## 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 : $\mathbb{Q}\left(\zeta_{n}\right)$.
- If $d \mid n$, then $\mathbb{Q}\left(\zeta_{d}\right) \subset \mathbb{Q}\left(\zeta_{n}\right)$.
- Primitive root of unity : $\zeta_{n}^{m}$ where $(n, m)=1$. Then $\mathbb{Q}\left(\zeta_{n}\right)=\mathbb{Q}\left(\zeta_{n}^{m}\right)$.
- Euler function : $\varphi(n)=\#\{m \in \mathbb{Z} ;(n, m)=1,1 \leq m \leq n\}$


### 3.2 Cyclotomic Polynomial

- The cyclotomoic polynomial is a monic polynomial whose roots are primitive roots of unity :

$$
\Phi_{n}(X)=\prod_{1 \leq m \leq n,(n, m)=1}\left(X-\zeta_{n}^{m}\right)
$$

- Then,

$$
\prod_{d \mid n} \Phi_{d}(X)=X^{n}-1
$$

and by Möbius inversion formula, we have

$$
\begin{equation*}
\Phi_{n}(X)=\prod_{d \mid n}\left(X^{d}-1\right)^{\mu(n / d)} \tag{1}
\end{equation*}
$$

where $\mu$ 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 : $\Phi_{6}(X)=\frac{\left(X^{6}-1\right)(X-1)}{\left(X^{3}-1\right)\left(X^{2}-1\right)}=X^{2}-X+1$
- Theorem 3.2.1 : $\Phi_{n}(X)$ is irreducible over $\mathbb{Q}$. In particular, $\operatorname{Irr}_{\mathbb{Q}}\left(\zeta_{n}\right)=\Phi_{n}(X)$ and $\left[\mathbb{Q}\left(\zeta_{n}\right): \mathbb{Q}\right]=\varphi(n)$.

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

$$
(h(X))^{p} \equiv h\left(X^{p}\right) \quad \bmod p
$$

Proof. Apply induction on the degree of $h$. If $\operatorname{deg} h=0$, the assertion is nothing but the Fermat's little theorem. Suppose $h=a X^{m}+g$ where $\operatorname{deg} g<\operatorname{deg} h$. Then

$$
\begin{aligned}
(h(X))^{p} & \equiv a^{p} X^{p m}+(g(X))^{p} \quad \bmod p \\
& \equiv a\left(X^{p}\right)^{m}+g\left(X^{p}\right) \quad \bmod p \\
& =h\left(X^{p}\right)
\end{aligned}
$$

and we are done.

- 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 $q \not \equiv 0 \bmod p$ and we have

$$
X^{n}-1 \equiv(X-q)\left(X^{n-1}+q X^{n-2}+\cdots+q^{n-1}\right) \quad \bmod p
$$

Substituting $q$ in $X$ in the right factor of the right hand side, and we obtain $n q^{n-1} \not \equiv \equiv$ $0 \bmod p$ by the assumption.

- Proof of Theorem 3.2.1. Let $\zeta$ 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 $\Phi_{n}\left(\zeta^{p}\right)=0$, either $g\left(\zeta^{p}\right)=0$ or $h\left(\zeta^{p}\right)=0$.

Suppose the later is the case. Then since $h\left(X^{p}\right)=0$ has a root $x=\zeta, h\left(X^{p}\right)$ is divisible by $g(X)$ and hence $h\left(X^{p}\right)=g(X) f(X)$. By Lemma 3.2.2, the left hand side equals $(h(X))^{p} \bmod p$ so that $h(X)$ and $g(X)$ have a common root in $\mathbb{F}_{p}$. Then since $g(X) h(X) \equiv \Phi_{n}(X) \bmod p, \quad \Phi_{n}(X)$ 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 $g\left(\zeta^{p}\right)=0$. In other word, we have shown that if a primitive root $\zeta$ is a root of $g(X)$, then $\zeta^{p}$ is also a root of $g(X)$ privided that $(n, p)=1$.

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

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

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

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

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

Proof. Rewriting

$$
\begin{aligned}
\Phi_{n}(X) & =\prod_{1 \leq m \leq n / 2,(n, m)=1}\left(X-\zeta_{n}^{m}\right)\left(X-\zeta_{n}^{-m}\right) \\
& =\prod_{1 \leq m \leq n / 2,(n, m)=1}\left(X^{2}-2 X \cos \frac{2 m \pi}{n}+1\right),
\end{aligned}
$$

we see that every fundamental symmetric polynomials of

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

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 $\geq 3$, then $\Phi_{2 n}(X)=\Phi_{n}(-X)$
4. (1) Show $\sqrt{-7} \in \mathbb{Q}\left(\zeta_{7}\right)$.
(2) Show $\sqrt{13} \in \mathbb{Q}\left(\zeta_{13}\right)$.
5. Suppose $p>2$ is prime. Then $\mathbb{Q}\left(\zeta_{p}\right)$ contains a real quadratic number field if and only if $p \equiv 1 \bmod 4$.
6. Suppose $n=3$ or $n \geq 5$, and show that the constant term of $\Psi_{n}(X)$ is

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

7. (1) Find the order of 2 in $\mathbb{F}_{11}$, and show that $\left(X^{11}-1\right) /(X-1) \in \mathbb{F}_{2}[X]$ is irreducible.
(2) Find the order of 2 in $\mathbb{F}_{17}$, and show that $\left(X^{17}-1\right) /(X-1) \in \mathbb{F}_{2}[X]$ factors into the product of two polynomials of degree 8 .
