = X^r Q(X)$, where r is a non negative integer and $Q(X)$ is a finite product of cyclotomic polynomials,

(iii) There is a positive integer m such that $P(X)$ divides $P(X^p)$ for every prime number $p \geq m$,

(iv) $P(X)$ divides $P(X^t)$ for some integer $t \geq 2$.

Proof. $(i) \Rightarrow (ii)$ from [4, Theorem 2].

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

$(ii) \Rightarrow (iii)$ Suppose that $P(X) := X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$, where r is a non negative integer. Set $m = 1 + Max\{a_i : 1 \leq i \leq s\}$ and let $p \geq m$ be a prime number. Since $\gcd(p, a_i) = 1$ for every $i \in \{1, 2, \ldots, s\}$, then ϕ_{a_i} divides $\phi_{a_i}(X^p)$ [2, Theorem 1.4], so $P(X)$ divides $P(X^p)$.

$(iii) \Rightarrow (iv)$ is trivial.

$(iv) \Rightarrow (i)$ Let λ be a nonzero root of $P(X)$. Since $P(X)$ divides $P(X^t)$ for some integer $t \geq 2$, then $\lambda^t, \lambda^{t^2}, \ldots, \lambda^{t^n}, \ldots$ are roots of $P(X)$. But, as $P(X)$ has finitely many roots, then $\lambda^{t^m} = \lambda^{t^{m+1}}$ for some positive integer m. Thus, $\lambda^{t^m(t-1)} = 1$ and $|\lambda| = 1$. ■

Consequently, every $G-$polynomial is a Kronecker polynomial. Since the set of all Kronecker polynomials of the same given degree is finite, we can conclude that $G[k]$ is also finite for $k \geq 3$. The following Lemma constitutes a significant improvement of [2, Theorem 1.4].

Lemma 3 *Let a, b, α, β and n be positive integers. Set $d := \gcd(n, a)$, then the following conditions are equivalent:*
(i) $(\phi_a)^\alpha$ divides $(\phi_b(X^n))^\beta$,
(ii) $(\phi_a)^\alpha$ divides $(\phi_b(X^d))^\beta$,
(iii) $\alpha \leq \beta$ and $a = bd$.

Proof. $(i) \Rightarrow (iii)$ Suppose that $(\phi_a)^\alpha$ divides $(\phi_b(X^n))^\beta$. Let λ be a root of ϕ_a, then λ^n is a root of ϕ_b and $o(\lambda^n) = b$. Considering the order of λ^n as an element of the cyclic group $< \lambda >$ generated by λ, then $o(\lambda^n) = \frac{o(\lambda)}{\gcd(n,a)} = \frac{a}{d}$. We derive the formula $a = bd$. Obviously, the multiplicity of λ relative to the polynomial $(\phi_a)^\alpha$ is α. Now, assume that $\phi_b = \prod_{i=1}^{t}(X - \mu_i)$. As λ^n is a root of ϕ_b, then $\lambda^n \in \{\mu_1, \mu_2, \ldots, \mu_t\}$, say $\lambda^n = \mu_1$. We have

$$(\phi_b(X^n))^\beta = \prod_{i=1}^{t}(X^n - \mu_i)^\beta = (X^n - \lambda^n)^\beta \prod_{i=2}^{t}(X^n - \mu_i)^\beta = (X - \lambda)^\beta Q(X),$$

where

$$Q(X) = (\sum_{i=1}^{n} X^{n-i}\lambda^{i-1})^\beta \prod_{i=2}^{t}(X^n - \mu_i)^\beta.$$

Since $Q(\lambda) = (n\lambda^{n-1})^\beta \prod_{i=2}^{t}(\mu_1 - \mu_i)^\beta \neq 0$, then the multiplicity of λ relative to $(\phi_b(X^n))^\beta$ is β. Finally, because $(\phi_a)^\alpha$ divides $(\phi_b(X^n))^\beta$, then $\alpha \leq \beta$.

$(iii) \Rightarrow (ii)$ Assume that $\alpha \leq \beta$ and $a = bd$. For every root λ of ϕ_a, we have $o(\lambda) = a$. Since $o(\lambda^d) = \frac{o(\lambda)}{\gcd(d,a)} = \frac{a}{d} = b$, then λ^d is a root of ϕ_b. We deduce that $\phi_b(X^d)$ vanishes on each root of ϕ_a. As the multiplicity of each root of ϕ_a is 1, we conclude that ϕ_a divides $\phi_b(X^d)$. Since $\alpha \leq \beta$, then $(\phi_a)^\alpha$ divides $(\phi_b(X^d))^\beta$.

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

$(ii) \Rightarrow (i)$ Suppose now that $(\phi_a)^\alpha$ divides $(\phi_b(X^d))^\beta$. By using a similar argument as in $(i) \Rightarrow (iii)$, we find that $\alpha \leq \beta$ and $a = b\gcd(d,a) = bd$. Since $\gcd(\frac{n}{d}, b) = 1$, then ϕ_b divides $\phi_b(X^{\frac{n}{d}})$ [2, Theorem 1.3], so $(\phi_b)^\alpha$ divides $(\phi_b(X^{\frac{n}{d}}))^\beta$. Thus, $(\phi_b(X^d)^\beta$ divides $(\phi_b((X^d)^{\frac{n}{d}}))^\beta = (\phi_b(X^n)^\beta$. Finally, as $(\phi_a)^\alpha$ additionally divides $(\phi_b(X^d))^\beta$, then $(\phi_a)^\alpha$ divides $(\phi_b(X^n))^\beta$. ■

For our convenience, if $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ is a Kronecker polynomial, we will assume that $a_1 < a_2 < \cdots < a_s$.

Theorem 4 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial. For every positive integer n, set $d_i := \gcd(n, a_i)$. Then the following conditions are equivalent:*

(i) $P(X)$ divides $P(X^n)$,

(ii) For each $i \in \{1, 2, \ldots, s\}$, there is $j \leq i$ (necessarily unique) such that $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_j}(X^n))^{\alpha_j}$.

(iii) For each $i \in \{1, 2, \ldots, s\}$, there is $j \leq i$ (necessarily unique) such that $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_j}(X^{d_i}))^{\alpha_j}$.

(iv) For each $i \in \{1, 2, \ldots, s\}$, there is $j \leq i$ (necessarily unique) such that $\alpha_i \leq \alpha_j$ and $a_i = a_j d_i$.

(v) For each $i \in \{1, 2, \ldots, s\}$, $d_i = 1$ or there is $j < i$ (necessarily unique) such that $\alpha_i \leq \alpha_j$ and $a_i = a_j d_i$.

Proof. $(i) \Rightarrow (ii)$ Suppose that $P(X)$ divides $P(X^n)$. Then for each $i \in \{1, 2, \ldots, s\}$, ϕ_{a_i} divides $P(X^n) = X^{nr}(\phi_{a_1}(X^n))^{\alpha_1}(\phi_{a_2}(X^n))^{\alpha_2}\cdots(\phi_{a_s}(X^n))^{\alpha_s}$. As ϕ_{a_i} is irreducible in $\mathbb{Z}[X]$, then ϕ_{a_i} divides $\phi_{a_j}(X^n)$ for some $j \in \{1, 2, \ldots, s\}$. In light of Lemma 3, we get $a_i = a_j d_i$ and $j \leq i$. Furthermore, from this latter relationship between a_i and a_j, we deduce that a_j is the sole among the $a_i's$ for which ϕ_{a_i} divides $\phi_{a_j}(X^n)$. Therefore, $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_j}(X^n))^{\alpha_j}$.

$(ii) \Rightarrow (iii) \Rightarrow (iv)$ Results directly from Lemma 3.

$(iv) \Leftrightarrow (v)$ is clear.

$(iv) \Rightarrow (i)$ Let $i \in \{1, 2, \ldots, s\}$. There is $j \in \{1, 2, \ldots, i\}$ such that $a_i = a_j d_i$ and $\alpha_i \leq \alpha_j$. In view of Lemma 3, ϕ_{a_i} divides $\phi_{a_j}(X^n)$, so $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_j}(X^n))^{\alpha_j}$. We conclude that $(\phi_{a_i})^{\alpha_i}$ divides $P(X^n)$ for every $i \in \{1, 2, \ldots, s\}$. As the polynomials $X^r, (\phi_{a_1})^{\alpha_1}, (\phi_{a_2})^{\alpha_2}, \cdots (\phi_{a_s})^{\alpha_s}$ are relatively prime, then $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ divides $P(X^n)$. ■

Remark that the factor X^r of $P(X)$ has no effect in Theorem 4. We can state the following direct result.

Corollary 5 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial and let $Q_h^v(X) = X^v(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_h})^{\alpha_h}$ for some $1 \leq h \leq s$ and $0 \leq v \leq r$. Then the following conditions are equivalent:*

(i) $P(X)$ divides $P(X^n)$

(ii) $Q_h^v(X)$ divides $Q_h^v(X^n)$ for every $h \in \{1, 2, \ldots, s\}$,

(iii) $Q_s^0(X)$ divides $Q_s^0(X^n)$.

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

Corollary 6 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial such that $P(X)$ divides $P(X^n)$. If $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_j}(X^n))^{\alpha_j}$ for some $i, j \in \{1, 2, \ldots, s\}$, set $d_i := \gcd(n, a_i)$ and $d_j := \gcd(n, a_j)$. Then*

(i) d_j divides d_i.

(ii) If, in addition, a_i is a square-free integer, then ϕ_{a_j} divides $\phi_{a_j}(X^n)$.

Proof. (i) By application of Theorem 4(iv), we have $a_i = d_i a_j$. If $d_j = 1$, there is nothing to prove. Let us assume that $d_j \neq 1$. Then there is $h \in \{1, 2, \ldots, s\}$ such that $a_j = d_j a_h$. It follows that $d_i = \gcd(n, a_i) = \gcd(n, d_i a_j) = \gcd(n, d_i d_j a_h) = d_j \gcd(n/d_j, d_i a_h)$. Thus, d_j divides d_i.

(ii) In view of the first point, $d_i = cd_j$ for some positive integer c. Suppose that $d_j \neq 1$. We necessarily have $d_i \neq 1$ and there is $h \in \{1, 2, \ldots, s\}$ such that $a_j = d_j a_h$. Therefore, $a_i = d_i a_j = c(d_j)^2 a_h$ and a_i is not a square-free integer. Hence, $d_j = 1$ and ϕ_{a_j} divides $\phi_{a_j}(X^n)$ [2, Theorem 1.4]. ■

3 The case where k is a prime number

Lemma 7 *Let $P(X) = X^r(\phi_{p_1^{m_1}})^{\alpha_1}(\phi_{p_2^{m_2}})^{\alpha_2}\cdots(\phi_{p_s^{m_s}})^{\alpha_s}$, where $p_1, p_2, \ldots, p_s$ are distinct primes. For every positive integer n, the following conditions are equivalent:*

(i) $P(X)$ divides $P(X^n)$,

(ii) $\gcd(n, p_1 p_2 \cdots p_s) = 1$.

Proof. $(i) \Rightarrow (ii)$ Let $i \in \{1, 2, \ldots, s\}$. By virtue of Theorem 4$(iv)$, since $P(X)$ divides $P(X^n)$, there is $j \in \{1, 2, \ldots, s\}$ such that $p_i^{m_i} = p_j^{m_j} \gcd(n, p_i^{m_i})$. We necessarily have $p_i = p_j$ and $\gcd(n, p_i^{m_i}) = 1$. Thus, $\gcd(n, p_i) = 1$ for all $i \in \{1, 2, \ldots, s\}$. It follows that $\gcd(n, p_1 p_2 \cdots p_s) = 1$.

$(ii) \Rightarrow (i)$ Assume that $\gcd(n, p_1 p_2 \cdots p_s) = 1$. Then $\gcd(n, p_i^{m_i}) = 1$ for all $i \in \{1, 2, \ldots, s\}$. Hence, $P(X)$ divides $P(X^n)$, by Theorem 4(iv), as desired. ■

The following Theorem determines explicitly the set $G[k]$ when k is a prime number.

Theorem 8 *$G[k] = \{A_k(X)\}$ if and only if k is a prime number.*

Proof. Suppose that k is a prime number and let $P(X) \in G[k]$. We need to show that $P(X) = A_k(X)$. Since $P(X)$ is a Kronecker polynomial, then $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$, where $r \geq 0$, $\alpha_i \geq 0$ and $a_i > 0$ are integers. As $\gcd(k, k) = k$, then $P(X)$ does not divide $P(X^k)$. So, there is $i \in \{1, 2, \ldots, s\}$ such that $(\phi_{a_i})^{\alpha_i}$ does not divide $(\phi_{a_i}(X^k))^{\alpha_i}$. By application of Lemma 3, $\gcd(a_i, k) \neq 1$. Since k is a prime number, then k must divide a_i and $\varphi(a_i) \geq \varphi(k) = k - 1$. But $\deg(P(X)) = r + \sum_{i=1}^{s} \alpha_i \varphi(a_i) = k - 1$, we necessarily have $r = 0$, $s = 1$, $\alpha_i = 1$ and $a_i = k$. Hence, $P(X) = \phi_{a_i} = A_k(X)$. Conversely, assume that $G[k]$ consists only of the polynomial $A_k(X)$. We shall prove that k is a prime number by using two steps:

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

Step 1: We first prove that k is square-free: By the contrapositive, suppose that k is a not square-free. Then there is a natural number $q \in \mathbb{N}\backslash\{0,1\}$ such that q^2 divides k. Let $m := k/q$ and consider the polynomial

$$P(X) = A_m(X)(X^{k-m} - 1) = A_m(X)((X^m)^{q-1} - 1).$$

We shall prove that $P(X)$ is a $G-$polynomial. Firstly, note that $P(X) \neq A_k(X)$ since $P(0) = -1$ while $A_k(0) = 1$. Let $n \in \{1, 2, \ldots, k\}$ such that $\gcd(n, k) = 1$. Since $\gcd(m, n) = 1$, then $A_m(X)$ divides $A_m(X^n)$ [1, Theorem 1.4]. Moreover, because $X^{k-m} - 1$ clearly divides $(X^n)^{k-m} - 1$, we deduce that $P(X)$ divides $P(X^n)$. Now, let $n \in \{1, 2, \ldots, k\}$ such that $\gcd(n, k) \neq 1$. We must prove that $P(X)$ does not divide $P(X^n)$. We claim that $\gcd(m, n) \neq 1$. Indeed, if p is a prime number that divides n and k, then p divides m or q. But, as q divides m, we can say that p divides m. Thus p divides m and n, so that $\gcd(m, n) \neq 1$. On the other hand, we have

$$\begin{aligned} P(X^n) &= A_m(X^n)((X^{mn})^{q-1} - 1) \\ &= A_m(X^n)((X^{m(q-1)})^n - 1) \\ &= A_m(X^n)((X^m)^{q-1} - 1)Q(X), \end{aligned}$$

where $Q(X) = \sum_{i=0}^{n-1} X^{im(q-1)}$. Assume that $P(X)$ divides $P(X^n)$. Then $A_m(X)$ divides $A_m(X^n)Q(X)$. Let $\lambda = \exp(\frac{2i\pi}{m})$, then the roots of $A_m(X)$ in $\mathbb{C}$ are $\lambda, \lambda^2, \ldots, \lambda^{m-1}$. Since the polynomial $Q(\lambda^i) = n$ for each $i \in \{1, 2, \ldots, m-1\}$, we conclude that $A_m(X^n)$ vanishes on each root of $A_m(X)$. This means that $A_m(X)$ divides $A_m(X^n)$. It follows that $\gcd(m, n) = 1$ by [2, Theorem 1.4], yielding a contradiction.

Step 2: Suppose, by way of contradiction, that k is not a prime number. Then $k = p_1 p_2 \ldots p_s$ for some prime numbers $p_1, p_2, \ldots, p_s$ with $s > 1$. Consider the polynomial

$$P(X) = X^r A_{p_1}(X) A_{p_2}(X) \cdots A_{p_s}(X),$$

where $r = k - 1 + s - \sum_{i=1}^{s} p_i$. In view of Lemma 7, $P(X)$ divides $P(X^n)$ for every $n \in \{1, 2, \ldots, k\}$ if and only if $\gcd(n, k) = 1$. It results that $P(X)$ is a $G-$polynomial, a contradiction since $G[k] = \{A_k(X)\}$. ■

According to Theorem 8, $G[3]$, $G[5]$, $G[7], \ldots$ are well-known. How about $G[k]$ for a composite number k?

4 The case where k is composite

Lemma 9 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2} \cdots (\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial and let n be a positive integer. If $P(X)$ divides $P(X^n)$, then $\gcd(n, a_1) = 1$.*

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

Proof. Suppose that $P(X)$ divides $P(X^n)$. According to Theorem 4(iv), we have $a_1 = \gcd(n, a_1)a_j$ for some $j \in \{1, 2, \ldots, s\}$. As $a_1 \leq a_j$, we necessarily have $\gcd(n, a_1) = 1$. ■

Set $\wp(1) := \varnothing$. If a is a positive integer, let $\wp(a)$ be the set of all prime numbers that divide a. Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial of degree $k-1$. To provide effective conditions under which $P(X)$ would be a $G-$polynomial, we need some preliminary results that will give us good ideas about the positive integers $a_1, a_2, \ldots, a_s$ of $P(X)$. To this end, we distinguish the cases where $\wp(a_i) \nsubseteq \wp(k)$ or $\wp(a_i) \subseteq \wp(k)$.

Proposition 10 *If $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ is a $G-$polynomial of degree $k-1$, then $\wp(a_1) \subseteq \wp(k) \subseteq \bigcup_{l=1}^{s} \wp(a_l)$.*

Proof. We may assume that $a_1 > 1$. Let $p \in \wp(a_1)$. Then $\gcd(p, a_1) = p$. In light of Lemma 9, $P(X)$ does not divides $P(X^p)$. It follows that $\gcd(p, k) \neq 1$ and $p \in \wp(k)$. Thus, $\wp(a_1) \subseteq \wp(k)$. Now, let $p \in \wp(k)$. Then $P(X)$ does not divide $P(X^p)$. It follows that ϕ_{a_j} does not divide $\phi_{a_j}(X^p)$ for some $j \in \{1, 2, \ldots, s\}$. Hence, $\gcd(p, a_j) \neq 1$ and $p \in \wp(a_j) \subseteq \bigcup_{l=1}^{s} \wp(a_l)$. ■

Corollary 11 (i) *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial of degree $k-1$. If $\bigcup_{l=2}^{s} \wp(a_l) \subseteq \wp(a_1) = \wp(k)$, then $P(X)$ is a $G-$polynomial.*

(ii) *$P(X) = X^r(\phi_a)^{\alpha}$ is a $G-$polynomial of degree $k-1$ if and only if $\wp(k) = \wp(a)$.*

Proof. Let n be a positive integer such that $1 \leq n \leq k$. If $\gcd(n, k) = 1$, then $\gcd(n, a_i) = 1$ and $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_i}(X^n))^{\alpha_i}$ for every $i \in \{1, 2, \ldots, s\}$. Hence, $P(X)$ divides $P(X^n)$. If $\gcd(n, k) \neq 1$, then there is a prime number $p \in \wp(k)$ such that p divides n. As $p \in \wp(a_1)$, then $\gcd(n, a_1) \neq 1$ and $P(X)$ does not divide $P(X^n)$ [Lemma 9]. We conclude that $P(X)$ is a $G-$polynomial. In particular, for $s = 1$, we derive the point (ii) that is a direct consequence of Proposition 10 and the point (i). ■

Corollary 12 (i) *If $P(X) = X^r(\phi_a)^{\alpha}$ is a $G-$polynomial and $\gcd(a, r+1) = 1$, then a is a square-free number and $a - \alpha\varphi(a) \leq r + 1$.*

(ii) *ϕ_a is a $G-$polynomial if and only if a is a prime number.*

Proof. Suppose that $\deg(P(X)) = k - 1$. Then $k = r + 1 + \alpha\varphi(a)$ and $\wp(k) = \wp(a)$ [Proposition 10]. If a has the factorization $a = p_1^{\nu_1}p_2^{\nu_2}\cdots p_s^{\nu_s}$ into prime numbers, then $\varphi(a) = p_1^{\nu_1-1}p_2^{\nu_2-1}\cdots p_s^{\nu_s-1}\prod_{i=1}^{s}(p_i - 1)$. For every

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

$i \in \{1, 2, \ldots, s\}$, p_i divides k and a. Since $\gcd(a, r+1) = 1$, then $\varphi(a)$ is not divisible by p_i. Therefore, $\nu_i = 1$ for all i and $a = p_1 p_2 \cdots p_s$ is a square-free number. We deduce, in particular, that $a \leq k = r + 1 + \alpha\varphi(a)$; that is $a - \alpha\varphi(a) \leq r + 1$. For the second statement, it is sufficient to apply the first point with $r = 0$ and $\alpha = 1$ to get $\varphi(a) = a - 1$. ■

Lemma 13 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2} \cdots (\phi_{a_s})^{\alpha_s}$ be a $G-$polynomial of degree $k-1$. If $i \geq 2$ and $\wp(a_i) \nsubseteq \wp(k)$, then for every $p \in \wp(a_i)\backslash\wp(k)$, there exists a unique $j < i$ such that $\alpha_i \leq \alpha_j$ and $a_i = pa_j$.*

Proof. Let $p \in \wp(a_i)\backslash\wp(k)$. Then $\gcd(p, k) = 1$ and $P(X)$ divides $P(X^p)$. By application of Theorem 4(iv), there exists a unique $j \leq i$ such that $\alpha_i \leq \alpha_j$ and $a_i = \gcd(p, a_i)a_j = pa_j$. In fact, we have $i \neq j$ since $a_i \neq a_j$. ■

Definition 14 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2} \cdots (\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial of degree $k-1$. We say that $P(X)$ is a quasi$-G-$polynomial if either $\wp(k) = \bigcup_{l=1}^{s} \wp(a_l)$; or for every a_i $(i \geq 2)$ such that $\wp(a_i) \nsubseteq \wp(k)$ and $p \in \wp(a_i)\backslash\wp(k)$, there exists a unique $j < i$ such that $\alpha_i \leq \alpha_j$ and $a_i = a_j p$.*

In view of Lemma 13, every $G-$polynomial is quasi$-G-$polynomial. The following Theorem provides several characterizations of quasi$-G-$polynomials.

Theorem 15 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2} \cdots (\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial of degree $k-1$. If $\wp(a_1) \subseteq \wp(k)$, then the following conditions are equivalent:*

(i) $P(X)$ is a quasi$-G-$polynomial,

(ii) If $\wp(a_i) \nsubseteq \wp(k)$ and $p_1, p_2, \ldots, p_u$ of $\wp(a_i)\backslash\wp(k)$ such that $p_1^{h_1}$, $p_2^{h_2}$, $\cdots$, $p_u^{h_u}$ divide a_i for positive integers $h_1, h_2, \ldots, h_u$, then there exists a unique $j < i$ such that $\alpha_i \leq \alpha_j$ and $a_i = p_1^{h_1} p_2^{h_2} \cdots p_u^{h_u} a_j$,

(iii) If $\wp(a_i) \nsubseteq \wp(k)$, then there exists a unique $j \leq i$ such that $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_j}(X^n))^{\alpha_j}$ for every positive integer n such that $\gcd(n, k) = 1$,

(iv) $P(X)$ divides $P(X^n)$ for every positive integer n such that $\gcd(n, k) = 1$,

(v) $P(X)$ divides $P(X^p)$ for every prime p such that $p \notin \wp(k)$.

Proof. $(i) \Rightarrow (ii)$ Since $P(X)$ is a quasi$-G-$polynomial, there exists a unique $j_1 < i$ such that $\alpha_i \leq \alpha_{j_1}$ and $a_i = p_1 a_{j_1}$. If $h_1 \geq 2$, then $p_1 \in \wp(a_{j_1})\backslash\wp(k)$, and there exists a unique $j_2 < j_1$ such that $\alpha_{j_1} \leq \alpha_{j_2}$ and $a_{j_1} = p_1 a_{j_2}$. Thus, $\alpha_i \leq \alpha_{j_1} \leq \alpha_{j_2}$ and $a_i = p_1^2 a_{j_2}$. We can continue and use the same argument to prove that there exists a unique $i_1 < i$ such that $\alpha_i \leq \alpha_{i_1}$ and $a_i = p_1^{h_1} a_{i_1}$. Moreover, we have $\{p_2, \ldots, p_u\} \subseteq \wp(a_{i_1})\backslash\wp(k)$. Repeating the same procedure for a_{i_1}, we find that there exists a unique $i_2 < i_1 < i$ such that $\alpha_{i_1} \leq \alpha_{i_2}$ and $a_{i_1} = p_2^{h_2} a_{i_2}$. Thus, $\alpha_i \leq \alpha_{i_2}$ and $a_i = p_1^{h_1} p_2^{h_2} a_{i_2}$. After some finite steps, we progressively realize that there exists a unique $j < i$ such that $\alpha_i \leq \alpha_j$ and $a_i = p_1^{h_1} p_2^{h_2} \cdots p_u^{h_u} a_j$.

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

$(ii) \Rightarrow (i)$ is trivial.

$(ii) \Rightarrow (iii)$ Let n be a positive integer such that $\gcd(n,k) = 1$, and assume that $\wp(a_i) \nsubseteq \wp(k)$. If $\gcd(n,a_i) = 1$, then $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_i}(X^n))^{\alpha_i}$ [2, Theorem 1.3]. Let us assume that $\gcd(n,a_i) \neq 1$. As $\gcd(n,k) = 1$, then $\gcd(n,a_i) = p_1^{h_1}p_2^{h_2}\cdots p_u^{h_u}$ for some primes $p_1, p_2 \ldots, p_u \in \wp(a_i)\backslash\wp(k)$ and non-negative integers $h_1, h_2 \ldots, h_u$ (not all equal to 0). Therefore, there exists a (unique) $j < i$ such that $\alpha_i \leq \alpha_j$ and $a_i = p_1^{h_1}p_2^{h_2}\cdots p_u^{h_u}a_j = \gcd(n,a_i)a_j$ Hence, there exists a unique $j \leq i$ such that $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_j}(X^n))^{\alpha_j}$.

$(iii) \Rightarrow (iv)$ Let n be a positive integer such that $\gcd(n,k) = 1$ and let $i \in \{1,2,\ldots,k\}$. Obviously, $\gcd(n,a_1) = 1$ since $\wp(a_1) \subseteq \wp(k)$. We may suppose that $i \geq 2$. If $d_i = \gcd(n,a_i) = 1$, we are done. If $d_i \neq 1$, then $\wp(a_i) \nsubseteq \wp(k)$. From (iii), there exists a unique $j \leq i$ such that $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_j}(X^n))^{\alpha_j}$. It follows that there is $j \leq i$ such that $\alpha_i \leq \alpha_j$ and $a_i = a_j d_i$. Hence, $P(X)$ divides $P(X^n)$ by Theorem 4(v).

$(iv) \Rightarrow (v)$ is trivial.

$(v) \Rightarrow (i)$ If $\wp(k) = \bigcup_{l=1}^{s} \wp(a_l)$, then we are done. Let a_i such that $\wp(a_i) \nsubseteq \wp(k)$. According to (v), for every prime $p \in \wp(a_i)\backslash\wp(k)$, $P(X)$ divides $P(X^p)$. By virtue of Theorem 4(iv), there is a unique $j < i$ such that $\alpha_i \leq \alpha_j$ and $a_i = \gcd(p,a_i)a_j = pa_j$. Hence, $P(X)$ is a quasi$-G-$polynomial. ■

Corollary 16 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ be a quasi$-G-$polynomial of degree $k-1$. If for $i \geq 2$, $\wp(a_i)\backslash\wp(k)$ consists of the primes $p_1, p_2, \ldots, p_u$, then there exists a unique $j < i$ and unique positive integers m_1, m_2, ..., m_u such that $\alpha_i \leq \alpha_j$ and $a_i = p_1^{m_1}p_2^{m_2}\cdots p_u^{m_u}a_j$ with $\wp(a_j) \subseteq \wp(k)$.*

Proof. Suppose that a_i has the factorization

$$a_i = p_1^{m_1}p_2^{m_2}\cdots p_u^{m_u}q_1^{n_1}q_2^{n_2}\cdots q_v^{n_v}$$

into primes such that $q_i \in \wp(k)$ while $p_i \notin \wp(k)$ for each i. In view of Theorem 15(ii), there exists a unique $j < i$ such that $\alpha_i \leq \alpha_j$ and $a_i = p_1^{m_1}p_2^{m_2}\cdots p_u^{m_u}a_j$. A fortiori, we have $a_j = q_1^{n_1}q_2^{n_2}\cdots q_v^{n_v}$ and $\wp(a_j) \subseteq \wp(k)$. ■

The following Corollary readily comes from Theorem 15 since any $G-$polynomial is a quasi$-G-$polynomial.

Corollary 17 *If $P(X)$ is a $G-$polynomial of degree $k-1$, then $P(X)$ divides $P(X^n)$ for every positive integer n such that $\gcd(n,k) = 1$.*

It is well-known [2, Theorem 1.4] that for every positive integer n, $A_k(X)$ divides $A_k(X^n)$ if and only if $\gcd(n,k) = 1$. A question arises: In the definition of a $G-$polynomial $P(X)$ of degree $k-1$, can we replace $n \in \{1,2,\ldots,k\}$ by any positive integer n? The next corollary provides a partial answer.

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

Corollary 18 *Let* $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ *be a Kronecker polynomial of degree* $k-1$. *If* a_i *divides* k *for each* $i \in \{1,2,\ldots,s\}$, *then the following conditions are equivalent:*

(*i*) $P(X)$ *is a* $G-$*polynomial,*

(*ii*) *For each positive integer* n, $P(X)$ *divides* $P(X^n)$ *if and only if* $\gcd(n,k) = 1$.

Proof. In view of Corollary 17, it is sufficient to prove that if $P(X)$ is a $G-$polynomial and n is a positive integer such that $\gcd(n,k) \neq 1$, then $P(X)$ does not divide $P(X^n)$. Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$. Set $m = \gcd(n,k)$, then $\gcd(k,m) = m \neq 1$ and $1 \leq m \leq k$, so $P(X)$ does not divide $P(X^m)$. By virtue of Theorem 4(*iii*), there exists $i \in \{1,2,\ldots,s\}$ such that for every $j \leq i$, $(\phi_{a_i})^{\alpha_i}$ does not divide $(\phi_{a_j}(X^{b_i}))^{\alpha_j}$, where $b_i = \gcd(m,a_i)$. Because a_i divides k, then

$$b_i = \gcd(m,a_i) = \gcd(\gcd(n,k),a_i) = \gcd(n,\gcd(k,a_i)) = \gcd(n,a_i) = d_i.$$

It follows that there exists $i \in \{1,2,\ldots,s\}$ such that for every $j \leq i$, $(\phi_{a_i})^{\alpha_i}$ does not divide $(\phi_{a_j}(X^{d_i}))^{\alpha_j}$. Once again, from Theorem 4(*iii*), we deduce that $P(X)$ does not divide $P(X^n)$. ■

The following Theorem provides some sufficient conditions for a polynomial to be a $G-$polynomial.

Theorem 19 *Let* $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ *be a Kronecker polynomial of degree* $k-1$. *If the following conditions are satisfied*

1) $\wp(a_1) \subseteq \wp(k) \subseteq \bigcup_{l=1}^{s} \wp(a_l)$,

2) $P(X)$ *is a quasi*$-G-$*polynomial, and*

3) *If for* $i \geq 2$, $\wp(a_i) \subseteq \wp(k)$, *then either* $\wp(a_i) \subseteq \bigcup_{l<i} \wp(a_l)$, *or for every* $j < i$, $\alpha_i > \alpha_j$ *or* $\frac{a_i}{a_j}$ *is not the product of primes of* $\wp(a_i) \setminus \bigcup_{l<i} \wp(a_l)$,

then $P(X)$ *is a* $G-$*polynomial.*

Proof. Suppose that the conditions (1), (2) and (3) are satisfied, and let n be a positive integer such that $1 \leq n \leq k$. Assume that $\gcd(n,k) = 1$. Since $P(X)$ is a quasi$-G-$polynomial [Theorem 15], then $P(X)$ divides $P(X^n)$. Assume now that $\gcd(n,k) \neq 1$. We need to show that $P(X)$ does not divide $P(X^n)$. We have $\gcd(n,k) = p_1^{h_1}p_2^{h_2}\cdots p_t^{h_t}$ for some primes $p_1,p_2,\ldots,p_t$ of $\wp(k)$ and nonnegative integers $h_1,h_2\ldots,h_t$ (not all equal to 0). Because of $\wp(k) \subseteq \bigcup_{l=1}^{s} \wp(a_l)$, every p_j must belong to some of the $\wp(a_l)$'s. Let a_i be the first among the a_l's that contains one of the p_j's, say p. Then p divides $\gcd(n,a_i)$ and $\gcd(n,a_i) \neq 1$. It is clear that $a_i \neq 1$. Moreover, if $i = 1$, then $\gcd(n,a_1) \neq 1$, so $P(X)$ does not divide $P(X^n)$ [Lemma 9]. Let us suppose that $i \geq 2$. If $\wp(a_i) \nsubseteq \wp(k)$, let

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

$q \in \wp(a_i)\backslash\wp(k)$. As $P(X)$ is a quasi$-G-$polynomial, there exists $j < i$ such that $\alpha_i \leq \alpha_j$ and $a_i = qa_j$. Notice that $q \neq p$ since $p \in \wp(k)$ while $q \notin \wp(k)$. Since p divides $a_i = qa_j$, then p divides a_j and $p \in \wp(a_j)$, but this contradicts the choice of a_i. We deduce that $\wp(a_i) \subseteq \wp(k)$. Moreover, according to the condition (3), if $\wp(a_i) \subseteq \bigcup_{l<i} \wp(a_l)$, then $p \in \wp(a_j)$ for some $j < i$, but this contradicts the choice of a_i. It follows that $\wp(a_i) \nsubseteq \bigcup_{l<i} \wp(a_l)$ for all i. Let $j \leq i$ be a positive integer. If $j = i$, then $(\phi_{a_i})^{\alpha_i}$ does not divide $(\phi_{a_i}(X^n))^{\alpha_i}$ since $\gcd(n, a_i) \neq 1$. Let $j < i$. If $(\phi_{a_i})^{\alpha_i}$ divides $(\phi_{a_j}(X^n))^{\alpha_j}$, then $\alpha_i < \alpha_j$ and $\frac{a_i}{a_j} = \gcd(n, a_i) = q_1^{m_1} q_2^{m_2} \cdots q_u^{m_u}$ for some primes $q_1, q_2, \ldots, q_t$ of $\wp(a_i)$ [Lemma 3]. As $\wp(a_i) \subseteq \wp(k)$, then $q_1, q_2, \ldots, q_u$ divide $\gcd(n, k) = p_1^{h_1} p_2^{h_2} \cdots p_t^{h_t}$, so $\{q_1, q_2, \ldots, q_u\} \subseteq \{p_1, p_2, \ldots, p_t\} \subseteq \wp(a_i)$. But this contradicts the fact $\alpha_i > \alpha_j$ or $\frac{a_i}{a_j}$ is not the product of primes of $\wp(a_i)\backslash\bigcup_{l<i} \wp(a_l)$. Hence, $(\phi_{a_i})^{\alpha_i}$ does not divide $(\phi_{a_j}(X^n))^{\alpha_j}$ for every $j \leq i$, and $P(X)$ does not divide $P(X^n)$ by Theorem 4(ii). ■

Remark 20 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2} \cdots (\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial of degree $k-1$. If $P(X)$ is a $G-$polynomial, then the conditions* (1) *and* (2) *of Theorem 19 are satisfied according to Proposition 10 and Lemma 13. However, the conditions* (3) *does not hold in general (see example 27). It follows that the converse of Theorem 19 is false.*

Consequently, we can derive various Corollaries that characterizes $G-$polynomials in special circumstances.

Corollary 21 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2} \cdots (\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial of degree $k-1$. If $\wp(k) = \bigcup_{l=1}^{s} \wp(a_l)$ and for every $j < i$, either $\alpha_i > \alpha_j$ or a_j does not divide a_i, then $P(X)$ is a $G-$polynomial.*

Corollary 22 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2} \cdots (\phi_{a_s})^{\alpha_s}$ be a Kronecker polynomial of degree $k-1$. If $\wp(a_i) \nsubseteq \wp(k)$ for every $i \geq 2$, then the following conditions are equivalent:*

(i) $P(X)$ is a $G-$polynomial,

(ii) $\wp(a_1) = \wp(k)$ and $P(X)$ is a quasi$-G-$polynomial.

Proof. $(i) \Rightarrow (ii)$ $P(X)$ is a quasi$-G-$polynomial by Lemma 13. For each $i \geq 2$, $\wp(a_i) \nsubseteq \wp(k)$. Then $a_i = p_1^{m_1} p_2^{m_2} \cdots p_u^{m_u} a_j$ for some primes $p_1, p_2, \ldots, p_u \notin \wp(k)$ and a_j such that $\wp(a_j) \subseteq \wp(k)$ [Corollary 16]. But a_1 is the sole element among the a_l 's that satisfies $\wp(a_1) \subseteq \wp(k)$. Thus, for each $i \geq 2$, $a_i = p_1^{m_1} p_2^{m_2} \cdots p_u^{m_u} a_1$. Since $\wp(a_1) \subseteq \wp(k) \subseteq \bigcup_{l=1}^{s} \wp(a_l)$ [Proposition 10], then $\wp(k) \subseteq \wp(a_1)$; that is $\wp(a_1) = \wp(k)$.

$(ii) \Rightarrow (i)$ directly results from Theorem 19. ■

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

Corollary 23 *Let $P(X) = X^r(\phi_{p_1^{m_1}})^{\alpha_1}(\phi_{p_2^{m_2}})^{\alpha_2}\cdots(\phi_{p_s^{m_s}})^{\alpha_s}$, where $p_1, p_2, \ldots, p_s$ are distinct primes. Then $P(X)$ is a $G-$polynomial of degree $k-1$ if and only if $\wp(k) = \{p_1, p_2, \ldots, p_s\}$.*

Proof. Suppose that $\wp(k) = \{p_1, p_2, \ldots, p_s\}$. Then $\wp(k) = \bigcup_{l=1}^{s} \wp(p_l^{m_l})$. As $p_i^{m_i}$ does not divide $p_j^{m_j}$ for each $j < i$, then $P(X)$ is a $G-$polynomial by Corollary 21. Conversely, assume now that $P(X)$ is $G-$polynomial. Let $p \in \{p_1, p_2, \ldots, p_s\}$. Then $\gcd(p, p_1p_2\cdots p_s) \neq 1$. In view of Lemma 7, $P(X)$ does not divide $P(X^p)$. Therefore, $\gcd(p, k) \neq 1$ and $p \in \wp(k)$. Thus, $\wp(k) = \{p_1, p_2, \ldots, p_s\}$. ■

As an application of Corollary 23, if $\wp(k) = \{p\}$, then $P(X) = X^r(\phi_{p^m})^{\alpha}$ is a polynomial of degree $k-1 = r + \alpha\varphi(p^m)$ and we have the following nice result.

Corollary 24 *Let p be a prime number. Then the following conditions are equivalent:*

(i) $P(X) = X^r(\phi_{p^m})^{\alpha}$ is a G-polynomial of degree $k-1$.

(ii) $k = p^{\upsilon}$, where $\upsilon = \log_p(r + 1 + \alpha p^m - \alpha p^{m-1})$.

The upcoming Theorem characterizes $G-$polynomials of the form $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}$. But before embarking in this direction, let us provide a preparatory Lemma concerning the condition (3) of Theorem 19.

Lemma 25 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}\cdots(\phi_{a_s})^{\alpha_s}$ be a $G-$polynomial of degree $k-1$. If $\wp(a_s) \subseteq \wp(k)$, then either $\wp(a_s) \subseteq \bigcup_{l<s} \wp(a_l)$, or for every $j < s$, $\alpha_s > \alpha_j$ or $\frac{a_s}{a_j}$ is not the product of primes of $\wp(a_s) \setminus \bigcup_{l<s} \wp(a_l)$.*

Proof. Suppose, by way of contradiction, that $\wp(a_s) \nsubseteq \bigcup_{l<s} \wp(a_l)$, and that there exists $j < s$ such that $\alpha_s \leq \alpha_j$ and $\frac{a_s}{a_j} = p_1^{h_1}p_2^{h_2}\cdots p_t^{h_t}$ for some primes $p_1, p_2, \ldots, p_t \in \wp(a_s) \setminus \bigcup_{l<s} \wp(a_l)$. Set $n = p_1^{h_1}p_2^{h_2}\cdots p_t^{h_t}$, then $\gcd(n, a_s) = n$. Therefore, $\alpha_s \leq \alpha_j$ and $a_s = a_j \gcd(n, a_s)$. On the other hand, we have $p_1, p_2, \ldots, p_t \notin \wp(a_l)$ for each $l < s$. Thus, $\gcd(n, a_l) = 1$ for each $l < s$. It results that $P(X)$ divides $P(X^n)$ [Theorem 4(*v*)]. But, as by assumption $\wp(a_s) \subseteq \wp(k)$, then $\gcd(n, k) \neq 1$, a contradiction. ■

Theorem 26 *Let $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}$ be a Kronecker polynomial of degree $k-1$*

(A) If $a_1 \neq 1$, then $P(X)$ is a $G-$polynomial if and only if

(1) $\wp(a_1) \subseteq \wp(k) \subseteq \wp(a_1) \cup \wp(a_2)$,

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

(2) $\wp(a_2) \nsubseteq \wp(k)$ *implies* $\alpha_2 \leq \alpha_1$ *and* $a_2 = pa_1$ *for some* $p \in \wp(a_2)\backslash\wp(k)$,

(3) $\wp(a_2) \subseteq \wp(k)$ *implies either* $\wp(a_2) \subseteq \wp(a_1)$, *or* $\alpha_2 > \alpha_1$ *or* $\frac{a_2}{a_1}$ *is not the product of primes of* $\wp(a_2)\backslash\wp(a_1)$.

(*B*) *If* $a_1 = 1$, *then* $P(X)$ *is a* $G-$*polynomial if and only if* $\wp(a_2) = \wp(k)$ *and* $\alpha_2 > \alpha_1$.

Proof. We begin by considering $a_1 \neq 1$. According to Theorem 19, if (1), (2) and (3) are satisfied, then $P(X)$ is a $G-$polynomial. Conversely, assume that $P(X)$ is a $G-$polynomial. Then (1) results from Proposition 10 and (2) comes from Lemma 13. Finally, the point (3) is a direct consequence of Lemma 25 for $s = 2$.

It remains to treat the case (*B*) where $a_1 = 1$. We have $\wp(a_1) = \varnothing$. Suppose that $P(X)$ is a $G-$polynomial. Then $\wp(k) \subseteq \wp(a_2)$ by Proposition 10. If $\wp(a_2) \nsubseteq \wp(k)$, then $\alpha_2 \leq \alpha_1$ and $a_2 = a_1 p = p$ for some $p \in \wp(a_2)\backslash\wp(k)$ [Lemma 13]. It follows that $P(X) = X^r(\phi_1)^{\alpha_1}(\phi_p)^{\alpha_2} = X^r(\phi_1)^{\alpha_1-\alpha_2}(\phi_1\phi_p)^{\alpha_2} = X^r(X-1)^{\alpha_1-\alpha_2}(X^p-1)^{\alpha_2}$, a contradiction because this is not a $G-$polynomial. Therefore, $\wp(a_2) = \wp(k)$. Since $\wp(a_2) \nsubseteq \wp(a_1)$ and $\frac{a_2}{a_1} = a_2$ is the product of prime elements of $\wp(a_2)\backslash\wp(a_1)$, then $\alpha_2 > \alpha_1$ [Lemma 25]. The converse is clear regarding Corollary 21. ■

5 Examples

We need the following list that consists of the first twenty cyclotomic polynomials.

$\phi_1 = X - 1$
$\phi_2 = X + 1$
$\phi_3 = X^2 + X + 1$
$\phi_4 = X^2 + 1$
$\phi_5 = X^4 + X^3 + X^2 + X + 1$
$\phi_6 = X^2 - X + 1$
$\phi_7 = X^6 + X^5 + \ldots + X^2 + X + 1$
$\phi_8 = X^4 + 1$
$\phi_9 = X^6 + X^3 + 1$
$\phi_{10} = X^4 - X^3 + X^2 - X + 1$
$\phi_{11} = X^{10} + X^9 + \ldots + X^2 + X + 1$
$\phi_{12} = X^4 - X^2 + 1$
$\phi_{13} = X^{12} + X^{11} + \ldots + X^2 + X + 1$
$\phi_{14} = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$
$\phi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$
$\phi_{16} = X^8 + 1$
$\phi_{17} = X^{16} + X^{15} + \ldots + X^2 + X + 1$
$\phi_{18} = X^6 - X^3 + 1$
$\phi_{19} = X^{18} + X^{17} + \ldots + X^2 + X + 1$

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

$$\phi_{20} = X^8 - X^6 + X^4 - X^2 + 1$$

Example 27 *Let* $P(X) = \phi_1\phi_4\phi_6 = (X-1)(X^2+1)(X^2-X+1) \in G[6]$.

It is well-known from [5] or [6] that, if p is a prime number, then
$\phi_m(X^p) = \phi_{pm}(X)$ if p divides m, and
$\phi_m(X^p) = \phi_{pm}(X)\phi_m(X)$ if p does not divide m.
With these facts recorded, one can check easily that

$$\begin{aligned}
P(X^2) &= (X^2-1)(X^4+1)(X^4-X^2+1) = \phi_1\phi_2\phi_8\phi_{12},\\
P(X^3) &= (X^3-1)(X^6+1)(X^6-X^3+1) = \phi_1\phi_3\phi_4\phi_{12}\phi_{18},\\
P(X^4) &= (X^4-1)(X^8+1)(X^8-X^4+1) = \phi_1\phi_2\phi_4\phi_{16}\phi_{24},\\
P(X^5) &= (X^5-1)(X^{10}+1)(X^{10}-X^5+1) = \phi_1\phi_4\phi_5\phi_6\phi_{30},\\
P(X^6) &= (X^6-1)(X^{12}+1)(X^{12}-X^6+1) = \phi_1\phi_2\phi_3\phi_6\phi_8\phi_{24}\phi_{36}.
\end{aligned}$$

Therefore, among all these polynomials, only $P(X^5)$ is divisible by $P(X)$. Hence, $P(X)$ is a $G-$polynomial. However, $P(X)$ does not satisfy the condition 3 of Theorem 19 since $\wp(4) \subseteq \wp(6)$, whereas $\wp(4) \nsubseteq \wp(1), \alpha_2 = \alpha_1 = 1$ and $\frac{a_2}{a_1} = 4 \in \wp(4)\backslash\wp(1) = \{4\}$.

Example 28 *Let* $P(X) \in G[4]$.

In view of the degrees of the first twenty cyclotomics, two cases may happen:

Case 1: $P(X) = X^r(\phi_{a_1})^{\alpha_1}$ and $\deg(P(X)) = r + \alpha_1\varphi(a_1) = 3$. From Corollary 11, we get

r	a_1	$\varphi(a_1)$	α_1	$P(X)$
0	2	1	3	$\phi_2^3 = (X+1)^3$
1	2	1	2	$X\phi_2^2 = X(X+1)^2$
1	4	2	1	$X\phi_4 = X(X^2+1)$
2	2	1	1	$X^2\phi_2 = X^2(X+1)$

Case 2: $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}$ and $\deg(P(X)) = r + \alpha_1\varphi(a_1) + \alpha_2\varphi(a_2) = 3$. From Theorem 26, we obtain

r	a_1	a_2	$\varphi(a_1)$	$\varphi(a_2)$	α_1	α_2	$P(X)$
0	1	2	1	1	1	2	$\phi_1\phi_2^2 = (X^2-1)(X+1)$
0	2	4	1	2	1	1	$\phi_2\phi_4 = (X+1)(X^2+1)$
0	2	6	1	2	1	1	$\phi_2\phi_6 = X^3+1$

Hence, $G[4]$ consists of the following $G-$polynomials:

$$(X^2-1)(X+1); (X+1)^3; (X+1)(X^2+1); X^3+1; X(X+1)^2;$$
$$X(X^2+1), X^2(X+1).$$

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

Example 29 *Let* $P(X) \in G[6]$.

According to the degrees of the first twenty cyclotomics, three cases have to be considered:

Case 1: $P(X) = X^r(\phi_{a_1})^{\alpha_1}$ and $\deg(P(X)) = r + \alpha_1\varphi(a_1) = 5$. From Corollary 11, we get

r	a_1	$\varphi(a_1)$	α_1	$P(X)$
1	6	2	2	$X\phi_6^2 = X(X^2 - X + 1)^2$
1	12	4	1	$X\phi_{12} = X(X^4 - X^2 + 1)$
3	6	2	1	$X^3\phi_6 = X^3(X^2 - X + 1)$

Case 2: $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}$ and $\deg(P(X)) = r + \alpha_1\varphi(a_1) + \alpha_2\varphi(a_2) = 5$. From Theorem 26, we obtain

r	a_1	a_2	$\varphi(a_1)$	$\varphi(a_2)$	α_1	α_2	$P(X)$
0	1	6	1	2	1	2	$\phi_1\phi_6^2 = (X-1)(X^2 - X + 1)^2$
0	2	3	1	2	1	2	$\phi_2\phi_3^2 = (X+1)(X^2 + X + 1)^2$
0	2	12	1	4	1	1	$\phi_2\phi_{12} = (X+1)(X^4 - X^2 + 1)$
1	3	4	2	2	1	1	$X\phi_3\phi_4 = X(X^2 + X + 1)(X^2 + 1)$
2	2	3	1	2	1	1	$X^2\phi_2\phi_3 = X^2(X+1)(X^2 + X + 1)^2$

Case 3: $P(X) = X^r(\phi_{a_1})^{\alpha_1}(\phi_{a_2})^{\alpha_2}(\phi_{a_3})^{\alpha_3}$ and $\deg(P(X)) = r + \alpha_1\varphi(a_1) + \alpha_2\varphi(a_2) + \alpha_3\varphi(a_3) = 5$.

If $\wp(a_3) \nsubseteq \wp(k) = \{2, 3\}$, then $a_3 = pa_1$ or $a_3 = pa_2$ for some prime $p \notin \wp(k)$. It results that $p \geq 5$ and $\varphi(a_3) \geq p - 1 \geq 4$. But this leads to the contradiction

$$\deg(P(X)) = r + \alpha_1\varphi(a_1) + \alpha_2\varphi(a_2) + \alpha_3\varphi(a_3) \geq 1 + 1 + 4 \geq 6.$$

We conclude that $\wp(a_3) \subseteq \wp(k) = \{2, 3\}$. By comparing $\varphi(a_3)$ to the degrees of the first twenty cyclotomics, we find that $1 \leq a_1 < a_2 < a_3 \leq 6$ and $r \in \{0, 1\}$. We deduce at least that $a_3 \in \{3, 4, 6\}$ and $\alpha_3 = 1$. Therefore, 3 subcases may occur:

Subcase 1: $a_3 = 3$. A fortiori $a_1 = 1$ and $a_2 = 2$. Thus, $P(X) = X^r(\phi_1)^{\alpha_1}(\phi_2)^{\alpha_2}\phi_3$. As $\wp(3) \nsubseteq \wp(1) \cup \wp(2)$, $\alpha_3 = \alpha_1 = 1$ and $\frac{a_3}{a_1} = 3 \in \wp(3)\backslash(\wp(1) \cup \wp(2)) = \{3\}$, then Lemma 25 ensures that $P(X)$ is not a $G-$polynomial.

Subcase 2: $a_3 = 4$.

$-$If $a_1 = 1$ and $a_2 = 2$, then $P(X) = X^r(\phi_1)^{\alpha_1}(\phi_2)^{\alpha_2}\phi_4$. By virtue of Proposition 10, $P(X)$ is not a $G-$polynomial because of $\wp(6) \nsubseteq \wp(1) \cup \wp(2) \cup \wp(3) = \{2\}$.

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

–If $a_1 = 1$ and $a_2 = 3$, then $P(X) = \phi_1\phi_3\phi_4$. As $\wp(4) \nsubseteq \wp(1) \cup \wp(3)$, $\alpha_3 = \alpha_1 = 1$ and $\frac{a_3}{a_1} = 4$ is a product of primes of $\wp(4)\backslash(\wp(1) \cup \wp(3)) = \{2\}$, then Lemma 25 enables us to conclude that $P(X)$ is not a $G-$polynomial.

Subcase 3: $a_3 = 6$.

–If $a_1 = 1$ and $a_2 = 2$, then $P(X) = X^r(\phi_1)^{\alpha_1}(\phi_2)^{\alpha_2}\phi_6$. As $\wp(6) \nsubseteq \wp(1) \cup \wp(2)$, $\alpha_3 = 1 \leq \alpha_2$ and $\frac{a_3}{a_2} = 3 \in \wp(6)\backslash(\wp(1) \cup \wp(2)) = \{3\}$, then $P(X)$ is not a $G-$polynomial by Lemma 25.

–If $a_1 = 1$ and $a_2 = 3$, then $P(X) = \phi_1\phi_3\phi_6$. As $\wp(6) \nsubseteq \wp(1) \cup \wp(3)$, $\alpha_3 = \alpha_1 = 1$ and $\frac{a_3}{a_2} = 2 \in \wp(6)\backslash(\wp(1) \cup \wp(3)) = \{2\}$, then $P(X)$ is not a $G-$polynomial by Lemma 25.

–If $a_1 = 1$ and $a_2 = 4$, then $P(X) = \phi_1\phi_4\phi_6$. We have already seen in Example 27 that $P(X)$ is a $G-$polynomial.

–If $a_1 = 2$ and $a_2 = 3$, then $P(X) = \phi_2\phi_3\phi_6$. As $\wp(6) = \wp(2) \cup \wp(3)$; $\wp(3) \nsubseteq \wp(2)$ and $\frac{a_2}{a_1} = 3/2$ is not the product of primes of $\wp(3)\backslash\wp(2)$, then $P(X)$ is a $G-$polynomial by Theorem 19.

–If $a_1 = 2$ and $a_2 = 4$, then $P(X) = \phi_2\phi_4\phi_6$. As $\wp(6) \nsubseteq \wp(2) \cup \wp(4)$, $\alpha_3 = \alpha_1 = 1$ and $\frac{a_3}{a_1} = 3 \in \wp(6)\backslash(\wp(2) \cup \wp(4)) = \{3\}$, then $P(X)$ is not a $G-$polynomial by Lemma 25.

Hence, $G[6]$ consists of the $G-$polynomials, namely:

$$X(X^2 - X + 1)^2; X(X^4 - X^2 + 1); X^3(X^2 - X + 1); (X - 1)(X^2 - X + 1)^2;$$
$$(X + 1)(X^2 + X + 1)^2; (X + 1)(X^4 - X^2 + 1); X(X^2 + X + 1)(X^2 + 1);$$
$$X^2(X + 1)(X^2 + X + 1)^2; (X - 1)(X^2 + 1)(X^2 - X + 1);$$
$$(X + 1)(X^2 + X + 1)(X^2 - X + 1).$$

I close this paper by stating some conjectures.

Conjecture 30 *Find a complete characterization of a $G-$polynomial of degree $k - 1$ for every $k \geq 3$.*

Conjecture 31 *Find an effective algorithm to determine all the elements of $G[k]$ for every $k \geq 3$.*

Acknowledgement: Thanks are due to the anonymous referee for his/her very valuable and helpful advice, corrections and remarks.

References

[1] D.Caragea, V. Ene, Problems10802, Amer. Math. Monthly 107 (2000), 462.

[2] A. Ayache, O. Echi and M. Naimi, On Kronecker polynomials, Rocky. Mountain. J. Math., 41 (2011), No. 3, 1 – 19.

[3] M. Ayad, O. Kihel, J. Larone, When does a given polynomial with integer coefficients divide another? Amer. Math. Monthly 123 (2) (2016), 376.

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.

[4] P. A. Damianou, Monic polynomials in Z[X] with roots in the unit disc. Amer. Math. Monthly, 108 (2001), No. 63, 253 – 257.

[5] Y. Ge, Elementary Properties of Cyclotomic Polynomials, http://www.yiming-ge.com/doc/cyclotomic polynomials. pdf.

[6] Yves Gallot, Cyclotomic Polynomials and Prime Numbers, http://perso.orange.fr/yves.gallot/papers/cyclotomic.pdf

[7] L. Kronecker, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, Crell, Oeuvres I (1857), 105-108.

[8] J. H. Nieto, On the divisibility of polynomials with integer cofficients, Divulg. Mat. 11 (2003), 149-152.

10 Jan 2023 22:13:53 PST
220806-Ayache Version 2 - Submitted to Rocky Mountain J. Math.