3.2 Decomposition of primes ①

L/K fin. ext. of #-fields

(more gen: A Dedekind, $K = \mathrm{Frac}(A)$,
L/K fin. sep. ext, $\mathcal{O}_L$ = integral
closure of $A = \mathcal{O}_K$ in L)

$\mathcal{O} \neq \mathfrak{p} \subseteq \mathcal{O}_K$ prime

$\Rightarrow \mathfrak{p} = \mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_g^{e_g}$, $\mathfrak{q}_i \neq \mathfrak{q}_j$ $i \neq j$

$e(\mathfrak{q}_i | \mathfrak{p}) := e_i$ ram. index

$f(\mathfrak{q}_i | \mathfrak{p}) := [k(\mathfrak{q}_i) | k(\mathfrak{p})]$
residue degree

Prop: Let $\mathfrak{q} \subseteq \mathcal{O}_L$ prime

1) $\mathfrak{q} \mid \mathfrak{p} \iff \mathfrak{q} = \mathfrak{q}_i$ for some i

$\iff \mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$

2) $\sum_{i=1}^{g} e(\mathfrak{q}_i \mid \mathfrak{p}) \cdot f(\mathfrak{q}_i \mid \mathfrak{p})$

$= [L:K]$

3) If L/K Galois, then $\mathrm{Gal}(L/K)$ acts transitively on $\{\mathfrak{q}_1, \dots, \mathfrak{q}_g\}$

$\iff e := e_1 = e_2 = \dots = e_g$,

$f := f_1 = \dots = f_g$

$\star$ $g \cdot e \cdot f = [L:K]$

Proof: 1) If $q \supseteq p\cdot\mathcal{O}_L = q_1^{e_1}\cdot\ldots\cdot q_g^{e_g}$

$\Rightarrow q \supseteq q_i \Rightarrow q = q_i$

q, q_i max.

$\Rightarrow q_i \cap \mathcal{O}_K$ prime $\forall i$

and $p \subseteq q_i \cap \mathcal{O}_K \Rightarrow p = q_i \cap \mathcal{O}_K$

$\nwarrow$ max. $\nearrow$

2) Note

e_i -- step filtr. by $k(q_i)$

$$\mathcal{O}_L/p\mathcal{O}_L \overset{\text{CRST}}{\cong} \prod_{i=1}^{g} \mathcal{O}_L/q_i^{e_i}$$

$$\Rightarrow \dim_{k(p)} \mathcal{O}_L/p\cdot\mathcal{O}_L = \sum_{i=1}^{g} e_i\cdot f_i$$

Claim: $[L:K] = \dim_{k(p)} \mathcal{O}_L/p\mathcal{O}_L$

Pf of claim: localize

$\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ at $S = \mathcal{O}_K \setminus \mathfrak{p}$

$\Rightarrow S^{-1}\mathcal{O}_L$ is a finite [redacted]

torsionfree module over the PID $S^{-1}\mathcal{O}_K = \mathcal{O}_{K,\mathfrak{p}}$ (Ex.)

$\Rightarrow S^{-1}\mathcal{O}_L$ finite free over $\mathcal{O}_{K,\mathfrak{p}}$ $\quad (\mathcal{O}_L \hookrightarrow L,\ S^{-1}\mathcal{O}_L \hookrightarrow S^{-1}L = L)$

$\Rightarrow [L:K] = \operatorname{rk}_{\mathcal{O}_{K,\mathfrak{p}}}(S^{-1}\mathcal{O}_L) =$

$\dim_{k(\mathfrak{p})}(S^{-1}\mathcal{O}_L/\mathfrak{p}\cdot S^{-1}\mathcal{O}_L)$

$= \dim_{k(\mathfrak{p})}\left(\frac{S^{-1}(\mathcal{O}_L/\mathfrak{p}\cdot \mathcal{O}_L)}{\cong \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L}\right)$

$$\mathcal{O}_L/\mathfrak{q}_i^{e_i} \supseteq \mathfrak{q}_i/\mathfrak{q}_i^{e_i} \supseteq \mathfrak{q}_i^2/\mathfrak{q}_i^{e_i}$$

quotients $\mathfrak{q}_i^i/\mathfrak{q}_i^{i+1} \simeq \mathcal{O}_L/\mathfrak{q}_i$

[redacted]

Lemma: A Dedekind ring
$\mathfrak{p} \subseteq A$ max.
$\Rightarrow \mathfrak{p}^i/\mathfrak{p}^{i+1} \simeq A/\mathfrak{p} \quad \forall i \geq 0$

Pf: $S = A \setminus \mathfrak{p}$
$\Rightarrow S^{-1}(\mathfrak{p}^i/\mathfrak{p}^{i+1}) \simeq \mathfrak{p}^i/\mathfrak{p}^{i+1}$
$S^{-1}A/\mathfrak{p} \simeq A/\mathfrak{p}$ (as both are modules over $k(\mathfrak{p})$)

$\Rightarrow$ ~~Why $A \subseteq S^{-1}A$~~

Replace A by $A_{\mathfrak{p}} = S^{-1}A$

Ex.

$\Rightarrow$ A PID

$\Rightarrow$ $\mathfrak{p}^i = (\pi^i)$, $(\pi) \simeq \mathfrak{p}$

$\Rightarrow$ $\pi^{-i} : \mathfrak{p}^i/\mathfrak{p}^{i+1} \xrightarrow{\sim} A/\mathfrak{p}$.

3) If $\sigma \in \mathrm{Gal}(L/K)$

$\Rightarrow$ $\sigma(\mathfrak{p} \cdot \mathcal{O}_L) = \mathfrak{p} \cdot \mathcal{O}_L$

as $\sigma(\mathfrak{p}) = \mathfrak{p}$

$\Rightarrow$ by uniqueness of factorization

$\Rightarrow$ $\mathrm{Gal}(L/K) \curvearrowright \{\mathfrak{q}_1, \dots, \mathfrak{q}_g\}$

"acts on"

Assume contrary

$\Rightarrow \exists j$ s.t. $\sigma(\mathfrak{q}_1) \neq \mathfrak{q}_j \ \forall \sigma \in \mathrm{Gal}(L/K)$

$\Rightarrow \mathfrak{q}_j \setminus \bigcup_{\sigma \in G} \sigma(\mathfrak{q}_1) \neq \emptyset$ $\quad G$!!

Prime avoidance

$\Rightarrow \exists x \in \mathfrak{q}_j \setminus \bigcup_{\sigma \in G} \sigma(\mathfrak{q}_1)$

Then $\sigma(x) \notin \mathfrak{q}_1 \ \forall \sigma \in G$,

but $x \in \mathfrak{q}_j$

$\Rightarrow N_{L/K}(x) \notin \mathfrak{q}_1 \cap \mathcal{O}_K = \mathfrak{p}$

$\&\ N_{L/K}(x) \in \mathfrak{q}_j \cap \mathcal{O}_K = \mathfrak{p}$ $\quad \lightning$

$\Rightarrow x \notin \sigma(\mathfrak{q}_1) \ \forall \sigma \in G$

Apply σ^{-1} $\Rightarrow \sigma^{-1}(x) \notin \mathfrak{q}_1 \ \forall \sigma \in G$

Lemma (prime avoidance):

R noetherian ring, $\mathfrak{q}_1, \dots, \mathfrak{q}_r \subseteq R$ prime,

$\mathfrak{b} \subseteq R$ ideal. Assume $\mathfrak{b} \setminus \mathfrak{q}_i \neq \emptyset$ $\forall i$

$$\Rightarrow \mathfrak{b} \setminus \bigcup_{i=1}^{r} \mathfrak{q}_i \neq \emptyset$$

Proof: Wlog $\mathfrak{q}_i \not\subseteq \mathfrak{q}_j$ for $i \neq j$

Pick $x_{ij} \in \mathfrak{q}_j \setminus \mathfrak{q}_i$, $i \neq j$.

& $a_i \in \mathfrak{b} \setminus \mathfrak{q}_i$

Consider $b_i := a_i \prod_{i \neq j} x_{ij}$

$$\Rightarrow b_i \in \left(\mathfrak{b} \cap \left(\bigcap_{i \neq j} \mathfrak{q}_j\right)\right) \setminus \mathfrak{q}_i$$

Set $b = \sum_{i=1}^{r} b_i \Rightarrow b \equiv b_i \neq 0 \bmod \mathfrak{q}_i$

$$\Rightarrow b \in \mathfrak{b} \setminus \bigcup_{i=1}^{r} \mathfrak{q}_i$$

∎

Thm (Kummer): $p \subseteq \mathcal{O}_K$ max.,
$\alpha \in \mathcal{O}_L$, s.t. $\mathcal{O}_L / p\mathcal{O}_L \simeq$ [illegible]

Let $f(x) \in \mathcal{O}_K[x]$ min. poly. of α

Assume that

$$f(x) \equiv \prod_{i=1}^{g} h_i(x)^{e_i} \bmod p\mathcal{O}_K[x]$$

where $e_i \geq 1$, $h_i(x) \in k(p)[x]$
pairwise dist., monic + irred.

Let $g_i(x) \in \mathcal{O}_K[x]$ be any lift
of h_i $\twoheadrightarrow k(p)[x]$

Then $\mathfrak{q}_i := p\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L \subseteq \mathcal{O}_L$
is maximal $\forall i$
and $p \cdot \mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_g^{e_g}$
& $f(\mathfrak{q}_i | p) = \deg h_i$

Ex: $L = \mathbb{Q}(\alpha), \alpha^3 = 2, K = \mathbb{Q}$

$\Rightarrow \mathcal{O}_L = \mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/x^3-2 \quad \Delta_L = -3^3 \cdot 2^2$

$p=2 \Rightarrow x^3-2 \equiv x^3 \mod(2)$

$\Rightarrow \mathfrak{p}_1 = (2,\alpha) = (\alpha)$

$\mathfrak{p}_1$ [illegible]

$\mathbb{Z}$

$2\mathcal{O}_L = \mathfrak{p}_1^3$

$p=3 \Rightarrow x^3-2 \equiv x^3+1 \mod 3$

$\equiv (x+1)^3$

$\Rightarrow (3) = (3,\alpha+1)^3$

$p=5 \Rightarrow x^3-2 \equiv (x+2)(x^2+3x-1) \mod(5)$

$\Rightarrow (5) = (5,\alpha+2) \cdot (5, \alpha^2+3\alpha-1)$

$\mathfrak{p}$ $\mathfrak{P}$

$f=1$ $f=2$

Pf: Set $R = \mathcal{O}_K[\alpha] \simeq \mathcal{O}_K[x]/f(x)$

$\wr$

$\mathcal{O}_L$

Then

$$R/\mathfrak{p}\cdot R \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \mathcal{O}_K/\mathfrak{p}[\bar{\alpha}]$$

is surjective, and $\dim_{k(\mathfrak{p})} R/\mathfrak{p}$

$= \deg \bar{f} \leq [L:K]$

$= \dim_{k(\mathfrak{p})} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$

$\Rightarrow R/\mathfrak{p}\cdot R \simeq \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$

Now, $R/\mathfrak{p} \simeq k(\mathfrak{p})[x]/\bar{f}(x)$ with

$\bar{f} \in k(\mathfrak{p})[x]$ the red. of f

$\overset{CRT}{\Rightarrow} R/\mathfrak{p} \simeq \prod_{i=1}^{g} k(\mathfrak{p})[x]/h_i(x)^{e_i}$

$$\Rightarrow \mathcal{O}_L/p\mathcal{O}_L \simeq \prod_{i=1}^{r} \mathcal{O}_L/(p, g_i(\alpha))^{e_i}$$

$\Rightarrow$ Claim

(Note: $\mathcal{O}_L/\underbrace{(p, g_i(\alpha))}_{\mathfrak{q}_i} \simeq k(p)[x]/h_i(x)$

$\Rightarrow f(\mathfrak{q}_i | p) = \deg h_i(x)$) $\square$

Lemma: The ass. $\mathcal{O}_L/p\mathcal{O}_L = \mathcal{O}_K/p\,[\alpha]$ is satisfied if

i) $\mathcal{O}_L = \mathcal{O}_K[\alpha]$

or

ii) $\underset{K(\alpha)=L}{\alpha \in \mathcal{O}_L}$, s.t. $p \nmid (N_{L/K}(f'(\alpha)))$

~~(holds for all but fin. many p, if $L = K(\alpha)$)~~

Ex: $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{5})$

$\Rightarrow \alpha = \sqrt{5}$ *, $\mathbb{Z}[\alpha] \subsetneq \mathcal{O}_L$

$N_{L/K}(f'(\alpha)) = \pm 4 \cdot 5$ ✓

$\forall\, p \neq 2, 5$

Prf of Ia: i) ✓

ii) [redacted]

[redacted] Set $d := \det(Tr_{L/K}(\alpha_i \alpha_j))$

$\Rightarrow \frac{1}{d} \mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L \subseteq \frac{1}{d} \cdot \mathcal{O}_K[\alpha]$

Prf. of Thm. 1.3.3.

If $p \nmid N_{L/K}(f'(\alpha)) \overset{\text{prop. calc}}{=} p \nmid (d)$

Prop. 1.3.2.