On Friday, we were analyzing possible factorizations in:

\[ L \triangleleft \mathbb{Q} \]

**Proposition:** \([ L : K ] = \sum_{i=1}^{r} e_i f_i \) where \( f_i = \text{residual degree} = [ \Omega / \Phi_i : \Omega / \Phi ] \)

If: CKT then \( \Omega / \Phi \Omega_L = \bigoplus_{i} \Omega / \Phi_i \Omega_L \)

**Main Thm.:** Write \( L = K(\theta) \) with \( \theta \in \Omega_L \), min. poly \( \phi_\theta(x) \in \Omega_K[x] \).

For almost all primes \( \mathfrak{p} \), we have following correspondence:

If \( \overline{\phi_\theta(x)} = \overline{\phi_1(x)}^{e_1} \ldots \overline{\phi_r(x)}^{e_r} \) in \( \Omega_K/\mathfrak{p} \), then

\[ \mathfrak{p} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r} \] as \( \Omega_L \)-ideals

where \( \mathfrak{p}_i = \mathfrak{p} \Omega_L + \phi_i(x) \Omega_L =: \langle \mathfrak{p}, \phi_i(x) \rangle \) with \( \phi_i \) = monic in \( \Omega_K \)

and \( f_i \) def \( [ \Omega / \phi_i : \Omega / \mathfrak{p} ] = \deg(\overline{\phi_i}) \).

**Remark:** This theorem holds without exception (as we will prove) if

\( \Omega_L = \Omega_K[\theta] \) where \( L = K(\theta) \).

**Example:** \( L = \mathbb{Q} \left( \sqrt{d} \right) \) \( d \equiv 2, 3 \pmod{4} \) then \( \Omega_L = \mathbb{Z}[\sqrt{d}] \) so by

remark, theorem applies. To determine how \( p \) factors, to all \( p \neq 2,3 \)

analyze \( x^2 \equiv -d \pmod{p} \). This factor if \( d \) is a residue mod. \( p \).

(see p. 43 of notes for more here...)
For (b), use similar arguments to before: Consider the chain

\[ \mathcal{O}_L \supset \mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_\ell. \]

We know \( \mathcal{O}_L / \mathfrak{p}_i \) is \( \mathfrak{f}_i \)-dim'\( \mathfrak{v} \)-dimensional vector space over \( \mathcal{O}_K / \mathfrak{p}_i \); this is defin. of \( \mathfrak{f}_i \).

But there's no proper ideal between \( \mathfrak{p}_i \) and \( \mathfrak{p}_{i+1} \), so \( \mathfrak{p}_i / \mathfrak{p}_{i+1} \) is 1-dim'\( \mathfrak{v} \)-dimensional over \( \mathcal{O}_K / \mathfrak{p}_i \), so also has \( \mathfrak{f}_i \)-dim'\( \mathfrak{v} \)-dimensional over \( \mathcal{O}_K / \mathfrak{p}_i \).

Dividing through by \( \mathfrak{p}_i \), and adding it up for each quotient, we get \( \mathfrak{f}_i \) as degree of \( \mathcal{O}_L / \mathfrak{p}_i \).

---

**Main Theorem**

**Proof:** Suppose \( \mathcal{O}_L = \mathcal{O}_K[\theta] \). Then we claim finitely many exceptions.

\[ \mathcal{O}_L / \mathfrak{p}_\mathcal{O}_L \cong \mathcal{O}_K / \mathfrak{p}_K[\theta] / \bar{\mathcal{O}}_\mathcal{O}(x). \]

Indeed we have surjective map \( \mathcal{O}_K[\theta] \twoheadrightarrow \mathcal{O}_K / \mathfrak{p}_K[\theta] / (\bar{\mathcal{O}}_\mathcal{O}(x)) \) with kernel \( < \mathfrak{p}, \phi_\mathcal{O}(x) > \), and

isomorphism follows since \( \mathcal{O}_L = \mathcal{O}_K[\theta] \cong \mathcal{O}_K[\theta] / (\phi_\mathcal{O}(x)) \)

It is explicitly realized as \( f(\theta) \mapsto f(x) \).

Given info about \( \mathcal{O}_K / \mathfrak{p}_K[\theta] / \bar{\mathcal{O}}_\mathcal{O}(x) \): know \( \bar{\phi}_\mathcal{O}(x) = \bar{\phi}_1(x) \cdots \bar{\phi}_r(x) \).

So C.R.T implies:

\[ \mathcal{O}_K / \mathfrak{p}_K[\theta] / (\bar{\mathcal{O}}_\mathcal{O}(x)) \cong \bigoplus_{i=1}^{r} \mathcal{O}_K / \mathfrak{p}_K[\theta] / (\bar{\phi}_i(x) \mathfrak{e}_i) \]

so that prime ideals of \( \mathcal{R} \) are the \( \bar{\phi}_i(x) \mod \bar{\mathcal{O}}_\mathcal{O}(x) \). Moreover...
\[ \frac{R}{(\overline{\Phi}_i)} : \frac{\Theta_k}{\Theta_0} = \deg(\overline{\Phi}_i) \] and in \( R \),

\[ (0) = (\bigcap_{i=1}^r \overline{\Phi}_i(x)) = \bigcap_{i=1}^r (\overline{\Phi}_i)_{e_i} \]

Transforming these conclusions to \( \Theta_k/\Theta_0 \) via \( f(x) \rightarrow f(\Theta) \) isomorphism

If prime ideals \( \overline{\Phi}_i \) of \( \Theta_k/\Theta_0 \) in bijection with \( (\overline{\Phi}_i)_{e_i} \)

They are principal ideals generated by \( \phi_i(\Theta) \mod \Theta_0 \).

Let \( \Phi_i \) be their preimage under \( \Theta_k \rightarrow \Theta_k/\Theta_0 \)

so \( \Phi_i = \Theta_0 + \phi_i(\Theta) \Theta_k \). These are precisely the ideals containing \( \Theta \) in \( \Theta_k \).

\[ \text{degree} \left[ \frac{\Theta_k/\Theta_0}{\Phi_i} : \frac{\Theta_k}{\Theta_0} \right] = \deg(\Phi_i) \]

\[ \frac{\Theta_k}{\Phi_i : \Theta_k/\Theta_0} \]

It remains to show \( \Theta = \Phi_1 e_1 \cdots \Phi_r e_r \) with \( \Phi_i = \Theta_0 + \phi_i(\Theta) \Theta_k \).

But \( (0) = \bigcap_{i=1}^r \Phi_i \) and \( \Phi_i = (\Phi_i)_{e_i} \) so \( \bigcap_{i=1}^r \Phi_i = \Theta_0 \).

\[ \Rightarrow \frac{\Theta_0}{\bigcap_{i=1}^r \Phi_i} \]

But by previous prop., \( \sum_{i} e_i(\Phi_i) = n \)

(as product is smaller ideal than intersection)

so this must be equality.

in number analogy, product of ideals is ideal gen. by product
intersection is ideal gen. by lcm.
Example: \( k = \mathbb{Q}(\sqrt[3]{2}) \), so \( \mathcal{O}_k = \mathbb{Z}[\sqrt[3]{2}] \) with \( \varphi_{\sqrt[3]{2}}(x) = x^3 - 2 \).

Analyze \( x^3 - 2 \pmod{p} \). E.g. \( \pmod{5} \):

\[
x^3 - 2 \equiv (x-3)(x^2+3x-1) \pmod{5}
\]

So \( 5 \cdot \mathcal{O}_k = g_1 g_2 \) with \( g_1 \) having inertia \( \deg 1 \)

\( g_2 \) having inertia \( \deg 2 \).

In proof of Main Theorem, we assumed \( \mathcal{O}_L = \mathcal{O}_k[\vartheta] \). Didn't need this.

Just needed that \( \mathcal{O}_L / g_0 \mathcal{O}_L \cong \mathcal{O}_k[\vartheta] / g \mathcal{O}_k[\vartheta] \).

This will be true for almost all primes \( g \). To give precise condition,

define the conductor of ring \( \mathcal{O}_k[\vartheta] \):

\[ \text{Nagel ideal } f \text{ in } \mathcal{O}_L \text{ contained in } \mathcal{O}_k[\vartheta], \text{ i.e.} \]

\[ f = \{ \alpha \in \mathcal{O}_L \mid \alpha \cdot \mathcal{O}_L \subseteq \mathcal{O}_k[\vartheta] \} \]

Claim: If \( g \) is relatively prime to \( f \), then \( \mathcal{O}_L / g \mathcal{O}_L \cong \mathcal{O}_k[\vartheta] / g \mathcal{O}_k[\vartheta] \) (as \( \mathcal{O}_L \) ideals)

Proof: \( g, f \) relatively prime means \( g \mathcal{O}_L + f = \mathcal{O}_L \)

Since \( f \in \mathcal{O}_k[\vartheta] \), then \( \mathcal{O}_L = g \mathcal{O}_L + \mathcal{O}_k[\vartheta] \) so

map \( \mathcal{O}_k[\vartheta] \rightarrow \mathcal{O}_L / g \mathcal{O}_L \) is surjective with kernel \( g \mathcal{O}_L \cap \mathcal{O}_k[\vartheta] \)

then \( g \mathcal{O}_L \cap \mathcal{O}_k[\vartheta] = (g + f)(g \mathcal{O}_L \cap \mathcal{O}_k[\vartheta]) \)

\[ = g \mathcal{O}_k[\vartheta] \]

since \( (g, f \cap \mathcal{O}_k) = 1 \)
pf of corollary: As before, \( L = K[\theta] \) with minimal polynomial \( \phi_\theta(x) \).

(coeffs in \( \Omega_K \))

Consider \( d(1, \theta, \ldots, \theta^{n-1}) \) (supposing \( \deg(\phi_\theta) = n = [L : K] \)).

We chased earlier \( d(1, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2, \quad \theta_i = \tau_i(\theta) \) d is an elt. of \( \Omega_K \).

\( \Rightarrow d \) is the classical disc. of \( \phi_\theta \).

\[ d \] records whether poly. has multiple roots.

\[ \phi_\theta \]

and similarly \( \overline{d} \pmod{\mathfrak{g}} \), i.e. as elt. of \( \Omega_K / \mathfrak{g} \) records whether \( \overline{\phi_\theta} \pmod{\mathfrak{g}} \) has multiple roots.

But previous theorem, which applies if \( \mathfrak{g} \) doesn't divide conductor,

\[ \overline{d} \not\equiv 0 \pmod{\mathfrak{g}} \implies e_i's \text{ all } 1. \]

So, at the moment, our condition is that \( \mathfrak{g} \) is unramified if \( \mathfrak{g} \)

doesn't divide conductor nor discriminant.

Remark 1: Neukirch also asks that \( \Omega_L / \Omega_i / \Omega_K / \mathfrak{g} \) is a separable

extension in his def's of unramified.

This is true since all extensions of finite fields are separable.

Remark 2: Sharper condition on ramification (to be proved later)

Define \( \text{disc}(\Omega_L) := \text{ideal generated by } d(d_1, \ldots, d_n) \)

where \( d_1, \ldots, d_n \) is any basis for \( L/K \)

prime divisors of \( \text{disc}(\Omega_L) \) are

exactly the ramified ones.

primes dividing \( \text{disc}(\Omega_L) \) are
Recall that we may attach "Legendre symbol" for a mod $p$ with $(a,p)=1$ as follows:

\[ \left( \frac{a}{p} \right) = a^{\frac{p-1}{2}} \pmod{p} \]

It is multiplicative char. \( \mathbb{Z}/p\mathbb{Z}^* \to \{\pm 1\} \), so we have natural extension to arbitrary integers (positive):

\[ \left( \frac{a}{n} \right) = \left( \frac{a}{p_1} \right)^{e_1} \cdots \left( \frac{a}{p_r} \right)^{e_r} \]

Either satisfies a reciprocity law.

For the Legendre symbol,

\[ \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \]

if $p,q$ distinct odd primes.

For Jacobi symbol, same for odd, coprime integers $m,n$.

In addition, we have supplementary laws:

\[ \left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}} \quad \left( \frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}} \]

i.e. depends on congruence mod 4.

In context of factoring in quadratic extension:

A.R. \Rightarrow we can characterize factorization of almost all primes in quadratic extension using congruence conditions mod $d$. 