Math 361 lecture for Friday, Week 4

Cyclotomic fields II

We continue our discussion from last time. Let $\zeta = e^{2\pi i/p}$ where $p \neq 0$ is a prime, and consider the cyclotomic field $K = \mathbb{Q}(\zeta)$. We saw that the minimal polynomial for ζ over $\mathbb{Q}$ is

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

So $[K : \mathbb{Q}] = p - 1$, and the embeddings $K \to \mathbb{Q}$ are given by $\sigma_i \colon \sigma \mapsto \zeta^i$ for $i = 1, \ldots, p-1$. We will need some of the calculations we did last time:

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

and

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

Our goal is to show that

$$\mathfrak{O}_K = \mathbb{Z}[\zeta] = \mathrm{Span}_{\mathbb{Z}}\{1, \zeta, \ldots, \zeta^{p-2}\}.$$

Proof. Let $\alpha \in \mathfrak{O}_K$. Since $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a $\mathbb{Q}$-basis for K, we may write

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

for some unique $a_0, \ldots, a_{p-2} \in \mathbb{Q}$. We must show that $a_i \in \mathbb{Z}$ for all i.

Last time, we showed that $b_i := pa_i \in \mathbb{Z}$ for all i. So it suffices to show that $p | b_i$ for all i. Defining $\lambda = 1 - \zeta$, we have

$$\begin{aligned} p\alpha &= pa_0 + pa_1\zeta + \cdots + pa_{p-2}\zeta^{p-2} \\ &= b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2} \\ &= b_0 + b_1(1 - \lambda) + \cdots + b_{p-2}(1 - \lambda)^{p-2}. \end{aligned}$$

If we expand this last equation as a polynomial in λ, what are the coefficients? The constant coefficient is

$$b_0 + b_1 + \cdots + b_{p-2}.$$

The coefficient of λ is

$$-b_1 - b_2 - \cdots - b_{p-2}.$$

The coefficient of λ^2 is

$$b_2\binom{2}{2} + b_3\binom{3}{2} + \cdots + b_{p-2}\binom{p-2}{2},$$

and so on. In general, for $i = 0, \ldots, p-2$, the coefficient of λ^i is

$$c_i := (-1)^i \sum_{j=i}^{p-2} \binom{j}{i} b_j \in \mathbb{Z}.$$

So we have

$$\begin{aligned} p\alpha &= b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2} \\ &= b_0 + b_1(1-\lambda) + \cdots + b_{p-2}(1-\lambda)^{p-2} \\ &= c_0 + c_1\lambda + \cdots + c_{p-2}\lambda^{p-2}. \end{aligned}$$

By symmetry, since $\zeta = 1 - \lambda$, we have

$$b_i = (-1)^i \sum_{j=i}^{p-2} \binom{j}{i} c_j.$$

Note that p does not divide any $\binom{j}{i}$ appearing in above. Hence, to achieve our goal of proving $p|b_i$ for each i, it suffice to show that $p|c_i$ for each i, which we now do by induction. For the case $i = 0$, we have

$$c_0 := (-1)^0 \sum_{j=0}^{p-2} \binom{j}{0} b_j = b_0 + \cdots + b_{p-2} = p(a_0 + \cdots + a_{p-2}).$$

We can not immediately conclude that $p|c_0$ since all we know about the a_i at this point is that they are rational numbers. However, we can use the fact that since $\alpha \in \mathfrak{O}_K$, we know its trace is an integer. Calculate:

$$\begin{aligned} T(\alpha) &= T(a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}) \\ &= T(a_0) + T(a_1\zeta) + \cdots + T(a_{p-2}\zeta^{p-2}), \end{aligned}$$

and since each σ_i is the identity on $\mathbb{Q}$,

$$T(a_k\zeta^k) = \sum_{i=1}^{p-2} \sigma_i(a_k\zeta^k) = \sum_{i=1}^{p-2} a_i\sigma_i(\zeta^k) = \sum_{i=1}^{p-2} a_k T(\zeta^k).$$

for each $k = 0, \ldots, p-2$. It follows from our earlier trace calculations that

$$\begin{aligned} T(\alpha) &= a_0(p-1) - a_1 - \cdots - a_{p-2} \\ &= pa_0 - a_0 - a_1 - \cdots - a_{p-2} \\ &= b_0 - (a_0 + \cdots + a_{p-2}). \end{aligned}$$

Since $T(\alpha)$ and b_0 are integers, so is $a_0 + \cdots + a_{p-2}$. Thus, we may finally conclude that $p|c_0$.

We proceed with the induction step. Let $1 \leq k \leq p-2$, and suppose that $p|c_i$ for $i < k$. Thus, we can write $c_i = pn_i$ for some $n_i \in \mathbb{Z}$ for $i = 0, \ldots, k-1$. Thus,

$$\begin{aligned} p\alpha &= \sum_{i=1}^{p-2} c_i \lambda^i \\ &= pn_0 + pn_1\lambda + \cdots + pn_{k-1}\lambda^{k-1} + \sum_{i=k}^{p-2} c_i \lambda^i. \end{aligned}$$

We now factor p in $\mathfrak{O}_K$, defining γ as follows:

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

Here, we are using the fact that $\frac{1-\zeta^i}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{i-1}$. Note that $(1-\zeta)^{p-1}$ and γ are in $\mathfrak{O}_K$. Hence, factors in $\mathfrak{O}_K$ as

$$p = (1-\zeta)^{p-1}\gamma = \lambda^{p-1}\gamma.$$

Continuing with our above calculation of $p\alpha$:

$$\begin{aligned} \lambda^{p-1}\gamma\alpha &= p\alpha \\ &= pn_0 + pn_1\lambda + \cdots + pn_{k-1}\lambda^{k-1} + \sum_{i=k}^{p-2} c_i\lambda^i \\ &= \lambda^{p-1} + \lambda^{p-1}\gamma n_1\lambda + \cdots + \lambda^{p-1}\gamma n_{k-1}\lambda^{k-1} + \sum_{i=k}^{p-2} c_i\lambda^i \end{aligned}$$

Solving for the $c_k\lambda^k$ term, we see

$$c^k\lambda^k = \lambda^{k+1}\mu$$

for some $\mu \in \mathfrak{O}_K$. It follows that $c_k = \lambda\mu$. Take norms:

$$c_k^{p-1} = N(c_k) = N(\lambda)N(\mu) = pN(\mu)$$

where $N(\mu) \in \mathbb{Z}$. Since p divides the integer c_k^{p-1} and p is prime, it follows that $p|c_k$. That completes the induction and the proof. $\square$