WWJMRD 2021; 7(7): 75-77
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
Impact Factor SJIF 2017: 5.182 2018: 5.51, (ISI) 2020-2021: 1.361
E-ISSN: 2454-6615
DOI: 10.17605/OSF.IO/WZBY5

Kwame Owusu Bempah
Department of Mathematics Education Akenten Appiah-Menkah University of Skills Training and Entrepreneural Development, Kumasi, Ghana

Kwasi Baah Gyamfi
Department of Mathematics Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

On the Concept of Cyclotomic Polynomials in Galois Fields

Kwame Owusu Bempah, Kwasi Baah Gyamfi

Abstract
Galois Theory brings about the connections and relations between groups and Field theory. It also relates polynomials, Field and groups. In this paper, we concentrate solely on the overview and construction of cyclotomic polynomials over a field.

Keywords: Field, Polynomials, Cyclotomic Polynomial

Introduction
Finding the roots of polynomials have been in existence for so many years and with the use of the quadratic formular, the roots of polynomials of degree 2 can be determined with ease. Cardan, Taraglia and Dal Ferro formulated a rule to be used in solving polynomials of degree 3 in the sixteenth century. A great mathematician called Ferrari also formulated and deduced an algorithm to be used for finding the roots of both polynomials of degree 2 and degree 3. Evariste Galois, a renowned mathematician in the nineteenth century played a major role in the area of abstract algebra which we can ultimately say the founder and brought about a connection between group and field theory. Galois became renowned at the age of 20 after producing his first work. The output of Galois results were seen and noted and has become the bedrock for many algebraic developments. An aspect of Galois field called cyclotomic polynomials is a subject of this thesis work.

Preliminaries
This section discusses the concept of Field and Cyclotomic polynomials by looking at some Definitions, Lemma, Theorems and examples which will assist us to grasp the concept of cyclotomic polynomial in Galois fields.

Definition 2.1 A Field is called prime if it has no proper subfield.
Lemma 2.1 Let F be a Finite Field containing a subfield T with r elements. Then F has r^m elements where $[F: T] = m$.

Proof: Let F be a vector space over T .Because F is finite, then it is finite dimensional as a vector space over k. Now if $[F : T] = m$, then we can say there is a basis of F over T which contains or consist of m elements denoting as say $b_1, b_2, \ldots. b_m$. So every element of F can be ≠written in the form $a_1b_1 + a_2b_2 + \ldots\ldots a_mb_m$, where $a_1, a_2, \ldots\ldots a_m \in T$. Since a_i can have r values, then F can have exactly r^m elements.

Theorem 2.2 Let $m \geq 2$ be a prime, then the mth. Cyclotomic polynomial denoted by φ_m is given by
$$\phi_m(x) = \frac{x^p - 1}{x - 1} - = C_1x^{p-1} + C_2x^{p-2} + \ldots . C_{n-1}x + C_n$$
Where $C_1, C_2, \ldots\ldots C_n$ are all unity.

Theorem 2.3 Let F be a Finte Field with q elements, then every $a \in F$ satisfies $a^q = a$

Correspondence:
Kwame Owusu Bempah
Department of Mathematics Education Akenten Appiah-Menkah University of Skills Training and Entrepreneural Development, Kumasi, Ghana

Proof: For the identity $a^q = a$ is very trivial for $a = 0$ but from other perspective, the non-zero elements of F form a group of order $q - 1$ in multiplication.
Therefore $a^{q-1} = 1$ for all $a \in F$ where $a \neq 0$ and multiplication by a produces the outcome.

Example 2.4
Considering F_5 with 5 as prime, the elements of $F^*_5 = \{1, 2, 3, 4\}$. This implies,
$3^5 = 243 = 3$ and also $3^{5-1} = 3^4 = 1$

Main Result
In this section, we will be discussing and determining Cyclotomic Polynomials over a Field.
Example: We are going to determine the following cyclotomic polynomials $\varphi_m(x)$ where m represent the degree of the polynomial used

- $\varphi_2(x)$ where 2 is the degree of the polynomial to use;
- $\varphi_3(x)$ where 3 is the degree of the polynomial to use;
- $\varphi_4(x)$ where 4 is the degree of the polynomial to use;
- $\varphi_5(5)$ where 5 is the degree of the polynomial to use;

1. for $\varphi_2(x)$, the degree of the polynomial to use is 2 which is given as
$f(x) = x^2 - 1$
and the field is F_2 where $F_2 = \{0, 1\}$ and $F^*_2 = \{1\}$
This means, the degree of the polynomial used will represent the field and F^* means exclusion of the zero element in the field. Using

$$C_k = e^{\frac{2\pi ik}{n}} = w = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$$

Where n = the degree of the polynomial used
k = elements within the field F^*. This implies that
$k = 1$. Now when k=1, we have

$$C_1 = w = \cos\frac{2\pi}{2} + i\sin\frac{2\pi}{2} = \cos 180 + i\sin 180 = -1$$

So we have $C_1 = w = -1$
Therefore,
$\varphi_2(x) = (x - (C_1)) = (x - (-1)) = x + 1$

2. Also for $\varphi_3(x)$, the degree of the polynomial to use is 3 and it is represented as
$f(x) = x^3 - 1$

This also implies that, the Field is F_3 and $F^*_3 = \{1,2\}$when k= 1, we have
Hence,

$$C_1 = w = \cos\frac{2\pi(1)}{3} + i\sin\frac{2\pi(1)}{3} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$$

$$C_1 = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$$

Also when k=2, we produce;

$$C_2 = w = \cos\frac{2\pi(2)}{3} + i\sin\frac{2\pi(2)}{3} = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$$

Hence,

$$C_2 = \frac{-1}{2} - \frac{\sqrt{3}}{2}i$$

Hence, $C_1 = w$ and $C_2 = w_2$. Therefore;
$\varphi_3(x) = (x - (C_1))\,(x - (C_2))$
Substituting the values of C_1 and C_2 produces;

$$\left[x - (\frac{-1}{2} + \frac{\sqrt{3}}{2}i)\right]\left[x - (\frac{-1}{2} + \frac{\sqrt{3}}{2}i)\right]$$

Expanding produces;
$\varphi_3(x) = x^2 + x + 1$

3. Considering φ_4(x) and taking the polynomial to be used with degree 4 as,
$f(x) = x^4 - 1$
This also means, the field is F_4 and $F^*_4 = \{1, 2, 3\}$. Now when k=1, we have

$$C_1 = w = \cos\frac{2\pi(1)}{4} + i\sin\frac{2\pi(1)}{4} = \cos\frac{2\pi}{4} + i\sin\frac{2\pi}{4}$$

Hence,

$$C_1 = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = \cos 90 + i\sin 90 = i$$

Also for k=2, we get

$$C_2 = w = \cos\frac{2\pi(2)}{4} + i\sin\frac{2\pi(2)}{4} = \cos\frac{2\pi}{4} + i\sin\frac{2\pi}{4}$$

Hence,
$C_2 = \cos\pi + i\sin\pi = \cos 180 + i\sin 180 = -1$
Considering k=3 also produces

$$C_3 = w = \cos\frac{2\pi(3)}{4} + i\sin\frac{2\pi(3)}{4} = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}$$

Hence,
$C_3 = \cos 270 + i\sin 270 = -i$
Therefore,
$\varphi_4(x) = (x - C_1)\,(x - C_3)$. Substituting C_1 and C_3 gives
$(x - i)(x + i)$
$\varphi_4(x) = x^2 + 1$

4. Also for $\varphi_5(x)$, the Field is F_5 and $F^*_5 = \{1, 2, 3, 4\}$ and the polynomial to be used is
$f(x) = x^5 - 1$

Since the degree of the polynomial is prime, then using Theorem 2.2 can bring out the Cyclotomic polynomial with ease; which is

$$\phi_m(x) = \frac{x^p - 1}{x - 1} - = C_1x^{p-1} + C_2x^{p-2} + ...C_{n-1}x + C_n$$

Where m is the fifth Cyclotomic, $p = 5$ is the degree of the polynomial used and C_1........C_n are all constants which are unity.
We then substitute and produces the results

$$\phi_5(x) = \frac{x^5 - 1}{x - 1} - = C_1x^{5-1} + C_2x^{5-2} + C_3x^{5-3} + C_4x^{5-4} + C_2x$$

We then have,

$$\phi_5(x) = \frac{x^5 - 1}{x - 1} = C_1x^4 + C_2x^3 + C_3x^2 + C_4x + C_5x^0$$

$$\phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

Conclusion
We have been discussing and constructing cyclotomic polynomials and detected that when p is prime, the cyclotomic polynomial can be gotten using $\varphi_m(x) = C_1x^{p-1}+C_2x^{p-2}+C_nx^{p-n}+.....C_{n-1}x+C_n$ where the coefficients are all unity and when p is even thus composite, the cyclotomic polynomial can also be constructed using $C_k = e^{\frac{2\pi ik}{n}} = w = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$

Recommendation
Studies have shown that prime numbers have a general rule for determining cyclotomic polynomials over a field whiles composite numbers also have a general trend in

determining cyclotomic polynomials. We therefore recommend that researchers finds out a general rule for the $\varphi_m(x)$ used; which can be applied to both prime and composite numbers in constructing Cyclotomic Polynomials

References

1. Allan Clark. Elements of abstract algebra. Courier Corporation, 1984
2. Grillet, Pierre Antoine: Abstract Algebra, GTM 242, Springer, 2006.
3. Rotman, Joseph: Galois Theory, Springer 1998.
4. R Cantor and M wilson. Constructive galois theory, 2000
5. Rudolf Lidl and Harald Niederreiter. Introduction to finite fields and their applications. Cambridge university press, 1994.