Lecture 18 : Cyclotomic Extensions II

Objectives

(1) Discriminant of $\Phi_p(x)$.
(2) Subfields of $\mathbb{Q}(\zeta_p)$.
(3) Kronecker-Weber Theorem for quadratic extensions of $\mathbb{Q}$.
(4) Algorithm for construction of primitive elements of subfields of $\mathbb{Q}(\zeta_p)$.
(5) Subfields of $\mathbb{Q}(\zeta_7)$, $\mathbb{Q}(\zeta_{13})$ and $\mathbb{Q}(\zeta_{17})$.

Keywords and phrases : Discriminant of $\Phi_p(x)$, Kronecker-Weber Theorem, subfields of $\mathbb{Q}(\zeta_p)$.

19. Subfields of $\mathbb{Q}(\zeta_p)$

A celebrated theorem of Kronecker and Weber states that a Galois extension E of $\mathbb{Q}$ with abelian Galois group is contained in a cyclotomic extension (an extension of $\mathbb{Q}$ obtained by adjoining roots of unity.) We will prove this theorem for quadratic extensions of $\mathbb{Q}$. For this purpose, we show that the square root of the discriminant of $\Phi_p(x)$ is a primitive element of the unique intermediate subfield of K of $\mathbb{Q}(\zeta_p)$ so that $[K:\mathbb{Q}] = 2$.

Lemma 19.1. *Let p be an odd prime. Then disc $(\Phi_p(x)) = (-1)^{\binom{p}{2}} p^{p-2}$.*

Proof. Let ζ_p be a primitive p^{th} root of unity. Since $x^p - 1 = \Phi_p(x)(x-1)$, and $px^{p-1} = \Phi_p(x) + (x-1)\Phi_p(x)$, we have for each $i = 1, 2, \ldots, p-1$,

$$p(\zeta_p^i)^{p-1} = (\zeta_p^i - 1)\Phi_p(\zeta_p^i).$$

Therefore

$$\begin{aligned} \prod_{i=1}^{p-1} \Phi_p(\zeta_p^i) &= \prod_{i=1}^{p-1} p(\zeta_p^i)^{p-1}/(\zeta_p^i - 1) \\ &= \frac{p^{p-1}}{\prod_{i=1}^{p-1}(\zeta_p^i - 1)} = \frac{p^{p-1}}{(-1)^{p-1}\Phi_p(1)} = p^{p-2}. \end{aligned}$$

Using the formula for discriminant in terms of derivatives, we get

$$\text{disc } (\Phi_p(x)) = (-1)^{\binom{p}{2}} p^{p-2}$$

□

Proposition 19.2. *The field $\mathbb{Q}(\zeta_p)$ contains a unique quadratic extension of $\mathbb{Q}$, namely*

$$\mathbb{Q}\left(\sqrt{\ disc\ (\Phi_p(x))}\right) = \mathbb{Q}\left(\sqrt{(-1)^{\binom{p}{2}}p}\right)$$

which is real if $p \equiv 1 (mod\ 4)$ and complex if $p \equiv 3 (mod\ 4)$.

Proof. The Galois group G of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is cyclic of order $p-1$. Hence there is a unique subgroup of G having index 2. Thus there is a unique subfield of $\mathbb{Q}(\zeta_p)$ which is a quadratic extension of $\mathbb{Q}$. As $\sqrt{\text{disc } (\Phi_p(x))} \in \mathbb{Q}(\zeta_p)\backslash\mathbb{Q}$ it generates the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$. □

Corollary 19.3. *Every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

Proof. If $p \equiv 3 (mod\ 4)$, then $\mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\zeta_p)$ and if $p \equiv 1 (mod\ 4)$ then $\mathbb{Q}(\sqrt{p}) \subseteq Q(\zeta_p)$. A quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{d})$ where d is a squarefree integer. Suppose $d = \pm p_1 p_2 \dots p_r$ where $p_1, p_2, \dots, p_r$ are distinct primes. Then $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_r}, i)$.

□

Proposition 19.4. *Let $L \subset \mathbb{Q}(\zeta_p)$ be a subfield with $[\mathbb{Q}(\zeta_p) : L] = 2$. Then*

$$L = Q(\zeta_p + \zeta_p^{-1}).$$

Proof. As ζ_p is a root of $x^2 - (\zeta_p + \zeta_p^{-1})x + 1 = 0$, $\left[\mathbb{Q}(\zeta_p) : Q(\zeta_p + \zeta_p^{-1})\right] \leq 2$. Since $L = Q(\zeta_p + \zeta_p^{-1}) \subseteq \mathbb{R}$, we conclude that $[\mathbb{Q}(\zeta_p) : L] = 2$. □

Proposition 19.5. *Let p be a prime number. Let ζ be a primitive p^{th} root of unity. Let H be a subgroup of $G = G(\mathbb{Q}(\zeta)/\mathbb{Q}) = U(p)$. Put $\beta_H = \sum_{\sigma \in H} \sigma(\zeta)$. Then*

$$E^H = \mathbb{Q}(\beta_H).$$

Proof. Let $\tau \in H$. Since H is finite, $H = \{\tau\sigma \mid \sigma \in H\}$. Hence $\tau(\beta_H) = \beta_H$ for all $\tau \in H$. Hence $\mathbb{Q}(\beta_H) \subseteq \mathbb{Q}(\zeta)^H$. Let $\tau \notin H$. We show that $\tau(\beta_H) \neq \beta_H$. The set

$$B = \{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$$

is a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}(\zeta)$. If $\tau(\beta_H) = \beta_H$ then $\zeta = \tau\sigma(\zeta)$ for some $\sigma \in H$. Hence $\tau\sigma = 1$ and so $\tau^{-1} = \sigma$. Therefore $\tau \in H$ which is a contradiction. If $\mathbb{Q}(\beta_H) \neq \mathbb{Q}(\zeta)^H$, then by FTGT, there is a subgroup $M > H$ such that $\mathbb{Q}(\beta_H) = \mathbb{Q}(\zeta)^M \subsetneq \mathbb{Q}(\zeta)^H$. Hence β_H is fixed by an element $\tau \in M \setminus H$. This is a contradiction.

□

Example 19.6. Let $p = 7$ and $\zeta_7 = w$. Then $\left[\mathbb{Q}(w + w^{-1}) : \mathbb{Q}\right] = 3$ Let us find the irreducible polynomial of $w + w^{-1} = w + w^6$. To do this find the orbit of $w + w^6$ under the action of the Galois group $G = G(\mathbb{Q}(w)/\mathbb{Q})$. G is is generated by the automorphism $\sigma(w) = w^2$. Hence The orbit of $w + w^6$ under the action of G is $\{\beta_1 = w + w^6, \beta_2 = w^2 + w^5, \beta_3 = w^4 + w^3\}$. Hence

$$\text{irr } (w + w^6, \mathbb{Q}) = \prod_{i=1}^{3}(x - \beta_i) = x^3 + x^2 - 2x - 1.$$

Example 19.7. Put $\zeta_{13} = \zeta$. We list all subfields of $E = \mathbb{Q}(\zeta)$ by using the procedure in the proposition above. Since Galois group G of the Galois extension $E/\mathbb{Q}$ is cyclic of oder 12 it has proper subgroups of orders $2, 3, 4$, and 6. The automorphism $\sigma(\zeta) = \zeta^2$ generates G. The action of powers of σ on ζ is described in the table:

i	1	2	3	4	5	6	7	8	9	10	11
$\sigma^i(\zeta) =$	ζ^2	ζ^4	ζ^8	ζ^3	ζ^6	ζ^{12}	ζ^{11}	ζ^9	ζ^5	ζ^{10}	ζ^7

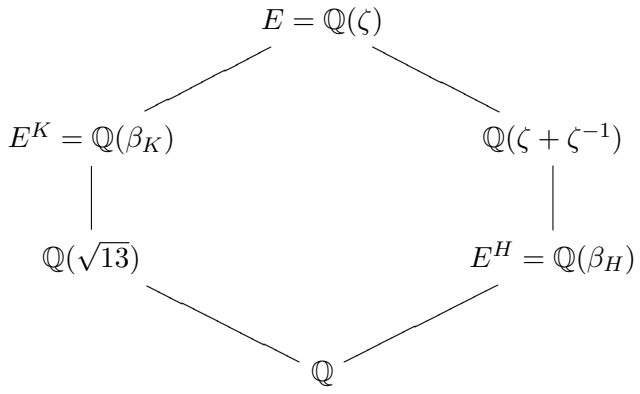
The unique quadratic extension of $\mathbb{Q}$ in E is $\mathbb{Q}(\sqrt{13})$. The unique subfield of degree 6 is $\mathbb{Q}(\zeta + \zeta^{12})$. The subgroup H of oder 4 is generated by σ^3. Hence $H = \{\sigma^3, \sigma^6, \sigma^9, id\}$. Hence a primitive element of the degree 3 extension of $\mathbb{Q}$ in E is

$$\beta_H = \zeta + \sigma^3(\zeta) + \sigma^6(\zeta) + \sigma^9(\zeta) = \zeta + \zeta^8 + \zeta^{12} + \zeta^5.$$

The subgroup K of G of order 3 is generated by σ^4. Hence a primitive element of $\mathbb{Q}(\zeta)^K$ is

$$\beta_K = \zeta + \sigma^4(\zeta) + \sigma^8(\zeta) = \zeta + \zeta^3 + \zeta^9.$$

Hence the poset of intermediate subfields of $\mathbb{Q}(\zeta)$ is



Example 19.8. Let E be the splitting field of $x^{17} - 1$ over $\mathbb{Q}$ generated by a primitive seventeenth root z of 1. So $\text{irr}(z, \mathbb{Q}) = x^{16} + x^{15} + \cdots + x + 1$ and $E = \mathbb{Q}(z)$. Therefore $[E : \mathbb{Q}] = 16$. Thus $|G(E/\mathbb{Q})| = |U(17)| = 16$.

The multiplicative group of units mod 17 can be generated by $3+(17)$. Thus $\eta : z \to z^3$ is a generator of $G(E/\mathbb{Q}) = \{\eta, \eta^2, \ldots, \eta^{16} = 1\}$. The subgroups of G and their orders are:

$$G = G_1 = \langle \eta \rangle \supset G_2 = \langle \eta^2 \rangle \supset G_3 = \langle \eta^4 \rangle \supset G_4 = \langle \eta^8 \rangle \supset \{id\}$$

$$|G_1| = 16, \;\; |G_2| = 8, \;\; |G_3| = 4, \text{ and } |G_4| = 2.$$

The chain of intermediate subfields is:

$$E^G = \mathbb{Q} \subset E^{G_2} \subset E^{G_3} \subset E^{G_4} \subset E.$$

We determine the generators for these fixed fields. Note that

$$\eta(z) = z^3, \eta^2(z) = z^{3^2}, \ldots, \eta^i(z) = z^{3^i}.$$

Let

$$x_1 = \sum_{i=1}^{8} (\eta^2)^i(z), \;\; y_1 = \sum_{i=1}^{4} (\eta^4)^i(z) \;\text{ and } z_1 = \sum_{i=1}^{2} (\eta^8)^i(z).$$

The fixed fields are

$$E^{G_2} = \mathbb{Q}(x_1) \subset E^{G_3} = \mathbb{Q}(x_1, y_1) \subset E^{G_4} = \mathbb{Q}(x_1, y_1, z_1).$$