Math 361 lecture for Wednesday, Week 4

Cyclotomic fields I

Let

$$\zeta_m = e^{2\pi i/m} = \cos(2\pi/m) + i\sin(2\pi/m),$$

for $m \in \mathbb{Z}_{\geq 2}$, and consider the field $K = \mathbb{Q}(\zeta_m)$. The powers of ζ_m are the *m-th roots of unity*:

$$x^m - 1 = \prod_{k=1}^{m}(x - \zeta^k).$$

Since ζ_m satisfies a monic polynomial with integer coefficients, it is an algebraic integer.

Example 1.

1. **Case $m = 2$.** We have $\zeta_2 = -1$ and $K = \mathbb{Q}$.
2. **Case $m = 3$.** We have

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1 + i\sqrt{3}}{2}$$
$$x^3 - 1 = (x-1)(x^2 + x + 1),$$

   and the minimal polynomial for ζ_3 is $x^2 + x + 1$. So $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.
3. **Case $m = 4$.** We have

$$\zeta_4 = \cos(2\pi/4) + i\sin(2\pi/4) = i$$
$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x-1)(x+1)(x^2+1)$$

   and the minimal polynomial for ζ_4 is $x^2 + 1$. So $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$, also.

Theorem 2. We have

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$$

where ϕ is the Euler totient function:

$$\phi(m) = |\{a : 1 \leq a < m \text{ and } \gcd(a, m) = 1\}| = m \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Further, $\mathfrak{O}_{\mathbb{Q}(\zeta_m)}$ has integral basis $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\phi(m)-1}$, i.e., $\mathfrak{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Q}[\zeta_m]$.

Example 3. Let $m = 4$. Then numbers 1 and 3 are relatively prime to m. Therefore,

$$\phi(4) = 2 = 4\left(1 - \frac{1}{2}\right).$$

The ring of integers in $\mathbb{Q}(i)$ is $\mathbb{Z}[i] = \mathrm{Span}_{\mathbb{Z}}\{1, i\}$.

Our next goal is to prove the above theorem in the case where m is an odd prime. **For the rest of this lecture**, let

$$\zeta = \zeta_p = e^{2\pi i/p}$$

where p is an prime. (In the case $p = 2$, we have $\zeta = 1$ and $\mathbb{Q}(\zeta) = \mathbb{Q}$.)

Minimal polynomial of ζ. We use the following criterion for irreducibility to find the minimal polynomial for ζ.

Theorem 4. (Eisenstein's criterion.) Let

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Suppose there is a prime $q \in \mathbb{Z}$ such that

- $q | a_i$ for $i = 0, 1, \ldots, n-1$,
- $q \nmid a_n$, and
- $q^2 \nmid a_0$.

Then up to a constant factor, f is irreducible in $\mathbb{Z}[x]$ and, hence, f is irreducible in $\mathbb{Q}[x]$.

Proof. See Theorem 1.8 in our text for the (easy) proof. □

Proposition 5. The minimal polynomial for ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proof. First note that

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1},$$

and, thus, all of the p-th roots of unity except 1 are zeros of f. So it remains to show that f is irreducible over $\mathbb{Q}$. For that, it suffices to show that $f(x+1)$ is irreducible since $f(x) = g(x)h(x)$ if and only if $f(x+1) = g(x+1)h(x+1)$. We have

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^p + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{1}x + 1 - 1}{x} \\ &= x^{p-1} + \binom{p}{p-1}x^{p-2} + \binom{p}{p-2}x^{p-3} + \cdots + \binom{p}{1}. \end{aligned}$$

Eisenstein's criterion now applies. Note that $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is divisible by p for $1 \leq k \leq p-1$. □

Corollary 6. We have $[K:\mathbb{Q}] = p-1$ and $\left\{1, \zeta, \ldots, \zeta^{p-2}\right\}$ is a $\mathbb{Q}$-basis for K.

Up to this point we have proved almost all of Theorem 2 for the case where m is prime. The only thing that is left is to show $1, \zeta, \ldots, \zeta^{p-2}$ is a $\mathbb{Z}$-basis $\mathfrak{O}_{\mathbb{Q}(\zeta)}$. For that, we will need to calculate some norms and traces and to prove a useful lemma. The complete proof of this special case of Theorem 2 will then be finished in the next lecture.

Some norms and traces. The minimal polynomial for ζ factors as

$$f(x) = \prod_{i=1}^{n-1}(x - \zeta^i).$$

Therefore, the field embeddings are given by

$$\begin{aligned} \sigma_i \colon K = \mathbb{Q}(\zeta) &\to K \subset \mathbb{C} \\ \zeta &\mapsto \zeta^i. \end{aligned}$$

The field polynomial for $\alpha \in \mathbb{Q}(\zeta)$ is

$$\begin{aligned} f_\alpha(x) &= \prod_{i=1}^{p-1}(x - \sigma_i(\alpha)) \\ &= x^{p-1} - (\sigma_1(\alpha) + + \cdots + \sigma_{p-1}(\alpha))x^{p-2} + \cdots + (-1)^{p-1}\sigma_1(\alpha)\cdots\sigma_{p-1}(\alpha), \end{aligned}$$

and the norm and trace of α are given by certain coefficients of f_α:

$$N(\alpha) = \prod_{i=1}^{p-1}\sigma_i(\alpha), \quad T(\alpha) = \sum_{i=1}^{p-1}\sigma_i(\alpha).$$

In particular, the field polynomial for ζ is its minimal polynomial:

$$f_\zeta(x) = f(x) = \prod_{i=1}^{p-1}(x - \zeta^i) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

from which we see (recalling that p is odd),

$$N(\zeta) = \zeta \cdot \zeta^2 \cdots \zeta^{p-1} = (-1)^{p-1} = 1$$

and

$$T(\zeta) = \zeta + \zeta^2 + \cdots \zeta^{p-1} = -1.$$

By multiplicativity of the norm,

$$N(\zeta^j) = 1$$

for all $j \in \mathbb{Z}$. What about the trace of powers of ζ? First note if $1 \leq i < k \leq p-1$,

$$\sigma_i(\zeta^j) = \sigma_k(\zeta^j) \iff \zeta^{ij} = \zeta^{kj} \iff \zeta^{(i-k)j} = 1 \iff (i-k)j = 0 \bmod p \iff j = 0 \bmod p.$$

Therefore, for $j \neq 0 \bmod p$,

$$\{\sigma_1(\zeta^j), \ldots, \sigma_{p-1}(\zeta^j)\} = \{\zeta, \zeta^2, \ldots, \zeta^{p-1}\},$$

from which it follows that

$$T(\zeta^j) = \sum_{i=1}^{p-1} \sigma_i(\zeta^j) = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1.$$

If $j = 0 \bmod p$, then $\zeta^j = 1$, and $T(1) = \sum_{i=1}^{p-1} \sigma_i(1) = \sum_{i=1}^{p-1} 1 = p-1$.
One last useful calculation:

$$N(1-\zeta) = \prod_{i=1}^{p-1} \sigma_i(1-\zeta) = \prod_{i=1}^{p-1}(1-\zeta^i) = f(1) = \underbrace{1 + \cdots + 1}_{p \text{ times}} = p.$$

To summarize:

Proposition 7. Let $\zeta = e^{2\pi i/p}$. Then

$$\begin{aligned} N(\zeta^j) &= 1 \qquad \text{for all } i \in \mathbb{Z} \\ N(1-\zeta) &= p \end{aligned}$$

and

$$T(\zeta^j) = \begin{cases} -1 & \text{if } j \neq 0 \bmod p \\ p-1 & \text{if } j = 0 \bmod p. \end{cases}$$

A useful lemma. Let $K = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_p$ for an odd prime p. Let $\alpha \in \mathfrak{O}_K$. Then since $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a $\mathbb{Q}$-basis for K, we can write

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

for some unique $a_i \in \mathbb{Q}$. To complete the proof of Theorem 2, we need to show the a_i are integers. We will prove that in the next lecture with the help of the following lemma:

Lemma 8. For $0 \leq k \leq p-2$,

$$T(\alpha\zeta^{-k} - \alpha\zeta) = pa_k \in \mathbb{Z}.$$

Proof. First note that since $\alpha \in \mathfrak{O}_K$, as is $\zeta^{-k} = \zeta^{p-k}$ and ζ, it follows that $\alpha\zeta^{-k} - \alpha\zeta \in \mathfrak{O}_K$ (recall that $\mathfrak{O}_K$ is a ring). Therefore, $T(\alpha\zeta^{-k} - \alpha\zeta)$ is an integer.

We then calculate:

$$\begin{aligned} T(\alpha\zeta^{-k} - \alpha\zeta) &= T(\alpha\zeta^{-k}) - T(\alpha\zeta) \\ &= T(a_0\zeta^{-k} + a_1\zeta^{-k+1} + \cdots + a_k + \cdots + a_{p-2}\zeta^{-k+p-2}) \\ &\quad - T(a_0\zeta + a_1\zeta^2 + \cdots + a_{p-2}\zeta^{p-1}) \\ &= -a_0 - a_1 - \cdots - a_{k-1} + (p-1)a_k - a_{k+1} - \cdots - a_{p-2} \\ &\quad - (-a_0 - a_1 - \cdots - a_{p-2}) \\ &= pa_k. \end{aligned}$$

Note, for instance, that

$$T(a_0\zeta^{-k}) = \sum_{i=1}^{p-1} \sigma_i(a_0\zeta^{-k}) = \sum_{i=1}^{p-1} a_0\sigma_i(\zeta^{-k}) = a_0 \sum_{i=1}^{p-1} \sigma_i(\zeta^{-k}) = a_0 T(\zeta^{-k}) = -a_0$$

since $a_0 \in \mathbb{Q}$ and $-k \neq 0 \bmod p$. □