Lecture 3

3 Cyclotomic Field

3.1 Root of Unity

- $\zeta_n = e^{2\pi i/n} = \cos 2\pi/n + i \sin 2\pi/n$.
- Cyclotopmic field : $\mathbb{Q}(\zeta_n)$.
- If $d|n$, then $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\zeta_n)$.
- Primitive root of unity : ζ_n^m where $(n, m) = 1$. Then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^m)$.
- Euler function : $\varphi(n) = \#\{m \in \mathbb{Z}\,;\,(n, m) = 1,\ 1 \le m \le n\}$

3.2 Cyclotomic Polynomial

- The cyclotomoic polynomial is a monic polynomial whose roots are primitive roots of unity :
$$\Phi_n(X) = \prod_{1\le m\le n,\,(n,m)=1} (X - \zeta_n^m).$$
- Then,
$$\prod_{d|n} \Phi_d(X) = X^n - 1,$$
and by Möbius inversion formula, we have
$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}, \tag{1}$$
where μ is the Möbius function defined for $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ by
$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^m & \text{if } e_1 = e_2 = \cdots = e_m = 1, \\ 0 & \text{otherwise.} \end{cases}$$
Since the left hand side of (1) is polynomial, the denominator of the right hand side divides the numerator. Also the denominator is monic, it implies that $\Phi_n(X)$ is a integer polynomial.
- **Example :** $\Phi_6(X) = \dfrac{(X^6 - 1)(X - 1)}{(X^3 - 1)(X^2 - 1)} = X^2 - X + 1$

- **Theorem 3.2.1 :** $\Phi_n(X)$ is irreducible over $\mathbb{Q}$. In particular, $\mathrm{Irr}_{\mathbb{Q}}(\zeta_n) = \Phi_n(X)$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

  To show this, we need two lemmas.

- **Lemma 3.2.2 :** Let p be a prime number and $h(X)$ a polynomial with integer coefficients. Then
$$(h(X))^p \equiv h(X^p) \mod p$$

  Proof. Apply induction on the degree of h. If $\deg h = 0$, the assertion is nothing but the Fermat's little theorem. Suppose $h = aX^m + g$ where $\deg g < \deg h$. Then
$$\begin{aligned}(h(X))^p &\equiv a^p X^{pm} + (g(X))^p \mod p\\ &\equiv a(X^p)^m + g(X^p) \mod p\\ &= h(X^p)\end{aligned}$$
  and we are done. $\square$

- **Lemma 3.2.3 :** Let p be a prime number and suppose that $(n, p) = 1$. Then, $X^n - 1$ does not have a multiple root in $\mathbb{F}_p$.

  Proof. Suppose that q is a root of $X^n - 1 = 0$ over $\mathbb{F}_p$. Then $q \not\equiv 0 \mod p$ and we have
$$X^n - 1 \equiv (X - q)(X^{n-1} + qX^{n-2} + \cdots + q^{n-1}) \mod p.$$
  Substituting q in X in the right factor of the right hand side, and we obtain $nq^{n-1} \not\equiv 0 \mod p$ by the assumption. $\square$

- *Proof of* **Theorem 3.2.1**. Let ζ ba a primitive n-th root of unity. Assume that $\Phi_n(X) = g(X)h(X)$ and that g is irreducible and $g(\zeta) = 0$. Choose a prime p such that $(p, n) = 1$. Then since $\Phi_n(\zeta^p) = 0$, either $g(\zeta^p) = 0$ or $h(\zeta^p) = 0$.

  Suppose the later is the case. Then since $h(X^p) = 0$ has a root $x = \zeta$, $h(X^p)$ is divisible by $g(X)$ and hence $h(X^p) = g(X)f(X)$. By Lemma 3.2.2, the left hand side equals $(h(X))^p \mod p$ so that $h(X)$ and $g(X)$ have a common root in $\mathbb{F}_p$. Then since $g(X)h(X) \equiv \Phi_n(X) \mod p$, $\Phi_n(X)$ has a multiple root in $\mathbb{F}_p$. On the other hand, $\Phi_n(X)$ is a factor of $X^n - 1$ over $\mathbb{Q}$, and $X^n - 1$ does not have a multiple root in $\mathbb{F}_p$ by Lemma 3.2.3, and hence so does $\Phi_n(X)$ in $\mathbb{F}_p$. This is a contradiction, and $g(\zeta^p) = 0$. In other word, we have shown that if a primitive root ζ is a root of $g(X)$, then ζ^p is also a root of $g(X)$ privided that $(n, p) = 1$.

  The rest done by induction since all primitive roots are obtained from ζ_n by taking a prime power coprime to n succesively. $\square$

3.3 $\mathbb{Q}(\cos\frac{2m\pi}{n})$

- $\zeta_n^m + \zeta_n^{-m} = 2\cos\frac{2m\pi}{n}$.
- A candidate for the irreducible polynomial of $\cos\frac{2M\pi}{n}$ over $\mathbb{Q}$:

$$\Psi_n(X) = \prod_{1\le m\le n/2,\,(m,n)=1} \left(X - \cos\frac{2m\pi}{n}\right).$$

- **Theorem 3.3.1 :** Let $n = 3$ or $n \ge 5$, m a positive integer such that $(n,m) = 1$. Then, $\Psi_n(X)$ is irreducible over $\mathbb{Q}$. In particular, $\mathrm{Irr}_{\mathbb{Q}}(\cos\frac{2m\pi}{n}) = \Psi_n(X)$ and $[\mathbb{Q}(\cos\frac{2m\pi}{n}) : \mathbb{Q}] = \varphi(n)/2$.

  Proof. Rewriting

$$\begin{aligned}\Phi_n(X) &= \prod_{1\le m\le n/2,(n,m)=1} (X-\zeta_n^m)(X-\zeta_n^{-m}) \\ &= \prod_{1\le m\le n/2,(n,m)=1} (X^2 - 2X\cos\frac{2m\pi}{n} + 1),\end{aligned}$$

  we see that every fundamental symmetric polynomials of

$$\left\{\cos\frac{2m\pi}{n}\ ;\ (n,m) = 1,\ 1 \le m \le n/2\right\}$$

  has value in $\mathbb{Q}$. Thus $\Psi_n(X) \in \mathbb{Q}[X]$.

  Suppose $\Psi_n(X)$ is not irreducible over $\mathbb{Q}$, then the factorization of $\Psi_n(X)$ over $\mathbb{Q}$ implies a factorization of $\Phi_n(X)$ over $\mathbb{Q}$, which is a contradiction. □

3.4 Homework

1. Suppose $n = p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m}$. Show

$$\varphi(n) = n\prod_j \left(1 - \frac{1}{p_j}\right).$$

2. Compute $\Phi_{105}(X)$, and find degree of which 2 appears as a coefficient.
3. Show that if n is odd, then $\Phi_{2n}(X) = \Phi_n(-X)$
4. (1) Show $\sqrt{-7} \in \mathbb{Q}(\zeta_7)$.

   (2) Show $\sqrt{13} \in \mathbb{Q}(\zeta_{13})$.
5. Suppose $p > 2$ is prime. Then $\mathbb{Q}(\zeta_p)$ contains a real quadratic number field if and only if $p \equiv 1 \mod 4$.

6. Suppose $n = 3$ or $n \geq 5$, and show that the constant term of $\Psi_n(X)$ is

$$\begin{cases} 2^{-\varphi(n)/2}p & \text{if } \ n = 4p^e \geq 8 \ \text{ and } p \text{ prime}, \\ 2^{-\varphi(n)/2} & \text{otherwise}. \end{cases}$$

7. (1) Find the order of 2 in $\mathbb{F}_{11}$, and show that $(X^{11} - 1)/(X - 1) \in \mathbb{F}_2[X]$ is irreducible.

   (2) Find the order of 2 in $\mathbb{F}_{17}$, and show that $(X^{17} - 1)/(X - 1) \in \mathbb{F}_2[X]$ factors into the product of two polynomials of degree 8.