NAP 2018 Module-V:Applications of Galois theory Lecture 3: July 11, 2018 (Wednesday)

Definition 1. A primitive n-th root of unity is an element of order n in the group $F^\times$.

Question 2. When does such an element exists ?

Proposition 3. *Let F be a field. Assume that either the characteristic of F is* 0 *or the characteristic of F is p (a prime number) which does not divide n. Let E be the splitting field of the polynomial* $X^n - 1$*. Then*

(a) *There exists a primitive n-th root of unity in E.*
(b) *Let* ζ *be a primitive n-th root of unity. Then* $E = F[\zeta]$*.*
(c) *There exists an injective group homomorphism, say,* $\theta : Gal(E/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

Recall that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of invertible elements (under multiplication) in $\mathbb{Z}/n\mathbb{Z}$, i, e.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \text{ there exists } \bar{b} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \bar{a} \cdot \bar{b} = 1\}$$

which is a group under multiplication. In fact, $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$.

Proof. (a) The polynomial $X^n - 1$ has distinct root. (Recall that a polynomial $f(X)$ has repeated roots if and only if $f(X)$ and $f'(X)$ have a common root). Further note that $G := \{a \in E : a^n = 1\} \subset E^\times$ is a finite subgroup of the multiplicative group $E^\times$. Recall from (Module 1) that a finite subgroup of $E^\times$ is cyclic. Therefore G is cyclic.
(b) The roots of $X^n - 1$ are $\zeta, \zeta^2, \cdots, \zeta^{n-1}, 1$. Therefore $E = F[\zeta]$.
(c) Let $\sigma \in Gal(E/F)$. Then $\sigma : E \to E$ is an automorphism. Since σ maps ζ to a root of $X^n - 1$, $\sigma(\zeta) = \zeta^i$ for some i. Since σ is an automorphism, $E = F[\zeta^i]$ which implies that $(i, n) = 1$. Thus $\bar{i} \in (\mathbb{Z}/n\mathbb{Z})^\times$. This defines a map, say, $\theta : Gal(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ where $\sigma \mapsto \bar{i}$ as above. Check that θ is a group homomorphism, i.e. $\theta(\sigma_1\sigma_2) = \theta(\sigma_1)\theta(\sigma_2)$.
Claim: The homomorphism θ is injective. We have to prove, if $\theta(\sigma) = 1$ for some $\sigma \in Gal(E/F)$ then $\sigma = id$. For this, just notice that if $\theta(\sigma) = 1$ then $\sigma(\zeta) = \zeta$. Since $E = F[\zeta]$, $\sigma = id$.

□

Remark 4. The map θ in the above proposition need not be surjective.

Example 5. (1) For example, if $F = \mathbb{C}$ then for any n we have $E = \mathbb{C}$. Therefore $\mathrm{Gal}(E/F) = \{1\}$. For $n > 2$ the order of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is > 1. Then θ can not be surjective.
(2) Take $F = \mathbb{R}$. If $n = 2$ then $E = \mathbb{R}$. Both the groups $Gal(E/F)$ and $(\mathbb{Z}/2\mathbb{Z})^\times$ are trivial. Then θ is onto (obvious !).
(3) Take $F = \mathbb{R}$. If $n = 3$ then $E = \mathbb{C}$ and $Gal(E/F) = \{1, -1\}$ a group of order two. Moreover $(\mathbb{Z}/3\mathbb{Z})^\times$ is also a group of order two. In this case, θ is surjective.
(4) Let $F = \mathbb{R}$ and $n > 3$. Then $E = \mathbb{C}$ and $Gal(E/F) = \{1, -1\}$. Therefore the map θ need not be surjective.

We prove that if $F = \mathbb{Q}$, then θ is surjective and hence is an isomorphism.

Remark 6. Consider $X^n - 1 \in \mathbb{Q}[X]$. This polynomial has some obvious factors. For example, if $d|n$ then $X^d - 1$ divides $X^n - 1$. In fact, if $n = qd$ for some $q \in \mathbb{N}$, then

$$X^n - 1 = (X^d - 1)(X^{n-d} + X^{n-2d} + \cdots + X^{n-(q-1)d} + 1).$$

Definition 7 (Cyclotomic polynomial)**.** For a positive integer n we define the *n-th cyclotomic polynomial* $\Phi_n(X) := \prod(X - \zeta)$ where the product ranges over primitive n-th roots of unity.

Property 1: $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Proof. First note that if a is a root of $X^n - 1$ in $E = F[\zeta]$, then order of a (in $\{\alpha : \alpha^n = 1\} \subseteq E^\times$) divides n. Thus every root of $X^n - 1$ is a root of exactly one $\Phi_d(X)$ for some $d|n$. □

Property 2: $\Phi_n(X) \in \mathbb{Z}[X]$.

Proof. First we observe that $\Phi_n(X) \in \mathbb{Q}[X]$. By Property 1, we have

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d \neq n} \Phi_d(X)}.$$

Therefore by induction on n, $\Phi_n(X) \in \mathbb{Q}[X]$. Write $X^n - 1 = \Phi_n(X)h(X)$ for some $h(X) \in \mathbb{Q}[X]$. Since $X^n - 1 \in \mathbb{Z}[X]$, $\Phi_n(X) \in \mathbb{Z}[X]$. (Recall that every monic factor in $\mathbb{Q}[X]$ of a polynomial in $\mathbb{Z}[X]$ lies in $\mathbb{Z}[X]$.) □

Property 3: The degree of $\Phi_n(X)$ is $\phi(n)$ where ϕ denotes the Euler's phi function. (Recall that $\phi(1) = 1, \phi(2) = 1, \phi(p) = p - 1$ for a prime number p.)

Proof. Since $\Phi_n(X)$ is product of $(X - \zeta^I)$ for all $I \leq i \leq n$ and $\gcd(i, n) = 1$. Then the number of linear factors is the degree of $\Phi_n(X)$ which is by definition $\phi(n)$. □

Example 8. (a) $\Phi_1(X) = X - 1$.
(b) $\Phi_2(X) = X + 1$.
(c) $\Phi_3(X) = (X - \omega)(X - \omega^2)$ where ω is the cube root of unity. On the other hand, $X^3 - 1 = \Phi_1(X)\Phi_3(X) = (X - 1)\Phi_3(X)$. Thus $\Phi_3(X) = X^2 + X + 1$.
(d) $\Phi_4(X) = (X - i)(X + i) = X^2 + 1$.
(e) $\Phi_6(X) = (X - \zeta)(X - \zeta^5) = X^2 - X + 1$.

These examples suggest that one can compute cyclotomic polynomial recursively (One can write a program in computer or type polycyclo(n,X) in PARI!)

If $n = p$ is a prime. Only factors of p are 1 and p. Then

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

Recall that $\Phi_p(x)$ is an irreducible polynomial (use Eisenstein criterion). In the following theorem we prove that $\Phi_n(X)$ in irreducible for every $n \in \mathbb{N}$.

Theorem 9. *The cyclotomic polynomial $\Phi_n(X) \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Q}[X]$.*

Proof. Let ζ be a primitive n-th root of unity and $f(X)$ be the minimal polynomial for ζ over $\mathbb{Q}$. We show that $\Phi_n(X) = f(X)$ and hence $\Phi_n(X)$ is irreducible. First we prove if p does not divide n, then $f(\zeta^p) = 0$. Since $\Phi_n(\zeta) = 0$, $f(X)$ divides $\Phi_n(X)$ in $\mathbb{Q}[X]$. Write $\Phi_n(X) = f(X)g(X)$ for some $g(X) \in \mathbb{Q}[X]$. Since $f(X)$ and $\Phi_n(X)$ both are monic polynomials and $\Phi_n(X) \in \mathbb{Z}[X]$, $f(X), g(X) \in \mathbb{Z}[X]$. Suppose $f(\zeta^p) \neq 0$. Since $\Phi_n(\zeta^p) = 0$, $g(\zeta^p) = 0$. In other words, $g(X^p)$ and $f(X)$ have a common factor, namely $X - \zeta$ in $(F[\zeta])[X]$. Let $h(X) = gcd(g(X^p), f(X))$ in $\mathbb{Q}[X]$. Since the gcd of $g(X^p)$ and $f(X)$ is same in $\mathbb{Q}[X]$ and in $(\mathbb{Q}[\zeta])[X]$, degree of $h(X)$ is ≥ 1. Morover, $h(X) \in \mathbb{Z}[X]$.

Therefore $\bar{f}(X)$ and $\bar{g}(X^p)$ have a common factor of degree ≥ 1 in $\mathbb{Z}/p\mathbb{Z}$ where $^{-}$denotes the image of a polynomial in the quotient ring $\mathbb{Z}/p\mathbb{Z}$. Since $\bar{g}(X^p) = (\bar{g}(X))^p$, $\bar{f}(X)$ and $\bar{g}(X)$ have a common factor of degree ≥ 1. Since $\overline{\Phi}_n(X)$ divides $X^n - 1$ in $(\mathbb{Z}/p\mathbb{Z})[X]$, this implies that $X^n - 1$ has a repeated root in $\mathbb{Z}/p\mathbb{Z}$, a contradiction. Thus $f(\zeta^p) = 0$.

Let $i \in \mathbb{N}$ with with $\gcd(i,n) = 1$. Write $i = p_1^{n_1} \dots p_k^{n_k}$. Then clearly, p_i do not divide n for all i. By above argument, $f(\zeta^{p_1}) = 0$. Since ζ^{p_1} is a primitive n-th root of unity, using the above argument again we get $f(\zeta^{p_1^2}) = 0$. By repeating this argument we get that $f(\zeta^i) = 0$. Hence $f(X) = \Phi_n(X)$.

□