THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Galois Theory and Cyclotomic Extensions

Parvinder Singh
Associate Professor, P. G. Department of Mathematics,
S.G.G.S. Khalsa College, Mahilpur (Hoshiarpur), Punjab, India

Abstract:
Gauss was led to his discovery of constructible polygons from $x^n - 1$ over the set Q of rational numbers. Inthis paper we examine that the factors of $x^n - 1$ and to show that how the Galois Theory can be used to determine that regular n-gons are constructible with a straightedge and compass. The irreducible factors of $x^n - 1$ are very important in number theory and in combinatorics.

1. Introduction

The ancient Greeks know that how to construct a regular polygon of 3,4,5,6,8,10 and 15 sides with the help of straightedge and compass and gives a construction of a regular n-gon. They also attempted to construct the polygons of 7, 9, 11, 13, 17, sides but failed. More than 2200 years passed before Gauss, at the age of 19 proved that a regular 17-gon was constructible and short after he solved the problem and said that n-gons are constructible. By this discovery he dedicate his life to mathematics. He was so proud of this accomplishment that he requested that a regular 17-sided polygonbe engraved on his tombstone.

As we know that the complex roots of $x^n - 1 = 0$ are $1, \omega, \omega^2, \omega^3, \ldots\ldots\ldots, \omega^{n-1}$where$\omega = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Thus the splitting field of $x^n - 1$ over Q is Q (ω), and is called the nth Cyclotomic Extension of Q also the irreducible factors of $x^n - 1$ over Q are called the Cyclotomic Polynomials.

As $\omega = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ generates a cyclic group oforder n under multiplication, the generators of $<\omega>$ are of the form $\omega^k$where $1 \leq k \leq n$ and (n,k) =1. These generators are called the Primitive nth roots of unity. Let $\phi(n)$ denote the number of positive integers less than or equal to n and relatively prime to n.

2. Definition

For any positive integer n, let $\omega_1, \omega_2, \ldots\ldots, \omega_{\phi(n)}$ denote the primitive nth roots of unity. The nth Cyclostomes Polynomial over Q is the polynomialΦ_n(x) = $(x - \omega_1)\,(x - \omega_2) \ldots.(x - \omega_{\phi(n)})$.

2.1. Example 1

Let Φ_1(x) = x -1, Since 1 is the only zero of the equation x -1= 0 and let Φ_2(x) = x +1 then zeroes of x^2 -1 =0 are 1 and -1 and -1 is the only primitive root.

If Φ_3(x) = $(x - \omega)(x - \omega^2)$ where $\omega = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ = (-1 +$i\sqrt{3}$)/2 and by direct calculations we can show that Φ_3(x) = x^2+ x +1. Also the roots of x^4 -1 = 0 are ± 1 *and* $\pm i$. Also $\pm i$ are primitive roots,Φ_4(x) =$(x - i)(x + i) = x^2$+ 1.

3. Theorem

For every positive integer n, x^n -1 = $\prod_{d\backslash n} \Phi_4$(x) where the product runs over all positive divisors d of n.

3.1. Proof

As both of the polynomials in the statement are monic so it is suffices to prove that they have the same zeros and all zeros have the multiplicity 1. Let$\omega = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Then $<\omega>$ is a cycle group order n and contains all n nth roots of unity. Then for each j the order ω^j is denoted by $|\omega^j|$ divides n so that $(x - \omega^j)$ appears as a factor in$\Phi_{|\omega^j|}$(x). Conversely if $(x - \alpha)$ is a factor of Φ_d(x) for some divisor d of n then α^d = 1 and hence α^n = 1. Hence$(x - \alpha)$ is a factor of $x^n - 1$. Finally since no root of $x^n - 1 = 0$ can be a root of Φ_d(x) for two different values of d which provestheresult.

4. Theorem

For every positive integer n,Φ_n(x) has integral coefficients.

4.1. Proof

If n = 1 the case is trivial hence by induction principle we may assume that $g(x) = \prod_{\substack{d\backslash n \\ d<n}} \Phi_d(x)$ has integral coefficients, then by theorem 1.3 we have $x^n - 1 = \Phi_n(x)g(x)$ and , as $g(x)$ is monic we may carry out the division in Z[x] and can say that $\Phi_n(x) \in$ Z[x] Hence proved the Φ_n(x) has integral coefficients.

5. Theorem

The Cyclotomic Polynomial Φ_n(x)is irreducible over the ring of integers Z.

5.1. Proof

Let $f(x) \in$ Z[x] be a monic irreducible factor of Φ_n(x). As Φ_n(x) is monic and has no multiple zeros is suffices to show that every root of Φ_n(x) is a root of $f(x)$. As Φ_n(x) divides $x^n - 1$ in Z[x], we can write $x^n - 1$ = f(x)$g(x)$where $g(x)$ ∈Z[x]. Let ω be a primitive nth root of unity that is a root of $f(x)$.Then $f(x)$ is a minimal polynomial over Q. Let p be any prime number that does not divide n. Then ω^p is also the primitive nth root of unity and hence $(\omega^p)^n$ - 1 = $f(\omega^p)$ $g(\omega^p)$ = 0 so that $f(\omega^p) = 0$ *or* $g(\omega^p) = 0$. suppose that $(\omega^p) \neq 0$, then $g(\omega^p) = 0$ therefore ω is a root of $g(x^p) = 0$, hence f(x) divides $g(x^p)$ in Z[x]. Since f(x) is monic f(x)actually divides $g(x^p)$ in Z[x], so $g(x^p) = f$(x)h(x) where h(x) ∈ Z[x]. Now let $g^/(x)$, $f^/(x)$ and $h^/(x)$ denote the polynomials in $Z_p[x]$ obtained from g(x), f(x)and h(x)respectively, by reducing each coefficient modulo p. This reduction is a ring homomophism from Z[x] to $Z_p[x]$, we have $g^/(x^p) = f^/(x)h^/(x)$ in $Z_p[x]$ then we have $(g^/(x))^p$= $g^/(x^p)$= $f^/(x)h^/(x)$and since $Z_p[x]$ is a unique factorization domain then it follows that $g^/(x)$ is a factor of $f^/(x)$ in $Z_p[x]$.Hence we may write $f^/(x)$ = k(x) $g^/(x)$ where k(x) ∈ $Z_p[x]$.Then keeping $x^n - 1$ as a member of $Z_p[x]$. We have $x^n - 1$= $f^/(x)g^/(x)$ = k(x)$(g^/(x))^2$. In particular, ω^p is a multiple root of $x^n - 1$ in $Z_p[x]$. As p does not divide n, the derivative nx^{n-1} of $x^n - 1$ is not 0 and so nx^{n-1} and $x^n - 1$ do not have a common factor of positive degree in $Z_p[x]$. Which contradicts criterion for multiple roots so we must have $f(\omega^p)$= 0.Now we reformulate what we have thus far proved as follows: If β is any primitive nth root of unity that is a root of f(x) and p is any prime that does not divide n, then β^p is a root of f(x) . Let k be any integer between 1 and n that is relatively prime to n. Then we can write k = $p_1p_2 \ldots\ldots p_t$ where p_i is a prime that does not divide n. Then it follows that each ofω, ω^{p_1},$(\omega^{p_1})^{p_2}$,………, $(\omega^{p_1p_2\ldots\ldots p_{k-1}})^{p_t} = \omega^k$ is a root of f(x). Since every root of Φ_n(x) has the form ω^k where k is between 1 and n and is relatively prime to n, we proved that every root of Φ_n(x) is a root of f(x). This completes the proof.

Further we have to determine the Galois group of the Cyclotomic extensions of Q.

6. Theorem

Let ω be a primitive nth root of unity then Gal (Q$(\omega)/Q$) $\approx U(n)$.

6.1. Proof

Since 1, ω, ω^2,…..ω^{n-1} are all the n nth roots of unity, Q(ω) is the splitting field of x^n-1 over Q. For each k in U(n), ω^k is primitive nth root of unity then there is a field automorphism of Q(ω), which is denoted by ϕ_k that carries $\omega$to ω^k and act as the identity on Q. Moreover these are all the automorphisms of Q(ω), since any automorphism maps a primitive nth root of unity to a primitive nth root of unity. Observe that for every r, s ∈ U(n), $(\phi_r\phi_s)(\omega) = \phi_r(\omega^s) = (\phi_r(\omega))^s = (\omega^r)^s = \omega^{rs} = \phi_{rs}(\omega)$. Which shows that the mapping from U(n) onto Gal(Q$(\omega)/Q$) given by k → ϕ_k is a group homomorphism. Clearly the mapping is an isomorphism since $\omega^r \neq \omega^s$ when r, s ∈ U(n), and r ≠ s , Hence the proof.

→ Example 2 : Let $a = \cos\frac{2\pi}{9} + i \sin\frac{2\pi}{9}$ and b $= \cos\frac{12\pi}{15} + i \sin\frac{12\pi}{15}$ then Gal(Q$(a)/Q$) $\approx U(9) \approx z_6$And Gal(Q$(b)/Q$) $\approx U(15) \approx z_4 \oplus z_2$.

→ Construction of Regular n-Gons: Byapplying both the of Cyclotomic Extensions and Galios Theory we can determine that regular n-Gons are constructible with a straightedge and compass. This can be proved as under:

7. Lemma

Let n be a positive integer and let $\omega = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$.

Then Q $(\cos\frac{2\pi}{n}) \subseteq$ Q(ω).

7.1. Proof

It can be observed that $(\cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n})(\cos\frac{2\pi}{n} - i \sin\frac{2\pi}{n}) = \cos^2\frac{2\pi}{n} + \sin^2\frac{2\pi}{n} = 1$ then we have $(\cos\frac{2\pi}{n} - i \sin\frac{2\pi}{n}) = \frac{1}{\omega}$, Moreover $(\omega + \frac{1}{\omega})$ / 2 = $(2\cos\frac{2\pi}{n})$ /2 = $\cos\frac{2\pi}{n}$. Hence$\cos\frac{2\pi}{n} \in$ Q(ω).

8. Theorem
The necessary and sufficient condition that it is possible to construct the regular n-gon with a straightedge and compass if nis of the form $2^k p_1 p_2 \dots . p_t$ where k ≥ 0 and p_i are all distinct primes of the form 2^m+ 1.

8.1. Proof: The Condition is Necessary
If it is possible to construct a regular n-gon then we can construct the angle $2\pi/n$ and therefore the number $\cos\frac{2\pi}{n}$. As we know that $\cos\frac{2\pi}{n}$ is constructible only if [Q(cos($\frac{2\pi}{n}$)): Q] is a power of 2. To determine when this is so we will use Galois theory as:
Let $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Then |Gal(Q($\omega$)/Q| = [Q($\omega$): Q] = $\phi(n)$. Then by the above lemma Q(cos($\frac{2\pi}{n}$)) ⊆ Q(ω) and we know that [Q(cos($\frac{2\pi}{n}$)): Q] = |Gal(Q(ω)/Q|/|Gal(Q(ω)/Q (cos($\frac{2\pi}{n}$)))| = $\phi(n)$/Gal(Q(ω)/ Q (cos($\frac{2\pi}{n}$))|.
Here the element σ of Gal(Q(ω)/ Q) have the property that $\sigma(\omega) = \omega^k$ for 1≤ $k \leq n$. That is σ((cos$\frac{2\pi}{n}$ + i sin$\frac{2\pi}{n}$) = (cos$\frac{2\pi k}{n}$ + i sin$\frac{2\pi k}{n}$). If such a σ belongs to Gal((Q(ω)/ Q(cos$\frac{2\pi}{n}$)), then we must have cos($\frac{2\pi k}{n}$) = cos($\frac{2\pi}{n}$). Clearly this holds only when k = 1 and k = n-1. So
| Gal((Q(ω)/ Q(cos$\frac{2\pi}{n}$))| = 2 and therefore [Q(cos($\frac{2\pi}{n}$) : Q] = $\phi(n)/2$. Thus if an n-gon is constructible then $\phi(n)/2$ must be a power of 2. Of course this implies that $\phi(n)$ is a power of 2. Hence write n = $2^k p_1^{n_1} p_2^{n_2} \dots . . p_t^{n_t}$ where k ≥ 0, thep_i are distinct odd primes and the n_i> 0. Then $\phi(n)$ = |U(n)| = |U(2^k)|| U($p_1^{n_1}$)||U($p_2^{n_2}$)|……… |U($p_t^{n_t}$)| = $2^{k-1} p_1^{n_1-1}(p_1-1) p_2^{n_2-1}(p_2-1) \dots . . p_t^{n_t-1}(p_t-1)$ must be a power of 2. This implies that each n_i =1 and each $p_i - 1$ is a power of 2. This completes the proof that the condition is necessary.

8.2. The Condition is Sufficient
Suppose that n is of the form $2^k p_1 p_2 \dots . p_t$ where k ≥ 0 and p_i are all distinct primes of the form 2^m+ 1 and let $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Then Q ($\omega$) is a splitting field of an irreducible polynomial over Q and therefore , by Fundamental Theorem of Galois Theory, $\phi(n)$= [(Q(ω): Q] = |Gal(Q(ω)/ Q|. Since $\phi(n)$ is a power of 2 and Gal(Q(ω)/ Q is an Abelian group, it follows that by the Principle of Induction there exist a series of subgroups $H_0 \subset H_1 \subset \cdots \subset H_t$ = Gal(Q(ω)/ Q where H_0 is the identity of the group and H_1 is the subgroup of Gal(Q(ω)/ Q of order 2 that fixes (cos($\frac{2\pi}{n}$)), and |H_{i+1}:H_i| = 2 for i = 0,1,2,……,t-1. By Fundamental Theorem of Galois Theory we have a series of subfields of the real numbers Q =$E_{H_t} \subset E_{H_{t-1}} \subset \cdots \dots \subset E_{H_1}$=Q (cos$\frac{2\pi}{n}$)$where$ [$E_{H_{i-1}}$:E_{H_i}]= 2. So for each i we can chose $\beta_i \in E_{H_i}$so that E_{H_i}= $E_{H_{i-1}(\beta_i)}$. Then β_i is the root of the polynomial $x^2 + b_i$x + $c_i \in E_{H_{i-1}}$[x] and it follows that $E_{H_i} = E_{H_{i-1}}(\sqrt{{b_i}^2} - 4c_i)$. Hence it follows that every element of Q(cos$\frac{2\pi}{n}$) is constructible.

9. References

i. Bryan, B. (1973). Cyclotomic fields and Kummer extensions, in Cassels, J.W.S. and Frohlich, A. (edd), Algebraic number theory, Academic Press, Chap.III, pp. 45–93.
ii. Daniel A. M. (1977).Number Fields, third edition, Springer-Verlag.
iii. Lam, T.Y. (1991). A First Course in Non commutative Rings, Springer-Verlag, New York.
iv. Lam, T. Y., & Cheung, K. H. (1996).On the cyclotomic polynomialpq (T), Amer. Math. Monthly.
v. Lang,S.(1990). Cyclotomic Fields I and II, Combined second edition. With an appendix by Karl Rubin. Graduate Texts in Mathematics, 121. Springer-Verlag, New York.
vi. Lawrence, W.C. (1997), Introduction to Cyclotomic Fields, Graduate Texts in Mathematics,83 (2ed.), New York: Springer-Verlag.