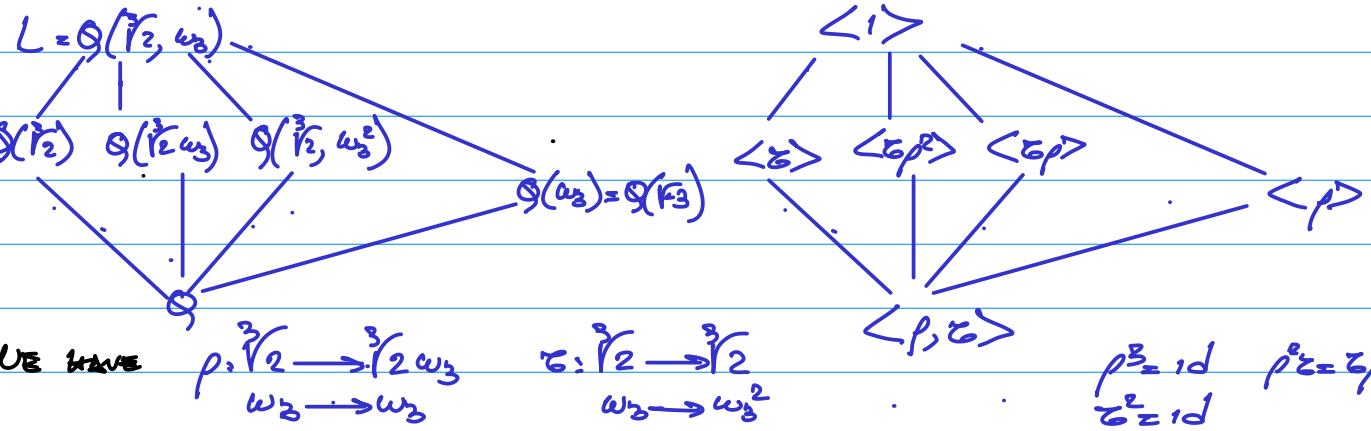
Galois Theory applied to Prime Decomposition

Recall that an extension of number fields L/k is Galois when $\forall \sigma: L/k \hookrightarrow \overline{\mathbb{Q}}$ k-embedding, $\sigma(L)\subseteq L$

The set of k-embeddings is the Galois group, denoted $\mathrm{Gal}(L/k)$

There is a correspondence between subgroups of the Galois group and subextensions.

Ex



We have $\rho:\sqrt[3]{2}\to\sqrt[3]{2}\omega_3$, $\omega_3\to\omega_3$ $\quad\tau:\sqrt[3]{2}\to\sqrt[3]{2}$, $\omega_3\to\omega_3^2$ $\quad\rho^3=1d$, $\tau^2=1d$, $\rho^2\tau=\tau\rho$

$\mathrm{Gal}(L/\mathbb{Q})=\langle\rho,\tau\rangle$ (here $K=\mathbb{Q}$)

The correspondence is $L^{\#} \longleftrightarrow H\leq \mathrm{Gal}(L/k)$

where $L^H=\{\ell\in L \mid \sigma(\ell)=\ell \ \forall\sigma\in H\}$

$K' \longleftrightarrow \mathrm{Gal}(L/K')$

where L/K' is always Galois and K'/k is Galois iff $\mathrm{Gal}(L/K')\trianglelefteq\mathrm{Gal}(L/k)$

Ex $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2},\omega_3)$ are Galois over $\mathbb{Q}$, while $\mathbb{Q}(\sqrt[3]{2})$ is not.

We have proved

Thm Let L/k a Galois extension of number fields, $\mathfrak{q},\mathfrak{q}'$ prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$ prime ideal of $\mathcal{O}_k$. Then there is $\sigma\in\mathrm{Gal}(L/k)$ such that $\mathfrak{q}'=\sigma(\mathfrak{q})$

Coro $e(\mathfrak{q}/\mathfrak{p})=e(\mathfrak{q}'/\mathfrak{p})$ $\quad f(\mathfrak{q}/\mathfrak{p})=f(\mathfrak{q}'/\mathfrak{p})$

$\mathfrak{p}\mathcal{O}_L=(\mathfrak{q}_1\cdots\mathfrak{q}_r)^e$ where $efr=n$

We say that $\mathfrak{p}$ ramifies if $e(\mathfrak{q}/\mathfrak{p})>1$

Thm If p prime in $\mathbb{Z}$, then p ramifies in $\mathcal{O}_K \Leftrightarrow p\mid \mathrm{disc}\,K$

Ex If $k/\mathbb{Q}$ quadratic, $efr=2$. We have three cases for p

① ramified, $e=2$, $f=r=1$, $p\mathcal{O}_K=\mathfrak{p}^2$ finitely many since $p\mid\mathrm{disc}\,K$

It is the same as having $m(x)$ mod p with a double root or

$p \mid \operatorname{disc} m(x)$. Ex, $\mathbb{Q}(\sqrt{5})$, $p=5$ (5) $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = (\sqrt{5})^2$

(2) INERT, $e=1, f=2, r=1$ $p\mathcal{O}_K = \mathfrak{P}$. Ex, $p=3$ $x^2-5 \equiv x^2+1 \pmod 3$

(3) $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = (3)$

(3) SPLITS, $e=f=1, r=2$ $\mathfrak{P}\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$ Ex, $p=11$ $x^2-5 \equiv (x-4)(x+4) \pmod{11}$

(11) $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = (11, \sqrt{5}+4)(11, \sqrt{5}-4)$

$\operatorname{disc}(x^2-5) = 4 \cdot 5$, p IS A SQUARE IFF $\left(\frac{5}{p}\right) = 1$

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 5 \quad \text{SPLITS} \\ -1 & p \equiv \pm 2 \pmod 5 \quad \text{INERT} \\ 0 & p = 5 \quad \text{RAMIFIES} \end{cases}$$

Def Let L/K a Galois extension of number fields, $[L:K]=n$, $\mathfrak{P} \subseteq \mathcal{O}_K$ prime, $\mathfrak{P}\mathcal{O}_L = (\mathfrak{q}_1 \cdots \mathfrak{q}_r)^e$ $efr = n$.

The DECOMPOSITION GROUP of $\mathfrak{q}$ over $\mathfrak{P}$ is given by

$$D(\mathfrak{q}/\mathfrak{P}) = \{\sigma \in \operatorname{Gal}(L/K) \mid \sigma\mathfrak{q} = \mathfrak{q}\}$$

The INERTIA GROUP of $\mathfrak{q}$ over $\mathfrak{P}$ is given by

$$I(\mathfrak{q}/\mathfrak{P}) = \{\sigma \in \operatorname{Gal}(L/K) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \ \forall \alpha \in \mathcal{O}_L\}$$

We have that $I(\mathfrak{q}/\mathfrak{P}) \subseteq D(\mathfrak{q}/\mathfrak{P}) \subseteq \operatorname{Gal}(L/K)$ since

$\sigma\mathfrak{q} = \mathfrak{q} \Leftrightarrow \{\sigma(\alpha) \equiv 0 \pmod{\mathfrak{q}} \Leftrightarrow \alpha \equiv 0 \pmod{\mathfrak{q}}\}$

If $\sigma \in D(\mathfrak{q}/\mathfrak{P})$, it induces $\mathcal{O}_L/\mathfrak{q} \xrightarrow{\bar{\sigma}} \mathcal{O}_L/\mathfrak{q}$ an automorphism that fixes $\mathcal{O}_K/\mathfrak{P}$ (because σ fixes K).

Then $\bar{\sigma} \in \operatorname{Gal}(\mathcal{O}_L/\mathfrak{q} \,/\, \mathcal{O}_K/\mathfrak{P}) = \bar{G}$ (extensions of finite groups are always Galois).

Then we have $D \xrightarrow{\varphi} \bar{G}$. What is the kernel?

$\varphi(\sigma) =$ identity iff $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$ $\forall \alpha \in \mathcal{O}_L$ iff $\sigma \in I$.

We will eventually prove this

Thus, $1 \longrightarrow I(\mathfrak{q}/\mathfrak{P}) \longrightarrow D(\mathfrak{q}/\mathfrak{P}) \longrightarrow \operatorname{Gal}(\mathcal{O}_L/\mathfrak{q} \,/\, \mathcal{O}_K/\mathfrak{P}) \longrightarrow 0$

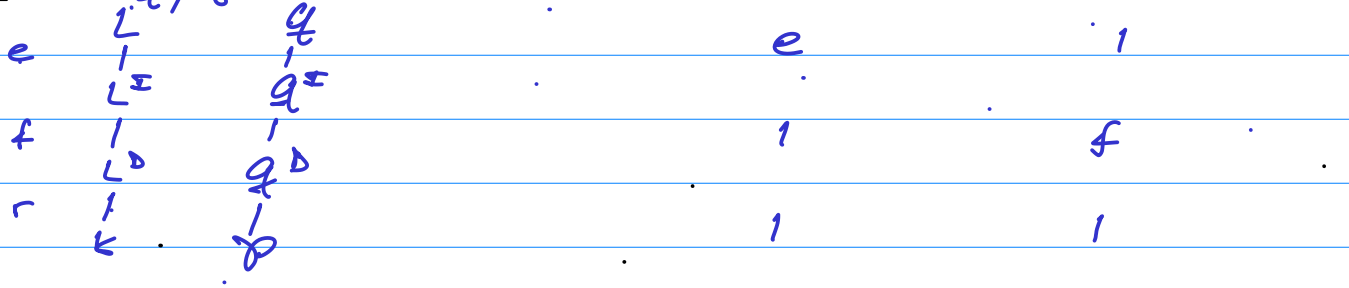
Let $H \leq \operatorname{Gal}(L/K)$. Recall

$$L^H = \{\ell \in L \mid \sigma(\ell) = \ell \ \forall \sigma \in H\}$$

If $X \subseteq L$, let $X^H = X \cap L^H$. Thus $\mathcal{O}_L^H = \mathcal{O}_L \cap L^H = \mathcal{O}_{(L^H)}$

$\mathfrak{q}^H = \mathfrak{q} \cap L^H$ is the prime lying under $\mathfrak{q}$ and above $\mathfrak{P}$.

Thm Fix $\mathfrak{q}/\mathfrak{P}$. We have



PROOF WE FIRST SHOW THAT $[L^D:k]=r$ BY GALOIS THEORY, WE HAVE $[L^D:k]=[G:D]$. EACH LEFT COSET σD SENDS $\mathcal{Q}$ TO $\sigma\mathcal{Q}$ AND $\sigma_1 D=\sigma_2 D$ IFF $\sigma_1\mathcal{Q}=\sigma_2\mathcal{Q}$. THE $\sigma\mathcal{Q}$ INCLUDE ALL THE PRIMES OF $\mathcal{O}_L$ LYING OVER $\mathfrak{P}$ AND THERE ARE r OF THEM. THEN $[L^D:k]=[G:D]=r$.

WE NOW SHOW $e(\mathcal{Q}^D/\mathfrak{P})=f(\mathcal{Q}^D/\mathfrak{P})=1$

$\mathcal{Q}$ IS THE ONLY PRIME OF $\mathcal{O}_L$ LYING OVER $\mathcal{Q}^D$ SINCE THE PRIMES LYING OVER $\mathcal{Q}^D$ ARE PERMUTED TRANSITIVELY BY $\mathrm{Gal}(L/L^D)=D$ WHICH FIXES $\mathcal{Q}$

THEN $ef=[L:L^D]=e(\mathcal{Q}/\mathcal{Q}^D)f(\mathcal{Q}/\mathcal{Q}^D)\leq ef$

$\Rightarrow e(\mathcal{Q}/\mathcal{Q}^D)=e$ AND $f(\mathcal{Q}/\mathcal{Q}^D)=f$, AND $e(\mathcal{Q}^D/\mathfrak{P})=f(\mathcal{Q}^D/\mathfrak{P})=1$

WE NOW SHOW $f(\mathcal{Q}/\mathcal{Q}^I)=1$ (THAT IS, $\mathcal{O}_L/\mathcal{Q}$ IS A TRIVIAL EXTENSION OF $\mathcal{O}_L^I/\mathcal{Q}^I$)

WE WILL SHOW THAT $\mathrm{Gal}(\mathcal{O}_L/\mathcal{Q}\,/\,\mathcal{O}_L^I/\mathcal{Q}^I)=\{1\}$.

LET $\bar{\alpha}\in\mathcal{O}_L/\mathcal{Q}$, $\alpha\in\mathcal{O}_L$ $\alpha=\bar{\alpha}$ CONSIDER

$g(x)=\prod_{\sigma\in I}(x-\sigma(\alpha))$, IT HAS COEFFICIENTS IN $\mathcal{O}_L^I$

REDUCING MODULO $\mathcal{Q}$, $\bar{g}\in(\mathcal{O}_L/\mathcal{Q})[x]$ HAS COEFFICIENTS IN $(\mathcal{O}_L^I/\mathcal{Q}^I)[x]$

NOW $\sigma(\alpha)$ REDUCES TO $\bar{\sigma}$ MODULO $\mathcal{Q}$ SINCE $\sigma(\bar{\alpha})=\sigma(\bar{\sigma})=\bar{\sigma}\pmod{\mathcal{Q}}$

HENCE $\bar{g}(x)=(x-\bar{\sigma})^{|I|}$. SINCE EVERY ELEMENT OF THE GALOIS GROUP SENDS $\bar{\sigma}$ TO $\bar{\sigma}$, WE GET $\mathrm{Gal}(\mathcal{O}_L/\mathcal{Q}\,/\,\mathcal{O}_L^I/\mathcal{Q}^I)=\{1\}\Rightarrow f(\mathcal{Q}/\mathcal{Q}^I)=1$

SINCE $f(\mathcal{Q}^D/\mathfrak{P})=1$, WE GET $f(\mathcal{Q}^I/\mathcal{Q}^D)=f(\mathcal{Q}/\mathfrak{P})=f$.

THEN $[L^I:L^D]\geq f$. BUT $D/I\hookrightarrow\overline{G}$ AND $|\overline{G}|=f\Rightarrow$

$[L^I:L^D]=|D/I|\leq f\Rightarrow[L^I:L^D]=f$

$\Rightarrow e(\mathcal{Q}^I/\mathcal{Q}^D)=1\Rightarrow[L:L^I]=e\quad e(\mathcal{Q}/\mathcal{Q}^I)=e$ #

COR IF $D\lhd G$, $\mathfrak{P}$ SPLITS INTO r DISTINCT PRIMES IN L^D.

IF $I\lhd G$ ALSO, THEN EACH PRIME REMAINS PRIME (INERT) IN L^I

EACH BECOMES AN e^{th} POWER IN L

PROOF: IF $D\lhd G$, THEN L^D/k IS GALOIS. WE HAVE $e(\mathcal{Q}^D/\mathfrak{P})=f(\mathcal{Q}^D/\mathfrak{P})=1$ AND THIS IS TRUE FOR EACH $\mathcal{Q}'\subset\mathcal{O}_{L^D}$ LYING OVER $\mathfrak{P}$. THEN THERE ARE r SUCH PRIMES. THEN THERE ARE r PRIMES IN $\mathcal{O}_{L^I}$ LYING OVER $\mathfrak{P}$. THEN $\mathcal{Q}'$ LIES UNDER A UNIQUE $\mathcal{Q}''$ OF $\mathcal{O}_{L^I}$. $\mathcal{Q}''$ COULD RAMIFY OVER $\mathcal{Q}'$.

IF $I\lhd G$, THEN L^I/k IS GALOIS. WE HAVE $e(\mathcal{Q}''/\mathfrak{P})=e(\mathcal{Q}^I/\mathfrak{P})=1$

$\Rightarrow e(\mathcal{Q}''/\mathcal{Q}')=1$. THEN $\mathcal{Q}'$ IS INERT IN L^I, $\mathcal{Q}''=\mathcal{Q}'\mathcal{O}_{L^I}$. THEN $\mathcal{Q}''$ BECOMES AN e^{th} POWER IN L #

EX CONSIDER $\mathbb{Q}(\sqrt{-23})\subseteq\mathbb{Q}(\omega_{23})$ BECAUSE $23\equiv-1\pmod 4$ AND

$\operatorname{disc}(\mathbb{Q}(\omega_{23}))=-23^{21}$. $\mathcal{O}_L=\mathbb{Z}[\omega_{23}]$

We have $\Phi_{23}(x)=x^{22}+\dots+1=(x^{11}+x^9+x^7+x^6+x^5+x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1) \pmod 2$

$\Rightarrow$ 2 splits into two primes in $\mathbb{Q}(\omega_{23})$. The decomposition field L^D has degree 2 over $\mathbb{Q}$. There is only one quadratic subfield since the Galois group is cyclic. Then $L^D=\mathbb{Q}(\sqrt{-23})$

In addition, 2 is unramified in $\mathbb{Q}(\omega_{23})\Rightarrow L^I=\mathbb{Q}(\omega_{23})$ #

Ex Let $L=\mathbb{Q}(i,\sqrt{2},\sqrt{3})$. It is Galois over $\mathbb{Q}$.

$\operatorname{Gal}(L/k)\cong\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$

5 splits into two primes in $\mathbb{Q}(i)$ because $x^2+1\equiv(x+2)(x+3) \pmod 5$

5 is inert in $\mathbb{Q}(\sqrt{2})$ $x^2-2 \pmod 5$ irreducible

$5=(\sqrt{5})^2$ ramifies in $\mathbb{Q}(\sqrt{5})$.

Then L must contain at least two primes lying over 5. And each must have $e\geq 2$, $f\geq 2$. It follows $e=f=r=2\Rightarrow[L^I:\mathbb{Q}]=4$ and 5 is unramified there $\Rightarrow L^I=\mathbb{Q}(i,\sqrt{2})$, $L^D=\mathbb{Q}(i)$. Thus $(2+i)(2-i)$ remain prime in $\mathbb{Q}(i,\sqrt{2})$ and become squares in L. #

Now consider L/k Galois and $k\subseteq k'\subseteq L$

Then $k'=L^H$ for some $H\leq\operatorname{Gal}(L/k)$ Moreover, L/L^H is Galois

For $\mathcal{Q}\subseteq\mathcal{O}_L$, let $\mathcal{P}'=\mathcal{Q}\cap\mathcal{O}_{L^H}$

Then we have $D(\mathcal{Q}/\mathcal{P}')=D(\mathcal{Q}/\mathcal{P})\cap H$, $I(\mathcal{Q}/\mathcal{P}')=I(\mathcal{Q}/\mathcal{P})\cap H$

By Galois theory, L^Dk', L^Ik' are the decomposition and inertia fields for $\mathcal{Q}$ over $\mathcal{P}'$.

Thm. ① L^D is the largest intermediate field k' such that $e(\mathcal{P}'/\mathcal{P})=f(\mathcal{P}'/\mathcal{P})=1$

② L^D is the smallest k' such that $\mathcal{Q}$ is the only prime of $\mathcal{O}_L$ lying over $\mathcal{P}'$

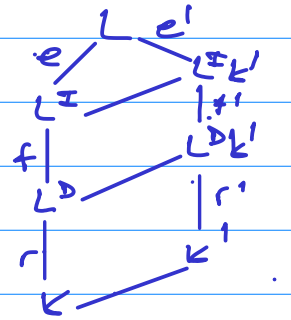
③ L^I is the largest k' such that $e(\mathcal{P}'/\mathcal{P})=1$

④ L^I is the smallest k' such that $\mathcal{Q}$ is totally ramified over $\mathcal{P}'$ ($e(\mathcal{Q}/\mathcal{P}')=[L:k']$)

Proof ② Let $k'=L^H$ such that $\mathcal{Q}$ is the only prime of $\mathcal{O}_L$ lying over $\mathcal{P}'$. For each $\sigma\in H$, $\sigma(\mathcal{Q})$ is a prime lying over $\mathcal{P}'\Rightarrow H\subseteq D(\mathcal{Q}/\mathcal{P}')\Rightarrow L^D\subseteq L^H=k'$

① Assume that $e(\mathcal{P}'/\mathcal{P})=f(\mathcal{P}'/\mathcal{P})=1$. We have $e=e'$, $f=f'$

$\Rightarrow[L:L^D]=[L:L^Dk']$ and $L^D\subseteq L^Dk'\Rightarrow L^D=L^Dk'\Rightarrow$



$k' \subseteq L^D$

③. IF $e(\mathfrak{P}'/\mathfrak{P})=1$, THEN $e=e' \Rightarrow L^I = L^I k' \Rightarrow k' \subseteq L^I$

④ IF $\mathfrak{q}$ IS TOTALLY RAMIFIED OVER $\mathfrak{P}'$, $[L:k']=e' \Rightarrow k' = L^I k' \Rightarrow L^I \subseteq k'$ #

DEF A PRIME $\mathfrak{P}$ IN $\mathcal{O}_k$ SPLITS COMPLETELY OR TOTALLY SPLITS IN L IF $\mathfrak{P}\mathcal{O}_L$ IS A PRODUCT OF $[L:k]$ PRIMES IN $\mathcal{O}_L \Leftrightarrow e_i=f_i=1 \ \forall i$

IF $\mathfrak{P}$ SPLITS COMPLETELY IN L, IT DOES SO IN ANY k', $k \subseteq k' \subseteq L$

COR IF $D \triangleleft G$ FOR SOME $\mathfrak{q}$ LYING OVER $\mathfrak{P}$, THEN $\mathfrak{P}$ SPLITS COMPLETELY IN K' IFF $k' \subset L^D$

PROOF: IF $\mathfrak{P}$ SPLITS COMPLETELY IN k', THEN $e(\mathfrak{P}'/\mathfrak{P}) = f(\mathfrak{P}'/\mathfrak{P})=1$ FOR $\mathfrak{P}' = \mathfrak{q} \cap \mathcal{O}_{k'}$. THEN $k' \subseteq L^D$ BY ① BY THM

CONVERSELY, $\mathfrak{P}$ SPLITS COMPLETELY IN L^D, HENCE THE SAME IS TRUE FOR $k \subseteq k' \subseteq L^D$ #

THM LET k BE A NUMBER FIELD, AND LET L AND M BE TWO EXTENSIONS OF k, $\mathfrak{P}$ PRIME OF $\mathcal{O}_k$. IF $\mathfrak{P}$ IS UNRAMIFIED (RESPECTIVELY, SPLITS COMPLETELY) IN BOTH L, M, THEN $\mathfrak{P}$ UNRAMIFIED (RESP. SPLITS COMPLETELY) IN LM

PROOF SUPPOSE $\mathfrak{P}$ IS UNRAMIFIED IN L, M. LET $\mathfrak{P}'$ IN LM LYING OVER $\mathfrak{P}$

WE WANT TO VERIFY THAT $e(\mathfrak{P}'/\mathfrak{P})=1$: LET F BE A GALOIS EXTENSION OF k CONTAINING LM. LET $\mathfrak{q}$ BE A PRIME OF F LYING OVER $\mathfrak{P}'$ (AND THUS OVER $\mathfrak{P}$). LET $I = I(\mathfrak{q}/\mathfrak{P})$ THE INERTIA GROUP. NOTICE THAT F^I CONTAINS L AND M, SINCE $\mathfrak{q} \cap L$ AND $\mathfrak{q} \cap M$ ARE UNRAMIFIED OVER $\mathfrak{P}$. THEN $LM \subseteq F^I \Rightarrow \mathfrak{q} \cap LM = \mathfrak{P}'$ IS UNRAMIFIED OVER $\mathfrak{P}$.

IF $\mathfrak{P}$ SPLITS COMPLETELY IN L, M, WE DO THE SAME WITH $D = D(\mathfrak{q}/\mathfrak{P})$ INSTEAD OF I #

COR LET $k \subseteq L$ NUMBER FIELD, $\mathfrak{P}$ PRIME IN k. IF $\mathfrak{P}$ IS UNRAMIFIED OR SPLITS COMPLETELY IN L, THEN THE SAME IS TRUE IN THE GALOIS CLOSURE M OF L (SMALLEST GALOIS EXTENSION M/k SUCH THAT $L \subseteq M$)

PROOF: NOTICE THAT $M = \prod_{\sigma: k\text{-EMBEDDINGS}} \sigma(L)$. IF $\mathfrak{P}$ IS UNRAMIFIED OVER L, THEN THE SAME IS TRUE IN $\sigma(L)$. THEN WE APPLY THE PREVIOUS THM. AND $\mathfrak{P}$ IS UNRAMIFIED IN M. WE DO THE SAME FOR SPLITS COMPLETELY #

THM LET k BE A NUMBER FIELD; $p \in \mathbb{Z}$ PRIME SUCH THAT $p \mid \operatorname{disc}(k)$. THEN p IS RAMIFIED IN k.

PROOF: FIX AN INTEGRAL BASIS $\alpha_1, \dots, \alpha_n$ OF $\mathcal{O}_k$. WE HAVE $\operatorname{disc}(k) = \det(\operatorname{Tr}_{k/\mathbb{Q}}(\alpha_i \alpha_j))$ REDUCING MODULO p, WE CAN THINK OF $\operatorname{disc}(k)$

in $\mathbb{Z}/p\mathbb{Z}$, and we have $\operatorname{disc}(k)\equiv 0 \pmod p$. This means that the rows are linearly dependent over $\mathbb{Z}/p\mathbb{Z}$. $\exists s_1,\dots,s_n\in\mathbb{Z}$ not all $\equiv 0 \pmod p$ such that $\sum_{i=1}^n s_i \operatorname{Tr}_{k/\mathbb{Q}}(\alpha_i\alpha_j)\equiv 0 \pmod p$ $\forall j$.

Set $\alpha=\sum_{i=1}^n s_i\alpha_i$. We have $p \mid \operatorname{Tr}_{k/\mathbb{Q}}(\alpha\alpha_j)$ $\forall j \Rightarrow \operatorname{Tr}_{k/\mathbb{Q}}(\alpha\mathcal{O}_k)\subseteq p\mathbb{Z}$

But $\alpha\notin p\mathcal{O}_k$ because not all s_i are divisible by p.

Suppose that p is unramified in k. Then $p\mathcal{O}_k$ is product of distinct primes and one of them does not contain α. Say $\alpha\notin\mathfrak{P}$ for $\mathfrak{P}$ lying over p.

Let L be the Galois closure of k over $\mathbb{Q}$. Then p is unramified in L. Fix $\mathfrak{q}$ in $\mathcal{O}_L$ lying over $\mathfrak{P}$. Then $\alpha\notin\mathfrak{q}$ since $\mathfrak{q}\cap\mathcal{O}_k=\mathfrak{P}$, and $\alpha\in\mathcal{O}_k$. Now $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\mathcal{O}_L)\subseteq p\mathbb{Z}$. To see this $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\mathcal{O}_L)=$
$=\operatorname{Tr}_{k/\mathbb{Q}}\operatorname{Tr}_{L/k}(\alpha\mathcal{O}_L)=\operatorname{Tr}_{k/\mathbb{Q}}(\alpha\operatorname{Tr}_{L/k}(\mathcal{O}_L))\subseteq\operatorname{Tr}_{k/\mathbb{Q}}(\alpha\mathcal{O}_k)\subseteq p\mathbb{Z}$,

Fix $\beta\in\mathcal{O}_L$, $\beta\notin\mathfrak{q}$ but $\beta\in$ all other primes of $\mathcal{O}_L$ lying over $\mathfrak{P}$ (this can be done by the Chinese Remainder Theorem). We claim

① $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\beta\mathcal{O}_L)\subseteq\mathfrak{q}$

② $\sigma(\alpha\beta\mathcal{O}_L)\subseteq\mathfrak{q}$ $\forall\sigma\in\operatorname{Gal}(L/\mathbb{Q})\setminus D(\mathfrak{q}/\mathfrak{P})$

① is clear since $\beta\in\mathcal{O}_L$ and $(p)\subseteq\mathfrak{q}$.

② We have $\sigma^{-1}(\mathfrak{q})\neq\mathfrak{q}$ since $\sigma\notin D(\mathfrak{q}/\mathfrak{P})$. Then $\beta\mathcal{O}_L\in\sigma^{-1}(\mathfrak{q})$
$\Rightarrow\sigma(\beta\mathcal{O}_L)\subseteq\mathfrak{q}\Rightarrow\sigma(\alpha\beta\mathcal{O}_L)\subseteq\mathfrak{q}$.

Thus ① and ② imply $\sum_{\sigma\in D(\mathfrak{q}/\mathfrak{P})}\sigma(\alpha\beta\mathcal{O}_L)\subseteq\mathfrak{q}$. This will lead to a contradiction. $\sigma\in D(\mathfrak{q}/\mathfrak{P})$ induces an automorphism of $\mathcal{O}_L/\mathfrak{q}$. We can reduce everything mod $\mathfrak{q}$: $\sum_{\sigma\in D(\mathfrak{q}/\mathfrak{P})}\overline{\sigma}(\overline{\alpha}\overline{\beta}\overline{\gamma})=0 \pmod{\mathfrak{q}}$ $\forall\gamma\in\mathcal{O}_L$ and $\overline{\alpha}\overline{\beta}\neq 0 \pmod{\mathfrak{q}}$ since $\alpha\beta\notin\mathfrak{q}\Rightarrow$

$\sum_{\sigma\in D(\mathfrak{q}/\mathfrak{P})}\overline{\sigma}(x)\equiv 0 \pmod{\mathfrak{q}}$ $\forall x\in\mathcal{O}_L/\mathfrak{q}$.

The $\overline{\sigma}$ are all distinct since $I(\mathfrak{q}/\mathfrak{P})$ is trivial as p is unramified in L. A sum of distinct automorphisms is never identically zero by independence of characters. Contradiction.

Lemma Let F be a field. $V=\{\sigma_1,\dots,\sigma_n: F\to F$ automorphisms$\}$. Any set $\{\sigma_1,\dots,\sigma_n\}\subseteq V$ is linearly independent.

Proof: Let $\sum_{i=1}^{\ell}a_i\sigma_i=0$, $a_i\in F$ with ℓ minimal such that all $a_i\neq 0$.

Fix x such that $\sigma_1(x)\neq\sigma_\ell(x)$. Since $\sum_{i=1}^{\ell}a_i\sigma_i(xy)=0$ $\forall y\in F$,

$\sum_{i=1}^{l} a_i \alpha_i(x)\alpha_i \equiv 0$. ALSO $\sum_{i=1}^{l} a_i \alpha_1(x)\alpha_i \equiv 0$. THEN

$\sum_{i=2}^{l} a_i (\alpha_i(x)-\alpha_1(x))\alpha_i \equiv 0$ CONTRADICTING MINIMALITY.

THE FROBENIUS AUTOMORPHISM

LET $K \subseteq L$ NUMBER FIELDS, $\mathfrak{p}$ A PRIME OF $\mathcal{O}_K$, $\mathfrak{q}$ A PRIME OF $\mathcal{O}_L$ LYING OVER $\mathfrak{p}$. WE HAVE

$$0 \to I(\mathfrak{q}/\mathfrak{p}) \to D(\mathfrak{q}/\mathfrak{p}) \xrightarrow{\Psi} Gal(\mathcal{O}_L/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p}) = \overline{G}$$

$\overline{G}$ HAS A SPECIAL ELEMENT. RECALL

$[\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}] = f(\mathfrak{q}/\mathfrak{p})$. THUS $|Gal(\mathcal{O}_L/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p})| = f(\mathfrak{q}/\mathfrak{p})$

$|\mathcal{O}_K/\mathfrak{p}| = N_K(\mathfrak{p})$ $|\mathcal{O}_L/\mathfrak{q}| = N_K(\mathfrak{p})^{f(\mathfrak{q}/\mathfrak{p})}$

DEF THE FROBENIUS AUTOMORPHISM OF $\mathfrak{q}$ OVER $\mathfrak{p}$ IS A $\phi \in Gal(\mathcal{O}_L/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p})$ DEFINED BY $\phi(\alpha) \equiv \alpha^{N_K(\mathfrak{p})} \pmod{\mathfrak{q}}$.

IT IS DEFINED UP TO INERTIA OVER A GENERATOR α OF $\mathcal{O}_L/\mathfrak{q} = \mathcal{O}_K/\mathfrak{p}(\alpha)$

THE ELEMENTS OF $\mathcal{O}_K/\mathfrak{p}$ ARE FIXED BY ϕ SINCE $\alpha^{p^k} = \alpha$ IN $\mathbb{F}_{p^k}$.

MOREOVER, ϕ GENERATES $\overline{G}$, WHICH IS CYCLIC. ϕ^e IS THE IDENTITY IFF $\alpha^{N_K(\mathfrak{p})^e} \equiv \alpha \pmod{\mathfrak{q}}$ IFF $f(\mathfrak{q}/\mathfrak{p}) \mid e$

NOW, SINCE $\phi(\alpha) \in \mathfrak{q}$ FOR $\alpha \in \mathfrak{q}$, WE HAVE $\phi \in D(\mathfrak{q}/\mathfrak{p})$ AND Ψ IS ONTO.

ϕ IS DENOTED BY $\phi(\mathfrak{q}/\mathfrak{p})$. IF $\mathfrak{p}$ IS UNRAMIFIED, $I(\mathfrak{q}/\mathfrak{p})$ IS TRIVIAL AND ϕ IS UNIQUELY DEFINED.

WE HAVE $\phi(\sigma\mathfrak{q}/\mathfrak{p}) = \sigma\phi(\mathfrak{q}/\mathfrak{p})\sigma^{-1}$ $\forall \sigma \in Gal(L/K)$

THE CONJUGACY CLASS OF $\phi(\mathfrak{q}/\mathfrak{p})$ IS UNIQUELY DETERMINED BY $\mathfrak{p}$.

WHEN $Gal(L/K)$ IS ABELIAN, $\phi(\mathfrak{q}/\mathfrak{p})$ IS UNIQUELY DETERMINED BY THE UNRAMIFIED PRIME $\mathfrak{p}$. HENCE

$$\phi(\alpha) \equiv \alpha^{N_K(\mathfrak{p})} \pmod{\mathfrak{q}} \quad \forall \mathfrak{q} \text{ LYING OVER } \mathfrak{p}.$$

$$\Rightarrow \quad \phi(\alpha) \equiv \alpha^{N_K(\mathfrak{p})} \pmod{\mathfrak{p}\mathcal{O}_L}$$

THM LET L/K BE A GALOIS EXTENSION OF NUMBER FIELDS, $\mathfrak{p}$ PRIME OF $\mathcal{O}_K$ UNRAMIFIED IN L. FOR $\mathfrak{q}$ OF L LYING OVER $\mathfrak{p}$, THERE IS A UNIQUE $\phi \in Gal(L/K)$ SUCH THAT $\phi(\alpha) \equiv \alpha^{N_K(\mathfrak{p})} \pmod{\mathfrak{q}}$ $\forall \alpha \in \mathcal{O}_L$

WHEN $Gal(L/K)$ ABELIAN, ϕ DEPENDS ONLY ON $\mathfrak{p}$ AND

$\phi(\alpha) \equiv \alpha^{N_K(\mathfrak{p})} \pmod{\mathfrak{p}\mathcal{O}_L}$ $\forall \alpha \in \mathcal{O}_L$

NOTICE THAT $\phi(\mathfrak{q}/\mathfrak{p})$ HAS ORDER $f(\mathfrak{q}/\mathfrak{p})$, SO $\phi(\mathfrak{q}/\mathfrak{p})$ INDICATES HOW $\mathfrak{p}$ SPLITS IN L. AN UNRAMIFIED PRIME $\mathfrak{p}$ SPLITS COMPLETELY IN A GALOIS EXTENSION IFF $\phi=1$

EX: LET $L=\mathbb{Q}(\omega_m)$, $\omega_m=e^{2\pi i/m}$ $k=\mathbb{Q}$. THEN $\mathrm{Gal}(L/k)=(\mathbb{Z}/m\mathbb{Z})^\times$ $\sigma\in\mathrm{Gal}(L/k)\longrightarrow t\in(\mathbb{Z}/m\mathbb{Z})^\times$ IFF $\sigma(\omega_m)=\omega_m^t$.

THE UNRAMIFIED PRIMES ARE THE ODD $p\nmid m$ AND 2 WHEN $m\equiv 2 \pmod 4$. (THIS COMES FROM $\mathrm{disc}(\omega_m)\mid m^{\varphi(m)}$, SEE HASSE, PAGE 29)

THE GALOIS GROUP IS ABELIAN, SO $\phi(\alpha)\equiv\alpha^p \pmod{p\mathbb{Z}[\omega_m]}$

$\phi\left(\sum a_i\omega_m^i\right)=\sum a_i\omega_m^{pi} \pmod p$ (SINCE $a_i\in\mathbb{Z}/p\mathbb{Z}$)

THUS, $\sum a_i\omega_m^{pi}\equiv\left(\sum a_i\omega_m^i\right)^p \pmod p$

IF $p\nmid m$, THEN f IS THE ORDER OF $p \pmod m$, SINCE THE ORDER OF FROBENIUS IS f, THEN

THM IF $p\nmid m$, THEN p SPLITS INTO $\frac{\varphi(m)}{f}$ DISTINCT PRIME IDEALS IN $\mathbb{Z}[\omega_m]$, WHERE f IS THE ORDER OF p MODULO m.

EX CONSIDER $\mathbb{Q}(\omega_{23})$ THEN $2^{11}\equiv 2\cdot(25)^2\equiv 2\cdot 2^2\equiv 2(-11)\equiv 1 \pmod{23}\Rightarrow$ 2 SPLITS INTO TWO PRIMES, $[G:D]=2\Rightarrow L^D=\mathbb{Q}(\sqrt{-23})$

2 IS UNRAMIFIED IN $\mathbb{Q}(\omega_{23})\Rightarrow L^F=\mathbb{Q}(\omega_{23})$

$x^{22}+\cdots+1\equiv(x^{11}+x^9+x^7+x^6+x^5+x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1) \pmod{23}$