Last week we saw how to factor ideals of the form $(p)$ with $p$ a prime number.

**Def$^n$**: Let $p$ be a prime number and $K$ a number field.

Let $(p) = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ be the factorization into prime ideals

$e_i = e_{\mathfrak{P}_i | p}$

- if for some $i$, we have $e_i > 1$ then we call $p$ ramified in $K$. Otherwise we call it unramified

e.g. $(p) = \mathfrak{P}_1^2 \mathfrak{P}_2 \mathfrak{P}_3$ or $(p) = \mathfrak{P}_1^3 \mathfrak{P}_2^7$

are both ramified

if $e_1 = [K:\mathbb{Q}]$ then we call it totally ramified

$$(p) = \mathfrak{P}^{[K:\mathbb{Q}]}$$

Recall that we have the following formula

$$[K:\mathbb{Q}] = \sum_i e_i f_{\mathfrak{P}_i | p}$$

- $p$ is called **inert** if its unramified and $r=1$.

  i.e. this means $\exists!\ \mathfrak{P} \mid (p)$ and $f_{\mathfrak{P}|p} = [K:\mathbb{Q}]$

  i.e $(p)$ is itself a prime ideal.

- $p$ is called split if its unramified and $\exists\ i$ such that

$$f_{\mathfrak{P}_i|p} = 1 = \left[\mathcal{O}_K/\mathfrak{P}_i : \underset{\mathbb{F}_p}{\underset{\shortparallel}{\mathbb{Z}/p\mathbb{Z}}}\right]$$

we say its totally split if $\forall\ i$ we have

$$f_{\mathfrak{P}_i|p} = 1.$$

$$(p) = \mathfrak{P}_1 \cdots \mathfrak{P}_r$$

---

Theorem: Let $p$ is a prime number and $K$ a number field

If $p$ is ramified in $K$ then

$$p \mid \Delta(\mathcal{O}_K).$$

(Converse is true but we wont prove it!)

**Def$^n$ from Galois theory** | We say a number field $K$ is **normal** if every embedding of $K$ has image again in $K$ i.e. each embedding$_{/\mathbb{Q}}$ is an automorphism of $K$. $\sigma: K \to K$. if $\sigma$ is an embedding.

We call $Gal(K/\mathbb{Q})$ the set of embeddings. which we can make into a group called the Galois group.

$$\sigma_1, \sigma_2 \in Gal(K/\mathbb{Q}) \qquad \sigma_i : K \to K.$$

- $(\sigma_1 \cdot \sigma_2)(x) = \sigma_1(\sigma_2(x))$ (multiplication)
- identity embedding is the identity element.

- If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ and $\sigma \in Gal(K/\mathbb{Q})$ then we let

$\sigma(\mathfrak{p}) :=$ ideal generated by the image of $\mathfrak{p}$ under $\sigma$.

Theorem (Decomposition theorem for cyclotomic fields)

Let $n \in \mathbb{Z}_{\geq 1}$ and $\zeta_n$ a (primitive) $n$-th root of unity.
Set $K = \mathbb{Q}(\zeta_n)$ and take $p$ a prime number.

Write $n = p^k \cdot m$ with $p \nmid m$ and let

$$e = \varphi(p^k) = p^{k-1}(p-1) \quad (\varphi = \text{Euler totient function})$$

and let $f$ be the order of $p$ in $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$

Then

$$(p) = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e \quad \text{with } e = e_{\mathfrak{P}_i|p} \ \forall i$$

$$\text{and } f = f_{\mathfrak{P}_i|p} \ \forall i$$

Example: Let $n=5$ and $K = \mathbb{Q}(\zeta_5)$, $p$ a prime number

| $p \bmod n (=5)$ | Order of $p$ in $(\mathbb{Z}/m)^\times$ (= residue degree) | factorization of $(p)$ | Norms |
|---|---|---|---|
| 0 | – | $(p) = \mathfrak{P}^4 = \mathfrak{P}^{[K:\mathbb{Q}]}$ | $N(\mathfrak{P}) = p^1$ |
| 1 | 1 | $(p) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4$ | $N(\mathfrak{P}_i) = p^1$ |
| 2 | 4 | $(p) = (p)$ inert | $N((p)) = p^4$ |
| 3 | 4 | $(p) = (p)$ | $N((p)) = p^4$ |

| | | | |
|---|---|---|---|
| 4 | 2 | $(p) = P_1 P_2$ | $N(P_i) = p^2$ |

We can use this to look $\mathbb{Q}(\zeta_{55})$

$$(11) = (P_1 P_2 P_3 P_4)^{10}$$