PEOPLE's DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Mohamed Boudiaf university of M'sila
Faculty of Mathematics and computer sciences
Departement of Mathematics

Master memory

Field : mathematics and computer sciences
Branch : Mathematics
Option : Algebra and Discrete mathematics

Theme

Cyclotomic Polynomials and Some Application

Presented by :
OUALID Farida

The jury composed of :

AMROUNE Abdelaziz	Prof,	University of M'sila	**President**.
LADJELAT Lahcene	MAA,	University of M'sila	**Supervisor.**
HEBOUB Lakhdar	MAA,	University of M'sila	**Examiner.**

University year 2019/2020

Depatement of Mathematics And Informatic
Depatement of Mathematics
specialite discrete mathematics

Memoir about:

Cyclotomic Polynomials and Some Applications

Denoted by:
OUALID Farida

Dricted by:
LADJELAT Lahcene

University year :2019-2020

Dedication

To my loved ones To the one who put me on the path of life, nurtured me, taught me, fought for me and made me feel precious, and most important loved me unconditionally. My mother To the cheerful soul and my cheerleaer. My phother wishing you a long life. To my siblings, those who have always been there for me to get through the obstacles in my life. I dedicate my dissertation to you.

Acknowledgements

Thanks and appreciation Thanks to God Almighty, who has enabled us to complete this thesis. I give sincere thanks and appreciation to my distinguished professor Dr. ***Ladjelat Lahcene****. I also express my gratitude and appreciation to the respected and respectable discussion committee.*

Contents

Introduction

Cyclotomic polynomials are a necessary and important type of polynomial that appears frequently throughout algebra. They are of particular importance because for any positive integer n, the irreducible factors of $x^n - 1$ over the rationals and integers are cyclotomic polynomials. Moreover, the minimal polynomial of any n^{th} root of unity over the rationals is a cyclotomic polynomial. Records indicate that certain cyclotomic polynomials were studied as early as Euler, but perhaps their most famous use is due to Gauss.

We will start off by developing some concepts behind where the cyclotomic polynomials come from, we take a look at the n^{th} root of unity, then we move on definition the polynomials themselves; first looking at general properties such as their degree and how they relate to each other. The next section we will prove that the cyclotomic polynomial are irreducible over the integers. After that we will explore the relationship between cyclotomic polynomial and prime numbers. After that we will apply some applications to cyclotomic polynomials and how they can be used in different proofs. We focus on two main results; Wedderburn's Theorem, and Dirichlet's Theorem.

Chapter 1

The Concept of The Field Theory

1.1 Generalities about Ring

In this section, we will give definition for each one of the following vocabularies: group, ring, morphism ring, field and extension field, finite field and minimal polynomial.

1.1.1 Group

Definition 1.1.1 *(Group). A group is a set G, together with a binary operation "$*$", such that the following axioms hold:*

1. ***Closure:*** *G is closed under the operation "$*$": $x, y \in G \Rightarrow x * y \in G$.*
2. ***Associativity:*** *$(x * y) * z = x * (y * z)$ for all $x, y, z \in G$.*
3. ***Identity:*** *there exists an element $e \in G$ (called the identity of G) such that $x * e = e * x = x$ for all $x \in G$.*
4. ***Inverses:*** *for every element $x \in G$ there exists an element $x^{-1} \in G$ (called the inverse of x) such that : $x * x^{-1} = x^{-1} * x = e$.*

Definition 1.1.2 *(Abelian group). Let G be a group with respect to "$*$". Then G is called an abelian group, or commutative group, i.e., $x * y = y * x$ for all $x \in G$.*

Example 1.1.1 *$(\mathbb{Z}, +)$, $(\mathbb{R}^*, \times)$ are groups abelian.*

1.1.2 Ring

Definition 1.1.3 *(Ring). A ring $(R, +, *)$ is a set R, together with two binary operations "$+$" and "$*$" on R satisfying the following axioms:*

- *$(R, +)$ is an abelian group .*
- *associativity of multiplication, i.e., $(x * y) * z = x * (y * z)$ for all $x, y, z \in R$.*
- *existence of multiplicative identity $1 \in R, i.e., x * 1 = 1 * x = x$ for all $x \in R$.*
- *two distributive laws hold in $R, i.e., x * (y + z) = x * y + x * z$ for all $x, y, z \in R$.*

Definition 1.1.4 *Let $(R,+,*)$ a ring, and B a part of R, we say that B is a subring of R if:*

- *B is stable by "$+$" and "$*$".*
- *$1_R \in B$ for all $x \in B$, $(-x) \in B$.*

Remark 1.1.1
- *Typically, we use 0 to denote the identity element of the abelian group R with respect to the addition and $(-x)$ to denote the additive inverse of $x \in R$.*
- *If the low "$*$" is commutative, i.e.,$x*y = y*x$ for all $x, y \in R$, we say that the ring is commutative.*
- *if the low "$*$" posses a neutral element, we say that the ring is unitary and we denoted by "1" .*

Example 1.1.2
1. *$(\mathbb{Z},+,\times),(\mathbb{Q},+,\times),(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ are commutative ring with identity*
2. *$(\mathbb{R}^n,+,\times)$ is commutative ring for the following internal law :*

$$(x_1,...,x_n)+(y_1,...,y_n) = (x_1+y_1,...,x_n+y_n)$$
$$(x_1,...x_n).(y_1,...y_n) = (x_1.y_1,...x_n.y_n).$$

Notation 1.1.1 *Let R a ring, denote R^* the set invertible element of R.*

Proposition 1.1.1 *If $(R,+,\times)$ is a ring, then $(R^*,\times)$ is a group is called a group of units of R.*

Definition 1.1.5 *An integral ring is ring satisfying to $x*y = 0 \Rightarrow x = 0$ or $y = 0$ for all $x, y \in R$.*

1.1.3 Morphism of Ring

Definition 1.1.6 *[15] Let $(R,+,\cdot)$ and $(S,\oplus,\otimes)$ be two rings, the map $f : R \longrightarrow S$ is called a ring morphism if for all $x, y \in R$:*

- $f(x+y) = f(x) \oplus f(y)$.
- $f(x \cdot y) = f(x) \otimes f(y)$.
- $f(1_R) = 1_S$.

A ring isomorphism is a bijective ring morphism, we say that R and S are isomorphic rings, and we write $R \cong S$.

1.2 Generalities about Field

1.2.1 Field

Definition 1.2.1 *A set F with two internal composition laws "$+$" and "$\times$" we say that $(F,+,\times)$ is a field if :*

- *$(F,+,\times)$ is a commutative ring.*
- *$0_F = 1_F$ (everything contains 1 and 0).*
- *every element of $F\backslash\{0\}$ admits an inverse for the product in F.*

Example 1.2.1 *1.* $(\mathbb{Z}/n\mathbb{Z},+,\times)$ *is a field if and only if n is prime.*

Definition 1.2.2 *Let* $(F,+,\times)$ *be a field and h part of F we say that h is a subfield of F if :*

- *h is stable of* $+$ *and* $\times$.
- *for all* $x \in h$, $(-x) \in h$ *and for all* $x \in h\backslash\{0\}$, $x^{-1} \in h$.
- $1_F \in h$.

Example 1.2.2 *1.* $\mathbb{R}$ *is a subfield of* $(\mathbb{C},+,\times)$.

2. $\mathbb{Q}$ *is a subfield of* $\mathbb{R}$.

1.2.2 Extension Fields

Definition 1.2.3 *If E is a field containing F as a subfield, then E is called an extension field of F.*

Theorem 1.2.1 *(Kronecker). if F is a field and* $f(x) \in F[x]$ *is a nonconstant polynomial, then there exist an extension field E of F and an* $\alpha \in E$ *with* $f(\alpha) = 0$.

Proof. If the degree of f is 1, then $f(x)$ is linear and we can choose $E = F$.
If the degree of f is greater than 1, write $f(x) = p(x)g(x)$, where $p(x)$ is irreducible.
The quotient ring $E = F[x]/ < p(x) >$ is a field. The natural map:

$$\varphi(a) : E \longmapsto F$$

defined by $\varphi(a) = a + < p(x) >$, is an isomorphism from F to the subfield $F' = \{a + < p(x) > : a \in F\}$ of E.
put $\alpha = x + < p(x) > \in E$. Let $p(x) = a_0 + a_1x + ... + a_{d-1}x^{d-1} + x^d$, where $a_i \in F$ for all i.
In $E = F[x]/ < p(x) >$, we have :

$$\begin{aligned} p(\alpha) &= (a_0 + < p(x) >) + (a_1 + < p(x) >)\alpha + ... + (1 + < p(x) >)\alpha^d \\ &= (a_0 + < p(x) >) + (a_1 + < p(x) >)(x + < p(x) >) + ... + (1 + < p(x) >)(x + < p(x) >)^d \\ &= (a_0 + < p(x) >) + (a_1x + < p(x) >) + ... + (1x^d + < p(x) >) \\ &= a_0 + a_1x + ... + x^d + < p(x) > \\ &= p(x) + < p(x) > = < p(x) > . \end{aligned}$$

,
because $p(x) \in < p(x) >$. But $< p(x) > = 0 + < p(x) >$ is the zero element of $E = F[x]/ < p(x) >$, and so α is a root of $p(x)$. ■

Example 1.2.3 *The polynomial* $x^2 + 1 \in \mathbb{R}[x]$ *is irreducible, and so* $K = \mathbb{R}[x]/ < x^2 + 1 >$ *is a field extension. If* α *is a root of* $x^2 + 1$*, then* $\alpha^2 = -1$*; moreover, every element of K has a unique expression of the form* $a + ba$*, where* $a, b \in \mathbb{R}$*. Clearly, this is another construction of* $\mathbb{C}$.

Definition 1.2.4 *field containing no proper subfields is called a prime field.*
For example, F_p *is a prime field, since any subfield must contain the elements* 0 *and* 1*, and since it is closed under addition it must contain all other elements, i.e. it must be the whole field.*

Remark 1.2.1 *The intersection of all subfields of a field F is itself a field, called the prime subfield of F.*

Proposition 1.2.1 *If* $K \subset L \subset H$ *are extension fields we have:*

$$[H : K] = [H : L][L : K].$$

Proof. We assume the finite dimension, if not the proposition is trivial. Let $(e_1,...,e_n)$ a bas of L on K, and $(f_1,...,f_p)$ a bas of H on L. We will show that the $(e_i f_j)(1 \leq i \leq n, 1 \leq j \leq p)$ form a bottom of H on K, which will mount the proposition.
These element are generators because if $x \in H$, we can write $x = \sum_{j=1}^{p} \lambda_j f_j$ with $\lambda_j \in L$
each λ_j can in turn develop on the botton $(e_i) : \lambda_j = \sum_1^n \lambda_{ij} e_i$ with $\lambda_{ij} \in K$ we then get :

$$\sum \lambda_{ij} e_i f_j$$

We also show who $e_i f_j$ form a free family : if we have a linear relation

$$\sum \lambda_{ij} e_i f_j = 0$$

we can write

$$\sum_{j=1}^{p} f_j (\sum_{i=1}^{n} \lambda_{ij} e_i) = 0$$

which implies $\sum_{i=1}^{n} \lambda_{ij} e_i = 0$ for everything j since the f_j are independent, then $\lambda_{ij} = 0$ since the e_i are independent. ■

1.2.3 Simple Extension

Definition 1.2.5 *Let E be an extension field of F and let $\alpha \in E$. The smallest subfield of E containing both F and α is called the simple extension of F and is denoted by $F(\alpha)$.*

If α is algebraic over F, then $F(\alpha) = \varphi_\alpha[F[x]]$. If α is transcendental over F, then $F(\alpha)$ is the quotient field of $\varphi_\alpha[F[x]]$.

Theorem 1.2.2 *Let E be an extension field of F and let $\alpha \in E$ be algebraic over F. Let $n = deg(\alpha, F)$. Then*

$$F(\alpha) = \{\alpha_0 + ...\alpha_{n-1}\alpha^{n-1} : \alpha_0, ..., \alpha_{n-1} \in F\}.$$

Example 1.2.4 *Let $F = \mathbb{Z}_2$, let $p(x) = x^2 + x + 1$, then $\mathbb{Z}_2(\alpha)$ is simple extension field of $\mathbb{Z}_2$ containing a zero α of $p(x)$. Then*

$$\mathbb{Z}_2(\alpha) = \{a_0 + a_1\alpha : a_0, a_1 \in \mathbb{Z}_2\}.$$

1.2.4 Finite Extensions

Definition 1.2.6 *Let E be an extension field of F. E is called an algebraic extension of F if every element of E is algebraic over F.*

Definition 1.2.7 *Let E be an extension field of F. E is called a finite extension of F if E is of finite dimension n as a vector space over F. We denote $[E : F] = n$.*

Theorem 1.2.3 *If E is a finite extension field of F, then E is an algebraic extension of F.*

1.2.5 Finite Field

Definition 1.2.8 *a finite field is a field which has a finite element number, we denote a finite field of order q par $\mathbb{F}_q$ (Field of order q) or $GF(q)$ (Galois field of order q). A finite field is of prime characteristic.*

Example 1.2.5
- $(\mathbb{Z}/n\mathbb{Z},+,\times)$ *is a field if and only if n is prime*
- *p prime* $\mathbb{Z}/p\mathbb{Z}$ *is a finite field*

Theorem 1.2.4 *Let* $n,m \in \mathbb{N}$*, p prime.*

$$m \mid n \Leftrightarrow \mathbb{F}_p^m \subset \mathbb{F}_p^n.$$

Proof.

- $\Rightarrow$ Suppose that $m \mid n,\ n = \alpha.m$
  We have:
  $X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + ... + X + 1)$
  $X - 1 \mid x^n - 1$.....$(*)$
  $m \mid n \Rightarrow p^m - 1 \mid p^n - 1$
  We have according $(*)$

  $$X - 1 \mid X^\alpha - 1.....(1)$$

  then $X = p^m$
  $p^m - 1 \mid (p^m)^\alpha - 1 = p^{m\alpha} - 1 = p^n - 1$
  Then
  $$X^{p^m-1} - 1 \mid X^{p^n-1} - 1,\ \textit{resulting of}$$
  $m \mid n \Rightarrow y^m - 1 \mid y^n - 1\ (X = y^n\ in(1))$
  $X^{p^m-1} - 1/X^{p^n-1} - 1$, at multiplying by X
  We deduce $X^{p^m} - X \mid X^{p^n} - X$
  { The roots of $X^{p^m} - X$}$\subset$ {The roots of $X^{p^n} - X$}
  $\{x \in F : x^{p^n} - x\} \subset \{x \in F : x^{p^n} - x = 0\}$
  Then $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$
- $\Leftarrow$ Suppose that $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$
  Let $\mathbb{F}_p \subset \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$
  We have $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \times [\mathbb{F}_{p^m} : \mathbb{F}_p]$
  $n = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}].m$
  Then $m \mid n$. ■

Proposition 1.2.2 *Let F a field of finite characteristic p*

1. $Car(F) = p$ *is prime.*
2. *If* $n.1 = 0$*, then* $p \mid n$.

Proof

1. since $Car(F) = p$ is finite $\Rightarrow p \neq 0$
   suppose that $p = a.b;\quad 1 < a < p,\ 1 < b < p.$
   $p.1 = (a.b).1 = (a.1).(b.1)$
   $0 = (a.1).(b.1)$
   $\Rightarrow a.1 = 0$ or $b.1 = 0$
   whitch contradicts the minimality of p hance the asseration 1

2. Let $n \in \mathbb{N}^*$, $n.1 = 0$
   doing the "÷" Euclidean of n on p $(n \geq p)$
   $n = q.p + r$, $0 \leq r < p$
   $n.1 = 0 \Leftrightarrow (p.q + r).1 = 0$
   $\Leftrightarrow (p.q).1 + r.1 = 0$
   $\Leftrightarrow (p.1).(q.1) + r.1 = 0$
   $\Leftrightarrow 0.(q.1) + r.1$
   $\Leftrightarrow r.1 = 0$

Then $r = 0$, i,e; $n = q \cdot p$. ■

Proposition 1.2.3 *Let F a field of finite characteristic p for $a, b \in F$ and $i \in \mathbb{N}$, we have*

$$(a+b)^{p^i} = a^{p^i} + b^{p^i}$$

Theorem 1.2.5 *If F is a finite field , then $|F| = p^n$, with $p = Car(F)$ prime and $n = [F : \mathbb{Z}/p\mathbb{Z}]$.*

He does not exist a finite field to 10 elements.

Theorem 1.2.6 *If F is a finite field order $q = |F|$ then, for all $\alpha \in F$,*

$$\alpha^q = \alpha.$$

Definition 1.2.9 *If F is a field, then F^* will denote the multiplicative group of all nonzero elements of F. Let us recall some facts about finite fields that have already been established.*

1.3 polynomial

1.3.1 Function Polynomial

Definition 1.3.1 *Let $S = a_0 + a_1X + ... + a_nX^n$ a polynomial of $\mathbb{K}[X]$ we say that function polynomial associated with: S the application $S : \mathbb{K} \longrightarrow \mathbb{K}$ which has all x of K matches the element $S(x) = a_0 + a_1x + ...a_nx^n of\ \mathbb{K}$.*

1.3.2 Irreducible Polynomial

Definition 1.3.2 *A polynomial $p \in K[x]$ is said to be irreducible if it is not invertible and If its only dividers are the associated element and the invertible element.*

Example 1.3.1 *Any polynomial of degree 1 is irreducible.*

1.3.3 The Minimal Polynomial

Definition 1.3.3 *[1] Let $F < E$. An element $\alpha \in E$ is said to be **algebraic** over F if α is a root of some polynomial over F. An element that is not algebraic over F is said to be **transcendental** over F.*

If α is algebraic over F, the set of all polynomials satisfied by α

$$I_\alpha = \{g(x) \in F[x] \mid g(\alpha) = 0\}$$

*is a nonzero ideal in $F[x]$ and is therefore generated by a unique monic polynomial $p(x)$, called the **minimal polynomial** of α over F and denoted by $p_\alpha(x)$, $p_{\alpha,F}(x)$ or $min(\alpha, F)$. The following theorem characterizes minimal polynomials in a variety of useful ways. Proof is left to the reader.*

Theorem 1.3.1 *[1] Let $F < E$ and let $\alpha \in E$ be algebraic over F. Then among all polynomials in $F[x]$, the polynomial $min(\alpha, F)$ is*

1. *the unique monic irreducible polynomial $p(x)$ for which $p(a) = 0$.*
2. *the unique monic polynomial $p(x)$ of smallest degree for which $p(\alpha) = 0$.*
3. *the unique monic polynomial $p(x)$ with the property that $f(\alpha) = 0$ if and only if $p(x)|f(x)$. In other words, $min(\alpha, F)$ is the unique monic generator of the ideal I_α.*

Definition 1.3.4 *[1] Let $F < E$. Then $\alpha, \beta \in E$, are said to be **conjugate** over F if they have the same minimal polynomial over F.*

Chapter 2

Cyclotomic Polynomials

2.1 Finite Fields I: Basic Properties

Finite Fields Redux

Let F is a field, then denote F^* the multiplicative group of all nonzero elements of F, Let is talk about finite field.

Theorem 2.1.1 *If F is a finite field and $[E:F]=d$ then $|E|=|F|^d$.*

Proof. If $\{\alpha_1,...,\alpha_d\}$ is a basis for E over F, then each element of E has a unique representation of the form $\alpha_1\alpha_1+...+\alpha_d\alpha_d$, where $\alpha_i\in F$. Since there are $|F|$ possibilities for each coefficient α_i, we deduce that $|E|=|F|^d$. ■

2.2 Finite Fields as Splitting Fields

Definition 2.2.1 *A splitting field for $\mathscr{F}$ it is an extension field E of F of the following properties:*

1. *For all $f_i(x)\in\mathscr{F}$ splits over E, and from it owns a full set of $deg(f_i)$ root in E.*
2. *The extension field E is the smallest field satisfying $F<K<E$ that contains the roots of each $f_i(x)\in E$.*

Remark 2.2.1 *(a) Let $\mathscr{F}=\{f_i(x)\mid i\in I\}$ be family of polynomials over a field F.*

(b) If a polynomial $f(x)\in F[x]$ factors into linear factors

$$f(x)=a(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$$

in an extension field E, that is, if $\alpha_1,\alpha_2,...\alpha_n\in E$, we say that $f(x)$ splits in E.

Let F be a finite field of size q. Then F^* has order $q-1$ and so every element $\alpha\in F^*$ has exponent $q-1$, that is, $\alpha^{q-1}=1$. It follows that every element of F is a root of the polynomial

$$f_q(x)=x^q-x$$

this polynomial has no multiple roots because $f_q'(x)=-1$ and the field F is the set of roots of $f_q(x)$ in some splitting field. In other words

$$F=Roots(f_q(x))=Split_{\mathbb{Z}_p}(f_q(x)).$$

Existence

As each that every finite field of characteristic p has $q = p^n$ elements for some $n > 0$. On the contrary, let $q = p^n$. If R is the set of roots of $f_q(x)$. Then R is indeed a field. For if $\alpha, \beta \in R$, then $\alpha^q = \alpha$ and $\beta^q = \beta$, whence

$$(\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta$$

and

$$(\alpha\beta^{-1})^q = \alpha^q(\beta^q)^{-1} = \alpha\beta^{-1}.$$

Then $\alpha\beta, \alpha\beta^{-1} \in R$. And therefore R is a field and hence a splitting field for $f_q(x)$. Since $f_q(x)$ do not have multiple roots, R has size q. Then, for every prime power $q = p^n$, there is a field of size q.

Corollary 2.2.1 *The extension $GF(q) < GF(q^n)$ is a finite Galois extension. Hence, in the Galois correspondence for $GF(q) < GF(q^n)$, all intermediate fields and all subgroups are closed.*

Remark 2.2.2 *Each finite field of size q is a splitting field for $f_q(x)$ over $\mathbb{Z}_p$ and all such fields are isomorphic.*
We symbolize a finite field of size q by F_q or $GF(q)$(Since the symbol represent for Galois Field.)

2.3 The Subfields of a Finite Field

In this is section we wish to examine the subfields of a finite field $GF(q^n)$. Note that if K and n are positive integers and $n = mk + r$ for $0 \leq r < k$, then

$$x^{mk+r} - 1 = (x^k - 1)x^{(m-1)k+r} + (x^{(m-1)k+r} - 1).$$

And from it $x^k - 1$ divides $x^{mk+r} - 1$ if only if $x^k - 1$ divides $x^{(m-1)k+r} - 1$.
And repeatedly we get $x^k - 1$ divides $x^{mk+r} - 1$ if and only if $x^k - 1$ divides $x^r - 1$, that is , if and only if $r = 0$. In symbols,

$$k \mid n \Leftrightarrow x^k - 1 \mid x^n - 1$$

over the prime subfield $\mathbb{Z}_p$.

Theorem 2.3.1 *The following are equivalent:*

1. $d \mid n$.
2. $f_{d^q}(x) \mid f_{d^q}(x)$, *this means The defining polynomial of $GF(q^d)$ divides the defining polynomial of $GF(q^n)$.*
3. $GF(q^d) < GF(q^n)$.

- $\lambda_n = \{d \mid \ 1 \leq d \leq n, d \text{ divides } n\}$, *under division.*
- $\{f_{q^d}(x) \mid f_{q^d}(x) \text{ divides } f_{q^n}(x)\}$, *under division.*
- *Subfields of $GF(q^n)$, under set inclusion.*

2.4 The Multiplicative Structure of a Finite Field

Definition 2.4.1 *Any element of $GF(q)$ that generates the cyclic group $GF(q)^*$ is called a **group primitive element** of $GF(q)$. In contrast, if $F < E$, then any element $\alpha \in E$ for which $E = F(\alpha)$ is called a **field primitive element** of E over F.*

Roots in a Finite Field

If $\beta \in GF(q)$, and when you are the equation $x^k = \beta$,then β has a kth root in $GF(q)$.

Theorem 2.4.1 *1. Let α be a group primitive element of $GF(q)$. Then α^i has a kth root in $GF(q)$ if and only if*

$$\gcd = (k, q-1) \mid i$$

2. Each element of $GF(q)$ he have a kth root if and only if k and $q-1$ are relatively prime, then each element has a unique kth root.

2.5 The Galois Group of a Finite Field

Since the extension $GF(q) < GF(q^n)$ is Galois, if G is the Galois group of $GF(q^n)$ over $GF(q)$ then

$$|G| = [GF(q^n) : GF(q)] = n.$$

Theorem 2.5.1 *The Galois group G of $GF(q^n)$ over $GF(q)$ is cyclic of order n , generated by the* ***Frobenius automorphism***

$$\sigma_q : \alpha \longmapsto \alpha^q.$$

Proof. If $\alpha \in GF(q)$, then $\sigma_q \alpha = \alpha^q = \alpha$ and so σ_q fixe $GF(q)$ and is therefore in the Galois group G. Moreover, the n automorphisms

$$\iota, \sigma_q, \sigma_q^2, ..., \sigma_q^{n-1}$$

are distinct elements of G, for if $\sigma_q^k = \iota$ then $\alpha^{q^k} = \alpha$ for all $\alpha \in GF(q^n)$ and so $GF(q^n) < GF(q^k)$, which implies that $k \geq n$. Finally, since $|G| = n$, note this $G =< \sigma_q >$. ■

2.6 Irreducible Polynomials over Finite Fields

Of the most remarkable properties of finite fields every finite field $GF(q)$ is not only the splitting field for the polynomial $f_q(x) = x^q - x$, But the set of roots of this is polynomial applies to the properties of irreducible polynomials over a finite field.

Existence of Irreducible Polynomials

If $GF(q)$ is a finite field and d is a positive integer, in this is case irreducible polynomial of degree d over $GF(q)$, the extension $GF(q) < GF(q^d)$ is simple and so $GF(q^d) = GF(q)(\alpha)$ for some $\alpha \in GF(q^d)$. Then the minimal polynomial $p(x) = min(\alpha, GF(q))$ is irreducible of degree d.

The Splitting Field and Roots of an Irreducible Polynomial

Let $p(x)$ be irreducible over $GF(q)$ of degree d and α a root of $p(x)$. As $GF(q) < GF(q)(\alpha)$ is normal, this is followed $p(x)$ splits in $GF(q)(\alpha)$ and so $GF(q)(\alpha) = GF(q^d)$ is a splitting field for $p(x)$. Then $p(x) \mid x^{q^d} - x$ in addition

$$p(x) \mid x^{q^n} - x \Leftrightarrow GF(q^d) < GF(q^n) \Leftrightarrow d \mid n.$$

Remark 2.6.1 *1. and from it the degree d it is the smallest positive integer for which* $p(x) \mid x^{q^d} - x$.

2. the Galois group is the cyclic group $< \sigma_q >$*, the roots of* $p(x)$ *are*

$$\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{d-1}}$$

3. d *it is the smallest positive integer for which* $\alpha^{q^d} = \alpha$.

2.7 Normal Bases

Since any extension $GF(q) < GF(q^d)$ is simple, there is an $\alpha \in GF(q^d)$ for which $GF(q^d) = GF(q)(\alpha)$. Moreover, the set $1, \alpha, ..., \alpha^{d-1}$ is a basis for E over F. This type of basis is called a **polynomial basis**.
Since the d roots of an irreducible polynomial $p(x)$ of degree d over $GF(q)$ are special.
a normal basis is a basis of roots of an irreducible polynomial.

Theorem 2.7.1 *There exists a normal basis* $\{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ *for* $GF(q^n)$ *over* $GF(q)$.

2.8 The Algebraic Closure of a Finite Field

In this section, we will define **the algebraic closure** of a finite field $GF(q)$.
Since $GF(q) < GF(q^n)$ is algebraic for all positive integers n, an algebraic closure of $GF(q)$ must contain all of the fields $GF(q^n)$.
As $n!/(n+1)!$, and from it

$$GF(q^{n!}) < GF(q^{(n+1)!})$$

and so

$$\Gamma(q) = \bigcup_{n=0}^{\infty} GF(q^{n!}).$$

It is an extension field of $GF(q)$ that contains $GF(q^n)$, each $n \geq 0$. In addition to that E is a field for which $GF(q) < E$ for all n, then $\Gamma(q) < E$ that is, $\Gamma(q)$ is the smallest field containing each $GF(q^n)$.

Theorem 2.8.1 *The field* $\Gamma(q)$ *is the algebraic closure of* $GF(q)$.

2.9 Orders of Element

Definition 2.9.1 *Let* $\mathbb{F}$ *be a field and let* $a \in \mathbb{F}^\times$*. The order of a in* $\mathbb{F}$*, denoted* $ord_{\mathbb{F}}(a)$*, is the smallest positive integer k for which* $a^k = 1$*. If no such k exists, then we say that a has* ***infinite order****.*

Example 2.9.1 *The element* $1+i$ *has order* 8 *in* $\mathbb{Z}_3(i)^\times$*, since*

$$(1+i)^1 = 1+i, \quad (1+i)^2 = 2i, \quad (1+i)^3 = 1+2i, \quad (1+i)^4 = 2,$$

$$(1+i)^5 = 2+2i, \quad (1+i)^6 = i, \quad (1+i)^7 = 2+i, \quad (1+i)^8 = 1.$$

Proposition 2.9.1 *(Powers That Equal One)*
Let $\mathbb{F}$ *be a field, let* $a \in \mathbb{F}^\times$*, and let* $n \geq 1$ *Therefore*

$$a^n = 1 \ \ if \ \ and \ \ only \ \ if \ \ ord_{\mathbb{F}}(a) \mid n \quad for \ \ all \ \ n \geq 1.$$

Proof. Let $k = ord_{\mathbb{F}}(a)$. If $k \mid n$, then $n = mk$ for some $m \geq 1$, so

$$a^n = a^{mk} = (a^k)^m = 1^m = 1.$$

Conversely, suppose that $a^m = 1$, and let i and j be integers so that

$$im + jk = \gcd(m,k)$$

Then

$$a^{\gcd(m,k)} = a^{im+jk} = (a^m)^i (a^k)^j = 1^i 1^j = 1.$$

Then $\gcd(m,k)$ must be greater than or equal to k,
so it follows that $\gcd(m,k) = k$, and hence $k \mid m$. ■

Corollary 2.9.1 *Let $\mathbb{F}$ be a field, let $a \in \mathbb{F}$, and suppose that $ord_{\mathbb{F}}(a) = k$. Then for any $n \geq 1$,*

$$ord_{\mathbb{F}}(a^n) = \frac{k}{\gcd(n,k)}.$$

Theorem 2.9.1 *Let $\mathbb{F}$ be a finite field with elements. Then*

$$a^{m-1} = 1 \quad for \ \ all \ \ a \in \mathbb{F}^{\times}.$$

Example 2.9.2 *recall that the field $\mathbb{Z}_7(i)$ has 49 elements. According to the above theorem,*

$$(a+bi)^{48} = 1$$

for any element $a + bi \in \mathbb{Z}_7(i)$.

Corollary 2.9.2 *If $\mathbb{F}$ is a finite field with m elements and $a \in \mathbb{F}^{\times}$, then*

$$ord_{\mathbb{F}}(a) \mid m-1.$$

2.10 Root of Unity

In mathematics, the unit root, which may be called a **de Moivre** number, is a complex number equal to one when raised to the power of an integer n. The unit roots are used in many fields and are of great importance in number theory, field theory, and discrete Fourier transform. The concept of unit roots can be defined in any field

Definition 2.10.1 *The unit root of degree n (or nth root of unity) where n is a positive integer (i.e.,$n = 1,2,3,...$) is complex number ζ that fulfills the following equation:*

$$\zeta^n = 1.$$

Example 2.10.1 *1 is the only first root of unity, and 1 and -1 are the only square roots of unity. It is easy to check that*

$$1, \ \ i, \ -1, \ \ and \ \ -i$$

are fourth roots of unity.

Proposition 2.10.1 *For any positive integer n, there are exactly n different nth roots of unity, namely the numbers*

$$e^{2k\pi i/n} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$$

for $0 \leq k < n$.

Proof. Note first that the n different numbers $e^{2k\pi i/n}$ for $0 \leq k < n$ are all distinct since they lie on the unit circle in the complex plane at angles of $2k\pi/n$ from the origin. Each of these numbers is an nt root of unity, since

$$(e^{2k\pi i/n})^n = e^{2k\pi i} = 1$$

for all k. But since any nth root of unity is a root of the polynomial $z^n - 1$, which has degree n, there can be at most n different nth roots of unity, and therefore the numbers $e^{2k\pi i/n}$ for $0 \leq k < n$ are the only possibilities.
According to this proposition, if we let

$$w = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$$

then the nth roots of unity are precisely the numbers

$$1,\ w,\ w^2,\ \ldots,\ w^{n-1},$$

since $w^k = e^{2k\pi i/n}$ for each k. For example, if $n = 4$ then $w = i$, and the fourth roots of unity are the powers of i:

$$i^0 = 1,\ i^1 = i,\ i^2 = -1,\ i^3 = -i. \qquad \blacksquare$$

Example 2.10.2 *The cube roots of unity consist of the number* 1 *together with*

$$w = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2} \ \text{ and } \ w^2 = e^{4\pi i/3} = \frac{-1-i\sqrt{3}}{2}.$$

Note that w and w^2 lie on the unit circle in the complex plane at angles of $2\pi/3 = 120^\circ$ and $4\pi/3 = 240^\circ$, respectively.

Example 2.10.3 *The fifth roots of unity are the numbers $1, w, w^2, w^3, w^4$, where*

$$w = e^{2\pi i/5} = \cos(\frac{2\pi}{5}) + i\sin((\frac{2\pi}{5}) = \frac{-1+\sqrt{5}+i\sqrt{10+\sqrt{5}}}{4}.$$

The five roots lie at equally spaced points on the unit circle, with angles of

$$0,\ 2\pi/5 = 72^\circ,\ 4\pi/5 = 144^\circ,\ 6\pi/5 = 216^\circ,\ 8\pi/5 = 288^\circ.$$

Example 2.10.4 *The sixth roots of unity are the numbers* $1,\ w,\ w^2,\ w^3,\ w^4,\ w^5$. *where*

$$w = e^{i\pi/3} = \cos(\frac{\pi}{3}) + i\sin(\frac{\pi}{3}) = \frac{1+i\sqrt{3}}{2}.$$

Note that $w^3 = -1$ is a square root of unity and that

$$w^2 = \frac{-1+i\sqrt{3}}{2} \ \text{ and } \ w^4 = \frac{-1-i\sqrt{3}}{2}.$$

are cube roots of unity. The last root is w^5, which is the complex conjugate of w.

Proposition 2.10.2 *Let $\zeta \in \mathbb{C}$ and let $n \geq 1$. Then ζ is an nth root of unity if and only if $ord_{\mathbb{C}}(\zeta) \mid n$.*

Definition 2.10.2 ***(primitive nth root of unity)***
A ***primitive root of unity*** *is any nth root of unity ζ for which $ord_{\mathbb{C}}(\zeta) = n$. We will let $P(n)$ denote the set of all primitive nth roots of unity.*

That is, $\zeta \in \mathbb{C}^\times$ is a primitive nth root of unity if $\zeta^n = 1$ but $\zeta^k \neq 1$ for any $k < n$. Applying Proposition 2.9.1, we obtain the following characterization of the nth roots in terms of primitive roots.

Corollary 2.10.1 *the union $\bigcup_{d/n} P(d)$, represent The set of all nth roots of unity .*

Example 2.10.5

$$P(1) \cup P(2) \cup P(4) = \{1\} \cup \{-1\} \cup \{i, -i\}$$

and the sixth roots of unity are the union
$P(1) \cup P(2) \cup P(3) \cup P(6) = \{1\} \cup \{-1\} \cup \{\frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\} \cup \{\frac{1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}\}$

Proposition 2.10.3 *(Characterization of Primitive nth Roots)*
Let n be a positive integer, let $\omega = e^{2\pi i/n}$, and let

$$\zeta = \omega^k$$

be an nth root of unity. Then ζ is a primitive nth root of unity if and only if

$$\gcd(k, n) = 1.$$

Proof. Clearly $ord_{\mathbb{C}}(\omega) = n$. Then $ord_{\mathbb{C}}(\omega^k) = n/\gcd(n,k)$ by Corollary 2.9.1. In particular, $ord_{\mathbb{C}}(\omega^k) = n$ if and only if $\gcd(n,k) = 1$. ■

Corollary 2.10.2 *For all $n \geq 1$, there are exactly $\phi(n)$ primitive nth roots of unity.*

By this Corollary and Corollary 2.10.1, we get the following the totient function.

Corollary 2.10.3 *(Sum of the Totient Function)*
If n is a positive integer, then

$$\sum_{d|n} \phi(d) = n$$

For example,

$$\phi(1) + \phi(2) + \phi(4) = 1 + 1 + 2 = 4$$

and

$$\phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$$

2.11 Cyclotomic Extension

When the circle is divided into equal parts, in this case we know a new term called **cyclotomy**, specifically, it is the effect obtained by blotting the nth root of unity over $\mathbb{Q}$ in the complex plane.

Definition 2.11.1 *Let F be a field and let S be a splitting field of $X^n - 1$ over F is called a **cyclotomic extension of order** n of F.*
Since

$$S = F(U_n) = F(\Omega_n) = F(w)$$

Remark 2.11.1

1. *$w \in \Omega_n$ is the splitting field of a separable polynomial, it follows that $F < S$ is a finite Galois extension and*

$$[S : F] = deg(min(w, F)) = |G_F(S)|.$$

2. *All $\sigma \in GF(S)$ it is determined by its value on a fixed $w \in \Omega_n$, and since σ preserves order, σ must be a root of primitive roots of unity in S, that is,*

$$\sigma w = w^{k(\sigma)}$$

Where $k(\sigma) \in \mathbb{Z}_n^*$.
Since

$$w^{k(\sigma\tau)} = (\sigma\tau)w = \sigma(w^{k(\tau)}) = (\sigma w)^{k(\tau)} = w^{k(\sigma)k(\tau)}$$

And from it

$$k(\sigma\tau) = k(\sigma)k(\tau) \ mod \ n.$$

3. *the map $k : GF(S) \longmapsto \mathbb{Z}_n^*$ is a homomorphism. Since $k(\sigma) = 1$ implies that $\sigma = \tau$, the map k is a monomorphism and from it $G_F(S)$ is isomorphic to a subgroup of $\mathbb{Z}_n^*$.*

Theorem 2.11.1 *If $F < S$ is a cyclotomic extension of order n, then $G_F(S)$ is isomorphic to a subgroup of $\mathbb{Z}_n^*$, the group of units of $\mathbb{Z}_n^*$. Hence, $G_F(S)$ is abelian and $[F : S] \mid \phi(n)$.*

Theorem 2.11.2 *Let $n = \prod p_i^{e_i}$, where the p_i's are distinct primes. Then*

$$\mathbb{Z}_n^* = \prod \mathbb{Z}_{p_i^{e_i}}^*.$$

Moreover, $\mathbb{Z}_n^*$ is cyclic if and only if $n = p^e$, $2p^e$ or 4, where p is an odd prime.

Corollary 2.11.1 *A cyclotomic extension $F < S$ is abelian and if $n = p^e, 2p^e$ or 4, where p is an odd prime, then $F < S$ is cyclic.*

2.12 Cyclotomic Polynomials

In mathematics, the eighth cyclotomic polynomial, for any integer n, is a unique, irreducible polynomial with integer coefficients representing a division of any integer and not a division of any integer. Its roots are all primitive roots of the unit, where k operates on a positive integer no more than n and an arithmetic number n.

Definition 2.12.1 *The nth cyclotomic polynomial Φ_n is defined by*

$$\Phi_n(x) = \prod_{\zeta \in p(n)} (X - \zeta)$$

Remark 2.12.1 *We mentioned previously that $p(n)$ Refers to the set of all primitive nth roots of unity.*

Example 2.12.1

- *Since $p(1) = \{1\}$ and $p(2) = \{-1\}$, the first and second cyclotomic polynomials are respectively*

$$\Phi_1(x) = x - 1 \text{ and } \Phi_2(x) = x + 1$$

- *Recall that $p(3) = \{w, w^2\}$, where $w = \frac{(-1+i\sqrt{3})}{2}$. Thus the third cyclotomic polynomial is*

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

- *Since $p(4) = \{i, -i\}$, the fourth cyclotomic polynomial is*

$$\Phi_4(x) = (x-i)(x+i) = x^2+1$$

.

Theorem 2.12.1 *Let $\Phi_n(x)$ is the nth cyclotomic polynomial over F.*

1. *$deg(\Phi_n(x)) = \phi(n)$.*

2. *We have*

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \;\; Fundamental \;\; Relation$$

3. *If n is a positive integer, then $\Phi_n(x)$ is monic.*

4. *If $F = \mathbb{Q}$ then the coefficients of $\Phi_n(x)$ are integers.*

Proof. (*Fundamental Relation*)
Every k such that $1 \leq k \leq 1$ has $(k,n) = n_1$ for some divisor n1 of n. When d runs through the divisors of n, so does $n_1 = n \mid d$. Hence

$$\prod_{n|d} \Phi_d(x) = \Pi_{k=1}^{n}[x - e(k \mid n)] = x^n - 1. \qquad \blacksquare$$

Example 2.12.2

- $x^2 - 1 = \Phi_1(x)\ \Phi_2(x) = (x-1)(x+1)$.
- $x^3 - 1 = \Phi_1(x)\ \Phi_3(x) = (x-1)(x^2+x+1)$.
- $x^4 - 1 = \Phi_1(x)\ \Phi_2(x)\ \Phi_4(x) = (x-1)(x+1)(x^2+1)$.
- $x^5 - 1 = \Phi_1(x)\ \Phi_5(x) = (x-1)(x^4+x^3+x^2+x+1)$.
- $x^6 - 1 = \Phi_1(x)\ \Phi_2(x)\ \Phi_3(x)\ \Phi_6(x) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$.

Theorem 2.12.2 *[2][4][3] Let m,n,k be positive integers so that $g.c.d.\{m,n\} = 1$ and m is divisible by every prime factor of k. Then*

$$\Phi_m(X^{nk}) = \prod_{d|n} \Phi_{mkd}(X). \tag{2.1}$$

In particular, we find that

$$\Phi_m(X^n) = \prod_{d|n} \Phi_{md}(X),\ if \;\; g.c.d.\{m,n\} = 1; \tag{2.2}$$

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}) = \Phi_{p^{r-1}}(X^p).$$
$$if\ p\ is\ a\ \ prime\ \ number\ \ and\ \ r \geq 2.$$

The purpose of this note is to provide several applications of formulae (2.1) and (2.2) Before proceeding to these applications, let us state a result which seems not well known.

Definition 2.12.2 *(Mobius Function). Suppose n is a positive integer with prime factorization* $\prod_{k=1}^{r} p_k^{f_k}$. *The function* $\mu : \mathbb{N} \longmapsto \mathbb{N}$ *given by*

$$\mu(n) = \begin{cases} (-1)^r & if\ f_k = 1\ for\ all\ k, \\ 0 & if\ \ f_k > 1\ for\ some\ k, \end{cases}$$

is called the Mobius function.

Proposition 2.12.1 *(Integer Coeffcients)*
Every cyclotomic polynomial $\Phi_n(x)$ *has integer coeffcients.*

Proposition 2.12.2 *If* $p > 2$ *is prime, and from him*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1$$

and

$$\Phi_{2p}(x) = x^{p-1} - x^{p-2} + ... - x + 1.$$

Proof.
Let p is prime, $\Rightarrow x^p - 1 = \Phi_1(x)\ \ \Phi_p(x)$, and therefore

$$\Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1.$$

In addition to that,

$$\begin{aligned} \Phi_{2p}(x) &= \tfrac{x^{2p}-1}{\Phi_1(x)\Phi_2(x)\Phi_p(x)} = \tfrac{x^{2p}-1}{(x^p-1)\Phi_2(x)} \\ &= \tfrac{x^{2p}-1}{(x^p-1)(x+1)} = \tfrac{x^p+1}{x+1} \\ &= x^{p-1} - x^{p-2} + ... - x + 1. \end{aligned}$$

■

Example 2.12.3

$$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

and

$$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1.$$

Lemma 2.12.1 *Let* $\mathbb{F}$ *be a field, let it be k and n be positive integers with* $k \mid n$. *and from him . For all* $a \in \mathbb{F}^{\times}$,

$$ord_{\mathbb{F}}(a) = nk \Leftrightarrow ord_{\mathbb{F}}(a^k) = n.$$

Proof. If $ord_{\mathbb{F}}(a) = nk$, then by Corollary 2.9.1, it follows that

$$ord_{\mathbb{F}}(a^k) = \frac{nk}{\gcd(k, nk)} = \frac{nk}{k} = n.$$

For the converse, suppose that $ord_{\mathbb{F}}(a^k) = n$, and let $m = ord_{\mathbb{F}}(a)$. By Corollary 2.9.1, we know that

$$ord_{\mathbb{F}}(a^k) = \frac{m}{\gcd(m, k)}$$

so

$$\frac{m}{\gcd(m, k)} = n.$$

Since $k \mid n$ and $m = n\gcd(m, k)$, we know that $k \mid m$, and therefore $\gcd(m, k) = k$.
It follows that $m = nk$. ■

Proposition 2.12.3 *Let n and k be positive integers with $k \mid n$. And from him*

$$\Phi_{nk}(x) = \Phi_n(x^k).$$

Proof. Let $\zeta \in \mathbb{C}^\times$. By the lemma, $\zeta \in P(nk)$ if and only if $\zeta^k \in P(n)$. Thus ζ is a root of $\Phi_{nk}(x)$ if and only if ζ^k is a root of $\Phi_n(x^k)$. Then $\Phi_{nk}(x)$ and $\Phi_n(x^k)$ are monic polynomials with the same roots, so they must be equal. ■

Example 2.12.4

$$\Phi_{18}(x) = \Phi_6(x^3) = (x^3)^2 - (x)^3 + 1 = x^6 - x^3 + 1$$

and

$$\Phi_{64}(x) = \Phi_8(x^8) = (x^8)^4 + 1 = x^{32} + 1.$$

2.13 Primitive Elements

In field theory, a primitive element of a finite field $GF(q)$ is a generator of the multiplicative group of the field. In other words, $a \in GF(q)$ is called a primitive element if it is a primitive $(q-1)$ th root of unity in $GF(q)$ this means that each non-zero element of $GF(q)$ can be written as a^i for some integer i. In this case, a primitive element is also called a primitive root modulo q.

Definition 2.13.1 *Let $\mathbb{F}$ be a finite field with m elements. If $ord_{\mathbb{F}}(a) = m-1$ in this case we call the element a **primitive element** of $\mathbb{F}$.*

Theorem 2.13.1 *Let $\mathbb{F}$ be a field, let $a \in \mathbb{F}^\times$, and suppose that $ord_{\mathbb{F}}(a) = n$. Then $\Phi_n(a) = 0$.*

Proof. By Fundamental Relation, we know that

$$\prod_{d|n} \Phi_d(a) = a^n - 1 = 0.$$

But for $d < n$, the polynomial $\Phi_d(x)$ is also a factor of $x^d - 1$. Since a is not a root of $x^d - 1$ for any $d < n$, it follows that $\Phi_d(a) \neq 0$ for any $d < n$, and therefore $\Phi_d(a) = 0$. ■

Theorem 2.13.2 *Let $\mathbb{F}$ be a finite field with m element and let d be a divisor of $m-1$. Therefore the polynomial $\Phi_d(x)$ has exactly $\phi(d)$ roots in $\mathbb{F}$, and these are precisely the elements of $\mathbb{F}^\times$ that have order d.*

Proof. For each divisor d of $m-1$, let $R(d)$ be the set of all roots of $\Phi_n(x)$ in $\mathbb{F}^\times$. By the previous proposition, if $a \in \mathbb{F}^\times$ has order d, then $d \in R(d)$. By Lagrange's theorem for finite fields, we know that the order of a divides $m-1$ for all $a \in \mathbb{F}^\times$, and hence

$$\bigcup_{d|m-1} R(d) = \mathbb{F}^\times.$$

But since each $\Phi_d(x)$ has degree $\phi(d)$, we know that $|R(d)| \leq \phi(d)$ for each d. By Corollary 2.10.3, we have

$$\sum_{d|m-1} \phi(d) = m - 1 = |\mathbb{F}^\times|.$$

so indeed $|R(d)| = \phi(d)$ for each $d \mid m-1$, Moreover, these sets must all be disjoint, so each element $a \in \mathbb{F}^\times$ of order d lies only in $R(d)$, and therefore each element of $R(d)$ must have order d. ■

Corollary 2.13.1 *Let $\mathbb{F}$ be a finite field with m elements. Then $\mathbb{F}$ has exactly $\phi(m-1)$ primitive elements*

Indeed, these primitive elements are precisely the roots of $\Phi_{(m-1)}(x)$ in $\mathbb{F}$. For example, the primitive elements of $\mathbb{Z}_7$ are 3 and 5, and these are precisely the roots of the polynomial $\Phi_6(x) = x^2 - x + 1$ in $\mathbb{Z}_7$. Indeed, it is easy to check that

$$x^2 - x + 1 \equiv (x-3)(x-5) \ (mod\ 7).$$

We can state this sort of factorization of $\Phi_k(x)$ in general.

Corollary 2.13.2 *Let p be a prime and let d be a divisor of $p-1$. Then*

$$\Phi_d(x) = \prod_{\zeta \in O(d)} (x - \zeta) \ \ (mod\ p)$$

where $O(d)$ denotes the set of elements of $\mathbb{Z}_p^\times$ of order d.

2.14 The Irreducibility of Cyclotomic Polynomials

The irreducibility of the cyclotomic polynomials is a fundamental result in algebraic number theory that has been proved many times, by many different authors, in varying degrees of generality and using a variety of approaches and methods of proof. We will examine this in the spirit.

Theorem 2.14.1 *If n is a positive integer, then $\Phi_n(x)$ is monic and its degree is $\phi(n)$, where ϕ is the Euler phi function.*

Theorem 2.14.2 *A polynomial $f(x)$ over a field F has a multiple zero in some extension field of F if and only if $f(x)$ and its derivative, $f'(x)$, have a common factor of a positive degree in $F[x]$.*

Lemma 2.14.1 *Let $g(x)$ and $h(x)$ belong to $\mathbb{Z}[x]$, and let $h(x)$ be monic. If $h(x)$ divides $g(x)$ in $\mathbb{Q}[x]$, then $h(x)$ divides $g(x)$ in $\mathbb{Z}[x]$.*

Lemma 2.14.2 *If $g(x) \in \mathbb{Z}_p[x]$ where p is prime, then*

$$(g(x))^p = g(x^p).$$

Proof. Consider the function $\psi : \mathbb{Z}_p[x] \longmapsto \mathbb{Z}_p[x]$ given by $\psi(f(x)) = (f(x))^p$. Suppose $f(x), h(x) \in \mathbb{Z}_p[x]$. Note that $\psi(f(x)h(x)) = (f(x)h(x))^p = (f(x))^p(h(x))^p$ Now, by [6, Theorem 3.17], if p is prime and $0 < j < p$, then p divides $\binom{p}{j}$ Because $\mathbb{Z}_p[x]$ has characteristic p, it follows from the binomial theorem that

$$\begin{aligned}
\psi(f(x)+h(x)) &= (f(x)+h(x))^p \\
&= \textstyle\sum_{j=0}^{p} \binom{p}{j} (f(x))^p (h(x))^p \\
&= (f(x))^p + (h(x))^p + \textstyle\sum_{j=1}^{p-1} \binom{p}{j} (f(x))^p (h(x))^p \\
&= \psi(f(x)) + \psi(h(x)) + \textstyle\sum_{j=0}^{p-1} 0 \cdot (f(x))^p (h(x))^p \\
&= \psi(f(x)) + \psi(h(x))
\end{aligned}$$

Therefore is operation preserving, and hence a homomorphism. Suppose $a \in \mathbb{Z}_p[x]$ and a is a constant polynomial. If $a \neq 0$, then $\gcd(a, p) = 1$, and so by Fermat's Little Theorem, $a^p \equiv a \ \ (mod\ p)$. Also $0^p = 0$, and therefore if a is a constant polynomial in $\mathbb{Z}_p[x]$, then $\psi(a) = a^p = a$. If $g(x) \in \mathbb{Z}_p[x]$, then we may write $g(x) = \sum_{j=0}^{n} a_j x^j$, It follows that

$$\begin{aligned}(g(x))^p &= \psi(g(x)) \\ &= \psi(\textstyle\sum_{j=0}^{n} a_j x^j) \\ &= \textstyle\sum_{j=0}^{n} \psi(a_j)\psi(x^j) \\ &= \textstyle\sum_{j=0}^{n} a_j x^{pj} \\ &= g(x^p)\end{aligned}$$

Theorem 2.14.3 *The cyclotomic polynomials $\Phi_n(x)$ are irreducible over $\mathbb{Z}$.*

Proof. Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible factor of $\Phi_n(x)$. We will show that every zero of $\Phi_n(x)$ is a zero of $f(x)$.
Since $\Phi_n(x)$ divides $x^n - 1$ in $\mathbb{Z}[x]$, there exists a polynomial $g(x) \in \mathbb{Z}[x]$ such that $x^n - 1 = f(x)g(x)$. Let ω be a primitive n^{th} root of unity that is a zero of $f(x)$. Let p be a prime that does not divide n; then $\gcd(p,n) = 1$, and so by [8, Lemma 3], ω^p is also a primitive n^{th} root of unity. It follows that $0 = (\omega^p)^n - 1 = f(\omega^p)g(\omega^p)$, and so ω^p is a zero of either $f(x)$ or $g(x)$. Suppose $f(\omega^p) \neq 0$, then $g(\omega^p) = 0$, so ω is a zero of $g(x^p)$. Because $f(x)$ is monic, irreducible, and has ω as a zero, by definition $f(x)$ is the minimal polynomial for ω over $\mathbb{Q}$. Therefore, by [5, Theorem 21.3], $f(x)$ divides $g(x^p)$ in $\mathbb{Q}[x]$, and so because $f(x)$ is monic, by Lemma 2.14.1, $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$. Say that $g(x^p) = f(x)h(x)$ where $h(x) \in \mathbb{Z}[x]$. Let $\bar{g}(x), \bar{f}(x)$ and $\bar{h}(x)$ be the polynomials in $\mathbb{Z}_p[x]$ formed by reducing the coefficients of $g(x), f(x)$, and $h(x)$ modulo p respectively; then $\bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$. Now by Lemma 2.14.2, $(\bar{g}(x))^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$. Since by [5, Corollary to Theorem 18.3], $\mathbb{Z}_p$ is a unique factorization domain, $\bar{f}(x)$ and $\bar{g}(x)$ share a common irreducible factor, call it $k(x)$. Thus for some $m_1(x), m_2(x) \in \mathbb{Z}_p[x]$, $\bar{f}(x) = k(x)m_1(x)$ and $\bar{g}(x) = k(x)m_2(x)$. It follows that in $\mathbb{Z}_p[x]$.

$$x^n - 1 = \bar{f}(x)\bar{g}(x) = (k(x))^2 m_1(x)m_2(x).$$

Hence $x^n - 1$ has a multiple zero in some extension field of $\mathbb{Z}_p$, and so by Theorem 2.14.2, $x^n - 1$ and its derivative, nx^{n-1}, must have a common factor of positive degree. Note that every factor of nx^{n-1} will be of the form c^{x^q}, where $c \mid n$ and $0 \leq q \leq n-1$. Also note that any element of this form with a positive degree cannot divide $x^n - 1$, which means that $x^n - 1$ and nx^{n-1} cannot share a common factor. Thus we have reached a contradiction, and so $f(\omega^p) = 0$. Therefore, if ω is any primitive n^{th} root of unity that is a zero of $f(x)$ and p is any prime that does not divide n, then ω^p is a zero of $f(x)$.
Still assuming that ω is a primitive n^{th} root of unity that is also a zero of $f(x)$, let ξ be any other primitive n^{th} root of unity. Because ω generates the group of n^{th} roots of unity, there exists an integer k such that $\omega^k = \xi$. Now by [8, Lemma 3], $\gcd(k,n) = 1$. It follows that $k = p_1 p_2 \ldots p_r$ where for all i, p_i is a prime that does not divide n. Therefore $\omega, \omega^{p_1}, (\omega^{p_1})^{p_2}, (\omega^{p_1 p_2})^{p_3}, \ldots, (\omega^{p_1 p_2 \cdots p_{r-1}})^{p_r} = \omega^k$ are all zeros of $f(x)$ that are primitive n^{th} roots of unity, in particular ξ is a zero of $f(x)$. Hence every primitive n^{th} root of unity is a zero of $f(x)$, and so $f(x)$ and $\Phi_n(x)$ share all their zeros. Since by Theorem 2.14.1, $\Phi_n(x)$ is monic, this means that $\Phi_n(x) = f(x)$, and so $\Phi_n(x)$ is irreducible over the integers. ■

Corollary 2.14.1 *The n^{th} cyclotomic polynomials $\Phi_n(x)$ are irreducible over $\mathbb{Q}$.*

Proof. Suppose that $\Phi_n(x) = f(x)g(x)$ in $\mathbb{Q}[x]$ with f of positive degree. Via Gauss' lemma, we can suppose that both f and g are monic and are in $\mathbb{Z}[x]$. Let $x - \zeta$ be a linear factor of $f(x)$ in $\mathbb{K}[x]$ for an extension field k of $\mathbb{Q}$. We wish to show that $x - \zeta^a$ is also a linear factor of f for every $a \in (\mathbb{Z}/n)^\times$, and thus that

$$\deg f = \varphi(n) = \deg \Phi_n$$

concluding that $f = \Phi_n$.
Since each $a \in (\mathbb{Z}/n)^\times$ is a product of primes p not dividing n, it suffices to show that $x - \zeta^p$ is a linear factor of $f(x)$ for all primes p not dividing n. If not, then $x - \zeta^p$ is necessarily a linear factor of $g(x)$,

by unique factorization in $K[x]$. That is, ζ is a root of $g(x^p) = 0$ in k, so $x - \zeta$ divides $g(x^p)$ in $K[x]$. Thus, in $\mathbb{Q}[x]$ the gcd of $f(x)$ and $g(x^p)$ is not 1: otherwise, there would be $r(x), s(x) \in \mathbb{Q}[x]$ such that

$$1 = r(x) \cdot f(x) + s(x) \cdot g(x^p)$$

Mapping $\mathbb{Q}[x]$ to k by $x \longmapsto \zeta$ would give the impossible

$$1 = r(\zeta) \cdot 0 + s(\zeta) \cdot 0$$

Thus, $d(x) = \gcd(f(x), g(x^p))$ in $\mathbb{Q}[x]$ is of positive degree. Let $a(x)$ and $b(x)$ be in $\mathbb{Q}[x]$ such that

$$f(x) = a(x) \cdot d(x) \qquad g(x^p) = b(x) \cdot d(x)$$

We can certainly take d to be in $\mathbb{Z}[x]$ and have content 1. By Gauss' lemma, $a(x)$ and $b(x)$ are in $\mathbb{Z}[x]$ and have content 1. In fact, adjusting by at most ± 1, we can take $a(x), b(x)$, and $d(x)$ all to be monic. Map everything to $\mathbb{F}_p[x]$. There $g(x^p) = g(x)^p$, so

$$\begin{cases} f(x) & = & a(x) \cdot b(x) \\ g(x)^p = g(x^p) & = & b \cdot d \end{cases}$$

Let $\delta(x) \in \mathbb{F}_p[x]$ be an irreducible dividing $d(x)$ in $\mathbb{F}_p[x]$. Then since $\delta(x)$ divides $g(x)^p$ in $\mathbb{F}_p[x]$ it divides $g(x)$. Also $\delta(x)$ divides $f(x)$ in $\mathbb{F}_p[x]$, so $\delta^2(x)$ apparently divides $\Phi_n(x) = f(x) \cdot g(x)$ in $\mathbb{F}_p[x]$. But p does not divide n, so $\Phi_n(x)$ has no repeated factor in $\mathbb{F}_p[x]$, contradiction. Thus, it could not have been that $\Phi_n(x)$ factored properly in $\mathbb{Q}[x]$. ■

Theorem 2.14.4 *[7] Let*

$$\Phi_m(X) = \prod_{0<a<m \ (a,m)=1} (X - \zeta^\alpha)$$

be the mth cyclotomic polynomial. Then $\Phi_m(X)$ is irreducible in $\mathbb{Q}[X]$.

Let $r(X)$ be an irreducible, primitive polynomial having ζ as zero. our proof of Theorem 2.14.4 will be based on

Theorem 2.14.5 *[7] Let p be a prime, $p \nmid m$. If $\eta \in \mathbb{C}$ is such that $r(\eta) = 0$, then $r(\eta^p) = 0$.*

Let us first show that Theorem 2.14.5 implies Theorem 2.14.4.
Since $r(X)$ is irreducible in $\mathbb{Q}[X]$,

it suffices to show that

$$r(X) = \Phi_m(X). \tag{2.3}$$

. If we show that

$$\Phi_m(X) \mid r(X), \tag{2.4}$$

therefore, since $\Phi_m(X) \in \mathbb{Q}[X]$, $\phi_m(\zeta) = 0$ and since any polynomial in $\mathbb{Q}[X]$ which has ζ as zero is divisible by $r(X)$, we deduce that (2.3) holds. Thus, let us show that Theorem 2.14.5 implies (2.4).
Let $0 \leq a \leq m-1, (a,m) = 1$.
Then $a = p_1 ..., p_i, p_i$ prime, $p_i \nmid m$. Then by repeated application of Theorem 2.14.5, we deduce that

$$\begin{aligned} r(\zeta) = 0 &\Longrightarrow r(\zeta^{p_1}) = 0 \\ &\Longrightarrow r(\zeta^{p_1 p_2}) = 0 \\ &\quad \vdots \\ &\Longrightarrow r(\zeta^a) = 0 \\ &\Longrightarrow X - \zeta^a \mid r(X) \\ &\Longrightarrow \Phi_m(X) \mid r(X) \end{aligned}$$

using Proof Theorem 2.14.5.
Let $s(X)$be an irreducible, primitive polynomial having η^p as zero and we also assume that $r(\eta^p) \neq 0$. We know that $r(X)$ and $s(X)$ are irreducible, note this $(r,s) = 1$. Then, since $s(X) \mid X^m - 1$, $r(X) \mid X^m - 1$, we deduce that

$$s(X)r(X) \mid X^m - 1.$$

Then, there exists $t(X) \in \mathbb{Q}[X]$ such. that

$$X^m - 1 = s(X)r(X)t(X). \tag{2.5}$$

Let a is the smallest positive integer such that $at(X) \in \mathbb{Z}[x]$. Therefore $a > 1$ and $at(X)$ is primitive. [For if the content of $at(X)$ is $b > 1$, we can replace a by a/b, contradicting the way in which a was chosen.] But then

$$a(X^m - 1) = s(X).r(X).at(X). \tag{2.6}$$

We have $s(X)$ and $r(X)$ are monic, and we know that both are primitive. Then, by Gauss's lemma, the right-hand side of (2.6) is primitive, so that its content is 1. But the content of $a(X^m - 1)$ is $a > 1$. And from him contradiction and $t \in \mathbb{Z}[X]$.
We see that $s(X^p)$ has η as a zero, so that

$$s(X^p) = r(X).u(X) \tag{2.7}$$

for some $u(X) \in \mathbb{Q}[X]$. As above, we may prove that $u(X) \in \mathbb{Z}[X]$.
Let us interrupt our proof to derive some facts about $\mathbb{Z}_p$ and $\mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field, $\mathbb{Z}_p[X]$ is a unique factorization domain.

Lemma 2.14.3 *[7] Let $\overline{a} \in \mathbb{Z}_p$. Then*

$$\overline{a}^p = \overline{a}.$$

Proof.
Theorem Fermat's little
if $a \in \mathbb{Z}, p \nmid a$, then

$$a^{p-1} \equiv 1 (mod\ p).$$

Therefore, if $p \nmid a$, we have

$$a^p \equiv a (mod\ p) \tag{2.8}$$

However, (2.8) also holds if $p \mid a$. Then, (2.8) holds for all $a \in \mathbb{Z}$, so that $\overline{a}^p = \overline{a}$ for all $\overline{a} \in \mathbb{Z}_p$.

Lemma 2.14.4 *[7] The mapping f: $\mathbb{Z}_p[X] \longrightarrow \mathbb{Z}_p[X]$, defined by*

$$f(a) = a^p \quad (a \in \mathbb{Z}_p[X]) \ \ is \ \ a \ \ ring \ \ homomorphism.$$

In other words,

if $a, b \in \mathbb{Z}_p[X]$, then

$$(a+b)^p = a^p + b^p \tag{2.9}$$

$$(ab)^p = a^p b^p \tag{2.10}$$

Proof. The proof of (2.10) is obvious. Let us verify (2.9). By the binomial theorem in $\mathbb{Z}_p[X]$,

$$(a+b)^p = a^p + \binom{p}{1}.a^{p-1}b + \binom{p}{2}.a^{p-2}b^2 + ... + \binom{p}{p-1}.ab^{p-1} + b^p,$$

where $\binom{p}{j}$ is the integer defined by

$$\binom{p}{j} = \frac{p\cdot(p-1)...(p-j+1)}{1\cdot 2...j} \quad (j+1,...,p-1).$$

we have $1\cdot 2...j$ is not divisible by p for $j = 1,2,...,p-1$
p is prime. Then. $\binom{p}{j}$ is divisible by p for $j = 1,2,...p-1$. But for x in $\mathbb{Z}_p[X], p\cdot x = 0$.

Then,

$$\binom{p}{j}a^{p+j}b^j = 0 \ \ for \ \ j = 1,2,...p-1,$$

and if $f(X) = a_0 + a_1X + ... + a_nX^n \in \mathbb{Z}[X]$, let us define the reduction of $f(X)$ *modulo* p, denoted $\overline{f(X)}$, by

$$\overline{f(X)} = \bar{a_0} + \bar{a_1}X + ...\bar{a_n}X^n = \mathbb{Z}_p[X].$$

It is easy to verify that the mapping

$$\begin{array}{c}\mathbb{Z}[X] \longrightarrow \mathbb{Z}_p[X],\\ f \longrightarrow \bar{f}\end{array}$$

is a ring homomorphism.

Lemma 2.14.5 *[7] Let $f = a_0 + a_1X + ... + a_nX^n \in \mathbb{Z}[X]$. Then*

$$\overline{f(X^p)} = \overline{f(X)^p}.$$

Proof. Using Lemma 2.14.3,

$$\begin{aligned}\overline{f(X^p)} &= \bar{a_0} + \bar{a_1}X^p + ... + \bar{a_n}X^{np}\\ &= \bar{a_0}^p + \bar{a_1}^pX^p + ... + \bar{a_n}^pX^{np}\\ &= \bar{a_0}^p + (\bar{a_1}X)^p + ... + (\bar{a_n}X^n)^p.\end{aligned}$$

Then, using Lemma 2.14.4,

$$\begin{aligned}\overline{f(X^p)} &= (\bar{a_0} + \bar{a_1}X + ... + \bar{a_n}X^n)^p\\ &= \overline{f(X)}^p.\end{aligned}$$

Let us now return to our proof of Theorem 2.14.5.
Proof of Theorem 2.14.5: we use Lemma 2.14.5 and (2.7), we conclude that

$$\overline{s(X)^p} = \overline{r(X)}\cdot\overline{u(X)}. \tag{2.11}$$

Let $\overline{v(X)}$ be an irreducible factor of $\overline{r(X)}$ in $\mathbb{Z}_p[X]$. Then by (2.11), $\overline{v(X)}$ divides $\overline{s(X)}$.
By , (2.5) however,

$$X^m - \bar{1} = \overline{X^m - 1} = \overline{s(X)}\cdot\overline{r(X)}\cdot\overline{t(X)},$$

so that $\overline{v(X)^2}$ divides $X^m - \bar{1}$. Thus,

$$X^m - \bar{1} = \overline{v(X)^2}\cdot\overline{w(X)}. \tag{2.12}$$

By taking the formal derivatives of both sides, note that $\overline{v(X)}$ divides $\bar{m}X^{m-1}$. But $p \nmid m$, so that $\bar{m} \neq \bar{0}$. Then,

$$\overline{v(X)} = \bar{a}\cdot X^b \ \ for \ \ some \ \ b \geq 1.$$

But since $\overline{v(X)}$ is irreducible, $\overline{v(X)} = \bar{a}\cdot X$, which contradicts (2.12). thus, $r(\eta^p) = 0$.

Remark 2.14.1 • *The rule or formula for the expansion of $(a+b)^n$, where n is any positive integral power, is called* ***binomial theorem****. For any positive integral n*

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r.$$

• ***(Gauss's Lemma)*** *If f and g a primitive polynomial then suppose that $f.g$ primitive polynomial.*

Chapter 3

Application of Cyclotomic Polynomials

3.1 Dirichlet's Theorem on Primes in Arithmetic Progressions

In number theory, Dirichlet's theorem, also called the Dirichlet prime number theorem, states that for any two positive coprime integers a and d, there are infinitely many primes of the form $a+nd$, where n is also a positive integer. In other words, there are infinitely many primes that are congruent to a modulo d. The numbers of the form $a+nd$ form an arithmetic progression and Dirichlet's theorem states that this sequence contains infinitely many prime numbers. The theorem, named after Peter Gustav Lejeune Dirichlet extends Euclid's theorem that there are infinitely many prime numbers. Stronger forms of Dirichlet's theorem state that for any such arithmetic progression,

$$a, a+d, a+2d, a+3d, ...,$$

the sum of the reciprocals of the prime numbers in the progression diverges and that different such arithmetic progressions with the same modulus have approximately the same proportions of primes. Equivalently, the primes are evenly distributed (asymptotically) among the congruence classes modulo d containing a's coprime to d.

Theorem 3.1.1 *For every integer n, there exist infinitely many primes*

$$p \equiv 1 (mod\ n).$$

The proof of this theorem relies on the following

Lemma 3.1.1 *For every integer n, there exists an integer $A > 0$ such that all prime divisors $p > A$ of values of $\Phi_n(c)$ at integer points c are congruent to 1 modulo n. In other words, prime divisors of values of the n^{th} cyclotomic polynomial either are "small" or are congruent to 1 modulo n.*

In this section we will explain how Lemma is used to prove theorem 3.1.1.
Assume that there are only finitely many primes congruent to 1 *modulo n*;
Let it be

$$p_1, ..., p_m \ \ are \ \ primes$$

Let us consider the number $c = A! p_1 p_2 ... p_m$. The number $k = \Phi_n(c)$ is relatively prime to c (Since the constant term of $\Phi_n(x) = \pm 1$)
Hence, they are not divisible by any of the primes $p_1, ..., p_m$, and do not contain divisor $d \leq A$ either.

We can find a new prime congruent to 1 *modulo n*: take any prime divisor p of k, and Lemma ensures that

$$p \equiv 1 \ (mod\ n).$$

The only problem that may occur is that $k = \pm 1$, so it has no prime divisor. In this case, replace k by Nk for N large enough, so that Nk is greater than all the roots of the equation $\Phi_n(x) = \pm 1$,
Proof. Let it be the polynomial

$$f(x) = (x-1)(x^2-1)...(x^{n-1}-1).$$

Since the polynomial $f(x)$ and $\Phi_n(x)$ it has no common roots, then gcd in $\mathbb{Q}[x]$ is equal to 1,

hence

$$a(x)f(x) + b(x)\Phi_n(x) = 1 \quad a(x), b(x) \in \mathbb{Q}[x].$$

Let A denote the common denominator of all coefficients of $a(x)$ and $b(x)$.
Then for

$$p(x) = Aa(x)$$

and

$$q(x) = Ab(x)$$

We have

$$p(x)f(x) + q(x)\Phi_n(x) = A \ \ and \ \ p(x), q(x) \in \mathbb{Z}[x].$$

Assume that a prime number $p > A$ divides $\Phi_n(c)$ for some c. Then c is a root of $\Phi_n(x) \ \ modulo \ \ p$.
Therefore

$$c^n \equiv 1 \ (mod\ p).$$

Let us notice that n is the order of c modulo p. Indeed, if $c^k \equiv 1 (mod\ p)$ for some $k < n$ then c is a root of $f(x)$ modulo p, but the equality $p(x)f(x) + q(x)\Phi_n(x) = A$ shows that $f(x)$ and $\Phi_n(x)$ are relatively prime modulo p. Recall that $c^{p-1} \equiv 1 (mod\ p)$ by Fermat's Little Theorem, so $p-1$ is divisible by n, the order of c, that is $p \equiv 1 (mod\ n)$, and the lemma is proved. ■

Remark 3.1.1 *Most available proofs of Theorem 3.1.1 that use cyclotomic polynomials use a different proof of Lemma. The main point that is being made by our proof is that it seems to accumulate the key ideas of elementary number theory: the Euclidean algorithm and its applications, the relationship between $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$, the techniques based on the reduction modulo p, and the multiplicative group of integers modulo p (through Fermat's Little Theorem).*

3.2 Wedderburn's Little Theorem

In mathematics, Wedderburn's little theorem states that every finite domain is a field. In other words, for finite rings, there is no distinction between domains, skew-fields and fields. The Artin-Zorn theorem generalizes the theorem to alternative rings: every finite alternative division ring is a field

Theorem 3.2.1 *Every finite division ring is commutative.*

By a ring we mean a set R with two operations (sum and product) satisfying the usual axioms. The product does not have to be commutative, e.g. square matrices of the given size form a ring, and quaternions form a ring too.
By a division ring, we mean a ring where every nonzero element is invertible, e.g. quaternions. Thus, the theorem states that if R is a finite division ring, then it in fact is a field. Let us recall several

definitions from ring theory that we need in this proof. For a ring R, its center $Z(R)$ consists of all elements that commute with all elements from R:

$$Z(R) = \{z \in R : zr = rz \ \ for \ \ all \ \ r \in R\}.$$

The center of a ring is closed under sum and product, and so forms a subring of R. If R is a division ring, then $Z(R)$ is a field, and R is a vector space over this field.
More generally, if $S \subset R$, the centraliser of S is defined as the set of all elements that commute with all elements from S:

$$C_S(R) = \{z \in R : zs = sz \ \ for \ \ all \ \ s \in S\}.$$

The centraliser of every subset is a subring of R, and in the case of a division ring, a field. Clearly

$$C_R(R) = Z(R).$$

The last ingredient of the proof we need is the class formula for finite groups.
Let G be a finite group. For $g \in G$, denote by $C(g)$ the conjugacy class of g, that is the set of all elements of the form $h^{-1}gh$, where $h \in G$. Then G is a disjoint union of conjugacy classes. We have $\#C(g) = \frac{\#G}{\#C_g}$, where C_g is the centraliser subgroup (consisting, as in the case of rings, of all elements that commute with g).

Proof. We want to prove $Z(R) = R$.

Let

$$q = \#Z(R).$$

Since R is a vector space over $Z(R)$,

we have $\#R = q^n$, where n is the dimension of this vector space.
Since R is a division ring, the set $G = R\backslash\{0\}$ is a group. Applying the class formula to this group, we obtain

$$q^n - 1 = \sum_{\text{conjugacy} \ \ classes} \#C(g) = \sum_{\text{conjugacy} \ \ classes} \frac{q^n - 1}{\#C_g}.$$

Let us look closer at this sum. It contains terms corresponding to conjugacy classes consisting of a single element (these are conjugacy classes of nonzero elements from the center) and all other conjugacy classes. Every centraliser C_g of such a conjugacy class, with the zero elements adjoined to it, forms a subring of R containing $Z(R)$, that is a vector space over $Z(R)$. Let n_g be the dimension of that vector space, $n_g < n$. We have

$$q^n - 1 = q - 1 + \sum_{non-central \ \ \text{conjugacy} \ \ classes} \frac{q^n - 1}{q^{n_g} - 1}.$$

It is easy to see that $\frac{q^n-1}{q^{n_g}-1}$ is an integer only if n_g divides n (generally $\gcd(q^n-1, q^k-1) = q^{\gcd(n,k)} - 1$), so in fact not only $\frac{q^n-1}{q^{n_g}-1}$ is an integer, but also $\frac{x^n-1}{x^{n_g}-1}$ is a polynomial with integer coefficients.
As polynomials in $x, x^{n_g} - 1$ and $\Phi_n(x)$ are coprime, so $x^n - 1$ is divisible by their product. This means that in our equality above all terms except for the term $q - 1$ are divisible by $\Phi_n(q)$. Thus $q - 1$ is divisible by $\Phi_n(q)$. But the latter is impossible for $n > 1$: $|q - \eta| > |q - 1|$ for all roots of unity $\eta \neq 1$, so $|\Phi_n(x)| = \prod_\eta |q - \eta| > |q - 1|$. This completes the proof. ■

Remark 3.2.1 *Irreducibility of cyclotomic polynomials, while of crucial importance for Galois Theory, is not really used in our proofs at all.*

Conclusion

We have reached to the end of the thesis: the nth cyclotomic polynomial for any positive integer n is a unique, irreducible polynomial, where there is an important relationship between cyclotomic polynomials and primitive roots of unity. And given its importance, we preferred to choose it from among the topics. We have also tried hard to elaborate and expand the topic, and there are several aspects that researchers will detail and explainin future research.

Bibliography

[1] Roman, S. (2005). Field theory (Vol. 158). Springer Science & Business Media.

[2] C.C. Cheng, J.H. McKay and S.S. Wang, Resultants of cyclotomic polynomials, proc. Amer. Math. Soc. **123** (1995), 1053-1059.

[3] P. Erdos and R.C. Vaughan, Bounds for the r-th coefficients of cyclotomic polynomials, J. London Math. Soc. **8** (1974), 393-400.

[4] D.H. Lehmer, Some properties of the cyclotomic polynomials, j. Math. Anal. Appl. **15** (1966), 105-117.

[5] Gallian, Joseph A. Contemporary Abstract Algebra. 7th ed. Belmont, CA: Books/Cole, Cengage Learning, 2010. Print.

[6] Robbins, Neville. Beginning Number Theory. 2nd ed. Sudbury, Mass.: Jones and Bartlett, 2006. Print.

[7] Goldstein, L. J. (1973). Abstract algebra: a first course. Prentice Hall.

[8] Yimin Ge, Elementary Properties of Cyclotomic polinomials, Mathematical Reflections 2 (2008) 8

[9] Gennady Bachman, On the coefficients of cyclotomic polynomials. Memoirs of the American Mathematical Society 106 (1993), no. 510, 1-80.

[10] G. Bachman. Flat cyclotomic polynomials of order three. Bull. London Math. Soc.,38(1):53-60, 2006. MR2201603 (2006j:11032)

[11] Marion Beiter, the midterm coefficient of the cyclotomic polynomials $F_{pq}(x)$, Amer. Math. Monthly 71 (1964), no. 7, 769-770.

[12] R.P. Brent, On computing factors of cyclotomic polynomials, Math. Comp. 61 (1993), 131-149.

[13] F.E Diederichsen, Uber die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetisher Aquivalenz, Abh. Math. Sem. Univ. Hamburg 13 (1940), 357-412.

[14] Lang, S. (2013). Algebraic number theory (Vol. 110). Springer Science & Business Media.

[15] I. Merzougui, Notions about elliptic curves and their uses in cryptography, Memory of master, University of msila, 2019.

ملخص

في هذه المذكرة، رأينا مفهوم متعدد الحدود الحلقي. لقد تمكنا من دراسة بعض خصائصه، مع التركيز بشكل خاص على عدم قابليته للاختزال وكيفية ارتباطه بالأعداد الأولية. علاوة على ذلك، قدمنا بعض التطبيقات من متعدد الحدود الحلقي أهمها نظرية ديريتشليت حول الأعداد الأولية في التعاقب الحسابي ونظرية ويديربورن الصغيرة.

كلمات مفتاحية

متعدد الحدود الحلقي
التعاقب الحسابي

Abstract

In this memory, we have viewed the concepte of cyclotomic polynddomails. We have managed to study some of its propert ies, specifially focusing on their irreducibility and how dddthey relate to primes. Moreover, we have presented sdome applications of cyclotomic polynomials the most impddortant, Dirichlet's theorem on primes in arithmetic progressions and Wedderburn's little theorem .

Key words :

Cyclotomic Polynomials.
Arithmetic progressions

Résumé

Dans cette mémoire, nous avons vu le concept des polynômes cyclotomiques. Nous avons réussi à étudier certaines de ses propriétés, en se concentrant spécifiquement sur leur irréductibilité et leur relation avec les nombres premiers. De plus, nous avons présenté quelques applications des polynômes cyclotomiques les plus importantes, Théorème de Dirichlet sur les nombres premiers dans les progressions arithmétiques et petit théorème de Wedderburn.

Mot-clés :

Polynômes Cyclotomiques.
Les progressions arithmétiques