Lecture 9: Cyclotomic Fields

Last time: $\mathcal{O}$ an int. of $\mathcal{O}_K$

$N(\mathcal{O}) = [\mathcal{O}_K : \mathcal{O}]$ multiplicative,

$N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$

Today:

Thm: $K = \mathbb{Q}(\zeta)$ where ζ is a primitive n^{th} root of 1. Then $\{1, \zeta, \zeta^2, \dots, \zeta^{d-1}\}$ is an integral basis for $\mathcal{O}_K$, where $d = [K:\mathbb{Q}] = \varphi(n)$.

Focus on case $n = p$, a *prime*.

Lemma: Set $\lambda = 1 - \zeta$. Then (λ) has norm p, and hence is prime. Moreover $(p) = (\lambda)^{p-1}$.

Pf: $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1 = \prod_{k=1}^{p-1} (x - \zeta^k)$.

So $\Phi_p(1) = p = \prod_{k=1}^{p-1} (1 - \zeta^k) = N_{K/\mathbb{Q}}(1 - \zeta) = N((\lambda))$.

Moreover, $(1 - \zeta^k) = (1 - \zeta)$ because

$$1 - \zeta^k = \varepsilon_k (1 - \zeta) \text{ where } \varepsilon_k = \frac{1 - \zeta^k}{1 - \zeta} = \zeta^{k-1} + \zeta^{k-2} + \dots + 1$$

is a unit: if $k'k \equiv 1 \bmod p$ then

$$\varepsilon_k^{-1} = \frac{1 - \zeta}{1 - \zeta^k} = \frac{1 - (\zeta^k)^{k'}}{1 - \zeta^k} = (\zeta^k)^{k'-1} + \dots + \zeta^k + 1 \in \mathcal{O}_K. \quad \blacksquare$$

Pf of Thm: We know $\mathcal{O}_K/(\lambda) \cong \mathbb{Z}/p\mathbb{Z}$.

Thus

$$\lambda\mathcal{O} + \mathbb{Z} = \mathcal{O} \Rightarrow \lambda\mathcal{O} + \mathbb{Z}[\zeta] = \mathcal{O}.$$

Mult by λ we get $\lambda^2\mathcal{O} + \lambda\mathbb{Z}[\zeta] = \lambda\mathcal{O}$.

Substituting in, we get

$$\mathcal{O} = \lambda^2\mathcal{O} + \lambda\mathbb{Z}[\zeta] + \mathbb{Z}[\zeta] = \lambda^2\mathcal{O} + \mathbb{Z}[\zeta]$$

Repeating, get $\lambda^2\mathcal{O} = \lambda^4\mathcal{O} + \lambda^2\mathbb{Z}[\zeta] \Rightarrow$

$\mathcal{O} = \lambda^4\mathcal{O} + \mathbb{Z}[\zeta]$. Continuing yields

$$\mathcal{O} = \lambda^t\mathcal{O} + \mathbb{Z}[\zeta] \text{ for all } t \geq 1.$$

Now by an earlier calculation,

$$\operatorname{disc}(1, \zeta, \zeta^2, \ldots, \zeta^{p-2}) = \pm p^{p-2}$$

Thus $p^{p-2}\mathcal{O} \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}$ ← e.g. by HW or the proof that $(\mathcal{O}, +) \cong \mathbb{Z}^n$.

So combining, we have

$$\mathcal{O} = \underbrace{(\lambda^{p-1})^{p-2}\mathcal{O}}_{p^{p-2}\mathcal{O} \subseteq \mathbb{Z}[\zeta]} + \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]$$

∎

Cor: $\Delta_K = \pm p^{p-2}$

Rmk: $p = (\lambda)^{p-1}$ ramifies in K, divides Δ_K.
Fits general pattern.

General case: First consider $n = p^v$. Same argument works: $(p) = (\lambda)^d$, $d = \varphi(p^v)$,
$\operatorname{disc}(1, \zeta, \dots, \zeta^{d-1}) = \pm p^s$ where $s = p^{v-1}(vp - v - 1)$,
blah, blah, ...

In general, $n = p_1^{v_1} \cdots p_k^{v_k}$ and
$K = \mathbb{Q}(\zeta_n)$ ← compositum of $\mathbb{Q}(p_i^{v_i})$

$\mathbb{Q}(\zeta_{p_1^{v_1}})$ $\mathbb{Q}(p_2^{v_2})$ $\cdots$ $\mathbb{Q}(p_k^{v_k})$

$\mathbb{Q}$

By mult. prop of ϕ, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \pi [\zeta_{p_i^{v_i}} : \mathbb{Q}]$
and as $\gcd(\Delta_{\mathbb{Q}(\zeta_{p_i}^{v_i})}, \Delta_{\mathbb{Q}(\zeta_{p_j}^{v_j})}) = 1$ we find

$$\mathcal{O}_K = \pi \mathcal{O}_{\mathbb{Q}(\zeta_{p_i^{v_i}})} = \pi \mathbb{Z}[\zeta_{p_i^{v_i}}] = \mathbb{Z}[\zeta]$$

Prime ideals in $\mathcal{O}_K$: $\mathfrak{p}$ prime

Then $\mathfrak{p}$ contains a unique rational prime p, since $\mathfrak{p} \cap \mathbb{Z}$ is a nonempty prime ideal

[we saw this earlier: $\alpha \in \mathfrak{p}$ sat $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$]

Thus $\mathfrak{p} \supseteq p\mathcal{O}_K$ and so

$N(\mathfrak{p}) \mid N(p\mathcal{O}_K) = p^n$. Thus $N(\mathfrak{p}) = p^v$.

Conversely, each rational prime p has

$$p\mathcal{O}_K = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_k^{v_k}$$

Discuss more on Friday

HW #3 (Due Wed Feb 18)

Ch 2: 33, 35.

Ch 3: 9, 11, 12, 13.

→ add (f) give the norms of the ideals $(\alpha+2)$, $(5, \alpha^2+3\alpha-1)$

are they prime?