On Friday, we were analyzing possible factorizations in: INTRO 9/29

$$\begin{array}{ccccc} & L & \mathcal{O}_L & & \mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r} \\ \text{sep.} & | & | & & | \\ & K & \underbrace{\mathcal{O}_K}_{\text{arb. Dedekind domain}} & \ni & \mathfrak{p} \end{array}$$

Proposition: $[L:K] = \sum_{i=1}^{r} e_i f_i$ where f_i = residual degree $= [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$

Pf: CRT on $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \bigoplus_i \mathcal{O}_L/\mathfrak{P}_i^{e_i}\mathcal{O}_L$

Main Thm: Write $L = K(\theta)$ with $\theta \in \mathcal{O}_L$, min. poly $\phi_\theta(x) \in \mathcal{O}_K[x]$.

For almost all primes* $\mathfrak{p}$, we have following correspondence:

If $\bar{\phi}_\theta(x) = \bar{\phi}_1(x)^{e_1}\cdots\bar{\phi}_r(x)^{e_r}$ in $\mathcal{O}_K/\mathfrak{p}$ then

$\mathfrak{p} = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r}$ as $\mathcal{O}_L$-ideals

where $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + \phi_i(x)\mathcal{O}_L =: \langle \mathfrak{p}, \phi_i(x)\rangle$ with ϕ_i: monic in $\mathcal{O}_K$ $\equiv \bar{\phi}_i \bmod \mathfrak{p}$.

and $f_i \overset{\text{def}}{=} [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}] = \deg(\bar{\phi}_i)$.

Remark: This theorem holds without exception (as we will prove) if $\mathcal{O}_L = \mathcal{O}_K[\theta]$ where $L = K(\theta)$.

Example: $L = \mathbb{Q}(\sqrt{d})$ $d \equiv 2,3\ (4)$ then $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$ so by remark, theorem applies to all $p \in \mathbb{Z}$. To determine how p factors, analyze $x^2 - d \pmod p$. This factors iff d is a quad. residue mod. p.

(See p. 43 of notes for more here....)

~~For (b), use similar argument to before: Consider the chain~~

~~$\mathcal{O}_L \supset \mathfrak{P}_i \supset \mathfrak{P}_i^2 \supset \dots \supset \mathfrak{P}_i^{e_i}$. We know $\mathcal{O}_L/\mathfrak{P}_i$ is f_i-dim'l vector space over $\mathcal{O}_K/\mathfrak{p}$; this is defn of f_i.~~

~~But there's no proper ideal between $\mathfrak{P}_i^j$ and $\mathfrak{P}_i^{j+1}$, so $\mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ is 1-dim'l v.s. over $\mathcal{O}_L/\mathfrak{P}_i$, so also has dim'n f_i over $\mathcal{O}_K/\mathfrak{p}$.~~

~~Dividing through by $\mathfrak{P}_i^{e_i}$ and Adding it up for~~ ~~each~~ ~~successive quotient, we get $e_i f_i$ as degree of $\mathcal{O}_L/\mathfrak{P}^{e_i}$.~~

Proof of ~~Proposition~~ Main Thm: Suppose $\mathcal{O}_L = \mathcal{O}_K[\theta]$. ~ the failure of this will force finitely many exceptions. Then we claim

$$\mathcal{O}_L / \mathfrak{p}\mathcal{O}_L \simeq \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \big/ \bar{\phi}_\theta(x).$$

Indeed we have surjective map $\mathcal{O}_K[x] \longrightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \big/ (\bar{\phi}_\theta(x))$

with kernel $\langle \mathfrak{p}, \phi_\theta(x) \rangle$, and

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

It is explicitly realized as $f(\theta) \longmapsto \bar{f}(x)$.

Given info about $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \big/ \bar{\phi}_\theta(x)$: Know $\bar{\phi}_\theta(x) = \bar{\phi}_1(x)^{e_1} \cdots \bar{\phi}_r(x)^{e_r}$

so C.R.T implies:

$$\underbrace{\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \big/ (\bar{\phi}_\theta(x))}_{R} = \bigoplus_{i=1}^{r} \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \big/ (\bar{\phi}_i(x)^{e_i})$$

so that prime ideals of R are the principal ideals gen'd by $\bar{\phi}_i(x)$ mod $\bar{\phi}_\theta(x)$. Moreover...

$$[R/(\bar{\phi}_i) : \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K] = \deg(\bar{\phi}_i), \quad \text{and in } R,$$

$$(0) = (\bar{\phi}_\theta(x)) = \bigcap_{i=1}^{r} (\bar{\phi}_i)^{e_i}$$

Transferring these conclusions to $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ via $f(x) \mapsto f(\theta)$ isomorphism

$\exists$ prime ideals $\bar{\mathfrak{P}}_i$ of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ in bijection with $(\bar{\phi}_i)$

They are principal ideals generated by $\phi_i(\theta)$ mod $\mathfrak{p}\mathcal{O}_L$.

Let $\mathfrak{P}_i$ be their preimage under $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$

so $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + \phi_i(\theta)\mathcal{O}_L$. These are precisely the ideals containing $\mathfrak{p}$ in $\mathcal{O}_L$.

(i.e. $\mathfrak{P}_i \mid \mathfrak{p}$).

---

degree $\left[\dfrac{\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L}{\bar{\mathfrak{P}}_i} : \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \right] = \deg(\bar{\phi}_i)$

$$\|$$

$$[\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K]$$

It remains to show $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ with $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + \phi_i(\theta)\mathcal{O}_L$.

But $(0) = \bigcap \bar{\mathfrak{P}}_i^{e_i}$ and $\bar{\mathfrak{P}}_i^{e_i} = (\bar{\mathfrak{P}}_i)^{e_i}$ so $\bigcap \mathfrak{P}_i^{e_i} \subseteq \mathfrak{p}\mathcal{O}_L$.

$\Rightarrow \mathfrak{p}\mathcal{O}_L \mid \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$. But by previous prop., $\sum_i e_i f_i = n$

(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 $\phi_{\sqrt[3]{2}}(x) = x^3 - 2$.

Analyze $x^3 - 2 \pmod p$. E.g. mod 5:

$$x^3 - 2 \equiv (x-3)(x^2+3x-1) \pmod 5$$

so $5 \cdot \mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2$ with $\mathfrak{p}_1$ having inertia deg 1, $\mathfrak{p}_2$ having inertia deg 2, $/ \mathbb{Z}/5\mathbb{Z}$

In pf. of Main Thm, we assumed $\mathcal{O}_L = \mathcal{O}_K[\theta]$. Didn't need this.

Just needed that $\mathcal{O}_L / \mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_K[\theta] / \mathfrak{p}\mathcal{O}_K[\theta]$.

This will be true for almost all primes $\mathfrak{p}$. To give precise condition,

define the conductor of ring $\mathcal{O}_K[\theta]$:

Largest ideal $\mathfrak{F}$ in $\mathcal{O}_L$ contained in $\mathcal{O}_K[\theta]$, i.e.

$$\mathfrak{F} = \{ \alpha \in \mathcal{O}_L \mid \alpha \cdot \mathcal{O}_L \subseteq \mathcal{O}_K[\theta] \}$$

claim: If $\mathfrak{p}$ is relatively prime to $\mathfrak{F}$ (as $\mathcal{O}_L$ ideals), then $\mathcal{O}_L / \mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_K[\theta] / \mathfrak{p}\mathcal{O}_K[\theta]$

pf: $\mathfrak{p}, \mathfrak{F}$ relatively prime means $\mathfrak{p}\mathcal{O}_L + \mathfrak{F} = \mathcal{O}_L$

Since $\mathfrak{F} \subseteq \mathcal{O}_K[\theta]$ then $\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L + \mathcal{O}_K[\theta]$ so

map $\mathcal{O}_K[\theta] \to \mathcal{O}_L / \mathfrak{p}\mathcal{O}_L$ is surjective with kernel $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\theta] = \mathfrak{p}\mathcal{O}_K[\theta]$,

then $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\theta] = (\mathfrak{p} + \mathfrak{F})(\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\theta])$

$\subseteq \mathfrak{p}\mathcal{O}_K[\theta]$

since $(\mathfrak{p}, \mathfrak{F} \cap \mathcal{O}_K) = 1$

$\subseteq \mathfrak{p}\mathcal{O}_K[\theta]$.

pf. of corollary: As before, $L = K[\theta]$ with minimal polynomial $\phi_\theta(x)$.

(coeffs. in $\mathcal{O}_K$)

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

We showed earlier $\underbrace{d(1, \dots, \theta^{n-1})}_{d} = \prod_{i<j} (\theta_i - \theta_j)^2$, $\theta_i = \tau_i(\theta)$

d is an elt. of $\mathcal{O}_K$.

$\|$

classical disc. of ϕ_θ.

d records whether poly. ϕ_θ has multiple roots.

and similarly $\bar{d}$ (mod $\mathfrak{p}$) i.e. as elt. of $\mathcal{O}_K/\mathfrak{p}$ records whether $\bar{\phi}_\theta$ mod $\mathfrak{p}$ has multiple roots.

But previous theorem, which applies if $\mathfrak{p}$ doesn't divide conductor,

says $\bar{d} \not\equiv 0$ mod $\mathfrak{p}$ $\Rightarrow$ e_i's all 1.

So, at the moment, our condition is that $\mathfrak{p}$ is unramified if $\mathfrak{p}$

doesn't divide conductor nor discriminant.

Remark 1: Neukirch also asks that $\mathcal{O}_L/\mathfrak{P}_i \,/\, \mathcal{O}_K/\mathfrak{p}$ is a separable

extension in his def'n of unramified.

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

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

Define $\mathrm{disc}(\mathcal{O}_L) :=$ ideal generated by $d(\alpha_1, \dots, \alpha_n)$

where $\alpha_1, \dots, \alpha_n$ is any basis for L/K

with elts in $\mathcal{O}_L$.

primes dividing $\mathrm{disc}(\mathcal{O}_L)$ are exactly the ramified ones.

Recall that we may attach "Legendre symbol" for a mod p ~~[illegible]~~ as follows:
with $(a,p)=1$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p \qquad \text{with} \quad \left(\frac{a}{p}\right) \in \{\pm 1\}$$

It is multiplicative char. $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$, so we have natural extension to arbitrary integers (positive) : $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}$

if $n = p_1^{e_1} \cdots p_r^{e_r}$

"Jacobi symbol"

Either satisfies a reciprocity law.

For the Legendre symbol,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \quad \text{if } p, q \text{ distinct odd primes.}$$

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

In addition, we have supplementary laws $\left(\frac{-1}{p}\right) = \underbrace{(-1)^{\frac{p-1}{2}}}_{\text{i.e. depends on cong. mod } 4.}$ $\quad \left(\frac{2}{p}\right) = \underbrace{(-1)^{\frac{p^2-1}{8}}}_{\text{i.e. depends on congruence mod } 8}$

In context of factoring in quadratic extension,

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