Rmk If G is abelian, $D(\mathfrak{P}|\mathfrak{q}), \dots$ only depend on $\mathfrak{q}$ (and L). $\rightsquigarrow D_{L|K}(\mathfrak{q}), I_{L|K}(\mathfrak{q}), \mathrm{Frob}_{L|K}(\mathfrak{q})$

Rmk If K is complete w.r.t. a disc. val. v, $\mathcal{O}_K = \mathcal{O}_v$ and $\mathcal{O}_L$ have just one max. id. $\rightsquigarrow \underbrace{D(L|K)}_{= \,\mathrm{Gal}(L|K)}, I(L|K), \mathrm{Frob}(L|K)$,

Rmk

$$
\begin{array}{ccccc}
 & M & \mathcal{O}_M & P \\
 & \mid H & \mid & \mid \\
G & L & \mathcal{O}_L & \mathfrak{P} \\
 & \mid & \mid & \mid \\
 & K & \mathcal{O}_K & \mathfrak{q}
\end{array}
$$

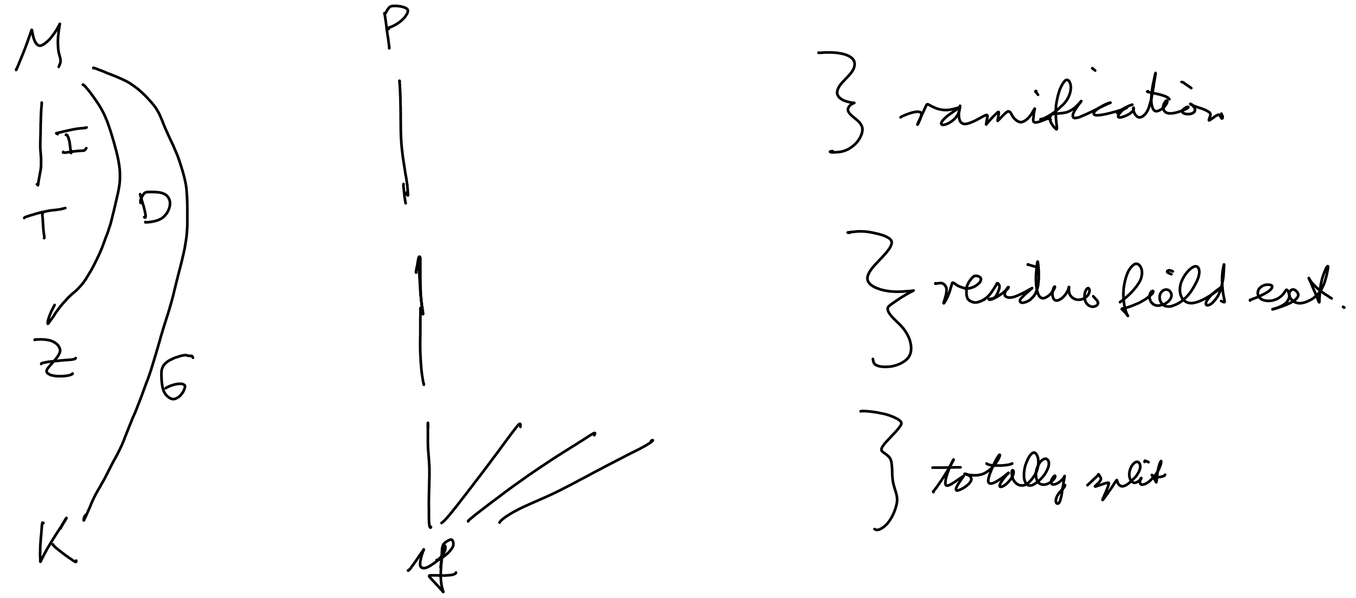
$$D(P|\mathfrak{P}) = D(P|\mathfrak{q}) \cap H$$
$$I \qquad\qquad\quad I$$

If $L|K$ is Galois, then

$D(\mathfrak{P}|\mathfrak{q})$ = image of $D(P|\mathfrak{q})$ under the restriction $G \to G/H$

$I \qquad\qquad\qquad\qquad\qquad I$

In particular, $\mathfrak{P}|\mathfrak{q}$ unramified $\Leftrightarrow I(P|\mathfrak{q}) \subseteq H$.



<u>Ex</u> $L = \mathbb{Q}(\zeta_\infty)$, $K = \mathbb{Q}$

$$I_{\mathbb{Q}(\zeta_\infty)|\mathbb{Q}}(p) \subseteq Gal(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}) = \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$$

If $p \nmid m$, then $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ is unram. at p.

$$\Rightarrow I(p) \subseteq Gal(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}(\zeta_m))$$
$$= \{ x \in \hat{\mathbb{Z}}^\times \mid \underbrace{x \equiv 1 \bmod m}_{\Leftrightarrow\ \zeta_m^x = \zeta_m} \}$$

$$\Rightarrow I(p) \subseteq \mathbb{Z}_p^\times$$

For any $k \geq 0$, $\mathbb{Q}(\zeta_{p^k})|\mathbb{Q}$ is totally ramified at p.

$\Rightarrow$ The restriction of the restriction map

$$\underset{\hat{\mathbb{Z}}^\times}{\underset{\parallel}{Gal(\mathbb{Q}(\zeta_\infty)|\mathbb{Q})}} \twoheadrightarrow \underset{(\mathbb{Z}/p^k\mathbb{Z})^\times}{\underset{\parallel}{Gal(\mathbb{Q}(\zeta_{p^k})|\mathbb{Q})}}$$

to $I(p)$ is surjective.

$\Rightarrow I(p) \cap U \neq \emptyset \qquad \forall$ open $\emptyset \neq U \subseteq \mathbb{Z}_p^\times$

$$\underset{\substack{\uparrow \\ I(p) \text{ closed}}}{\Rightarrow} \quad \boxed{I(p) = \mathbb{Z}_p^\times}.$$

max. ext. $Z_p \subseteq \mathbb{Q}(\zeta_\infty)$ unram. at p:

$$Z_p = \bigcup_{\substack{m \geq 1: \\ p \nmid m}} \mathbb{Q}(\zeta_m) \qquad (\text{field fixed by } \mathbb{Z}_p^\times)$$

$$\mathrm{Frob}_{Z_p|\mathbb{Q}}(p) = \underset{\substack{\parallel \\ (p,p,\dots)}}{p} \in \underset{\substack{\ell \neq p}}{\prod} \mathbb{Z}_\ell^\times = \mathrm{Gal}(Z_p|\mathbb{Q})$$

$$\prod_{\ell \neq p} \mathbb{Z}_\ell^\times \subseteq \hat{\mathbb{Z}}^\times$$

($\zeta_m \mapsto \zeta_m^p \Rightarrow$ induces Frobenius aut. $x \mapsto x^p$ in the residue field extension).

<u>Ex</u> Let K be a local field with residue field $\mathbb{F}_q$.

$\Rightarrow$ The max. unram. ext. of K is

$$\bigcup_{n \geq 1} K(\zeta_{q^n-1}) = \bigcup_{\substack{m \geq 1: \\ \gcd(m,q)=1}} K(\zeta_m).$$

<u>Pf</u> See problem 2 on problem set 3. $\square$

3. Chebotarev density theorem

Thm 3.1 Let K be a number field and $n \geq 1$.
Then, the following are equivalent:

a) $\forall p \equiv p' \bmod n$ prime numbers:
p and p' split in the same way in $\mathcal{O}_K$
$\left(p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \quad p'\mathcal{O}_K = \mathfrak{P}_1'^{e_1} \cdots \mathfrak{P}_r'^{e_r}, \right.$

$\left. \kappa(\mathfrak{P}_i) = \kappa(\mathfrak{P}_i') \ \forall i \right)$

b) $K \subseteq \mathbb{Q}(\zeta_n)$.

c) $\forall p \equiv p' \bmod n$ prime numbers:
If p splits completely in K, then p' splits completely in K.

Pf a) $\Rightarrow$ c) clear

b) $\Rightarrow$ a) Case 1: $p, p' \nmid n$

$\Rightarrow p, p'$ unram. in $\mathbb{Q}(\zeta_n)$
$\qquad$ – " – – $\quad K$ (with $\mathbb{Q}(\zeta_n) \supseteq K$)

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) &= (\mathbb{Z}/n\mathbb{Z})^\times \\
\mathrm{Frob}(p) &= p \bmod n \\
&\quad \| \\
\mathrm{Frob}(p') &= p \bmod n
\end{aligned}$$

$\Rightarrow \mathrm{Frob}_{\mathbb{Q}(\zeta_n)}(p) = \mathrm{Frob}_{\mathbb{Q}(\zeta_n)}(p')$

$\Rightarrow \mathrm{Frob}_K(p) = \mathrm{Frob}_K(p')$

$\Rightarrow D_K(p) = D_K(p')$

$\Rightarrow p, p'$ split in the same way in K.

Case 2: $p \mid n$ or $p' \mid n$

Since $p \equiv p' \bmod n$, this implies $p = p'$. $\square$

c) $\Rightarrow$ b) today's goal!

Chebotarev density theorem (Чеботарёв, Чоботарьов)

Let K be a number field and $L|K$ a finite Galois extension with Galois group G. Let C be a conjugacy class in G. Then, the density of primes $\mathfrak{q} \subset \mathcal{O}_K$ with $\mathrm{Frob}_{L|K}(\mathfrak{q}) = C$, when ordered by norm $N(\mathfrak{q})$,

is $\dfrac{\#C}{\#G}$. More precisely:

$$\lim_{X \to \infty} \frac{\#\{\mathfrak{q} : N(\mathfrak{q}) \leq X,\ \mathrm{Frob}_{L|K}(C)\}}{\#\{\mathfrak{q} : N(\mathfrak{q}) \leq X\}} = \frac{\#C}{\#G}.$$

(Frob only makes sense for unram. $\mathfrak{q}$, but the finitely many ramified primes don't matter as $X \to \infty$.)

Ex ($\mathbb{Q}(\zeta_n)|\mathbb{Q}$) (Dirichlet's theorem on primes in arithmetic progressions)

$\Rightarrow$ For any $c \in (\mathbb{Z}/n\mathbb{Z})^\times$, the density of prime numbers p s.t. $p \equiv c \mod n$ is

$\frac{1}{\#(\mathbb{Z}/n\mathbb{Z})^\times} = \frac{1}{\varphi(n)}$. (All invertible residues mod n occur "equally often".)

Ex ($G = S_3$)   in L in $F = L^{\langle(23)\rangle}$

$C_1 = \{id\}$ $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_6 = \mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$

$\Rightarrow D = \{id\}$

for $\frac{1}{6}$ of $\mathfrak{q}$

$C_2 = \{(12), (13), (23)\}$

$\Rightarrow D =$ group of order 2 $\mathfrak{q} = \mathfrak{q}_1 \mathfrak{q}_2 \mathfrak{q}_3 = \underset{f=1}{\underset{\uparrow}{\mathfrak{P}_1}} \; \underset{f=2}{\underset{\uparrow}{\mathfrak{P}_2}}$

for $\frac{1}{2}$ of $\mathfrak{q}$

$C_3 = \{(123), (132)\}$

$\Rightarrow D = \langle(123)\rangle$ $\mathfrak{q} = \mathfrak{q}_1 \mathfrak{q}_2 = \underset{f_1=3}{\underset{\uparrow}{\mathfrak{P}_1}}$

for $\frac{1}{3}$ of $\mathfrak{q}$

Pf of Chebotarev density theorem

cf. last chapter of Neukirch: Alg. Number Theory

Pf of c) $\Rightarrow$ b) in Thm 1

p splits completely in K if and only if p splits completely in the Galois closure of $K|\mathbb{Q}$.
(See problem 1 on problem set 4.)

$\Rightarrow$ We can assume that K is a Galois extension of $\mathbb{Q}$.

An (unram.) prime p splits completely in K if and only if $\mathrm{Frob}_{K|\mathbb{Q}}(p) = \{id\}$.

Let L be the compositum of K and $\mathbb{Q}(\zeta_n)$.

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathrm{Gal}(L|\mathbb{Q}) \arrow[dl] \arrow[dr] & \\
\mathrm{Gal}(K|\mathbb{Q}) & & \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \arrow[d, phantom, "\parallel"] \\
 & & (\mathbb{Z}/n\mathbb{Z})^\times
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathrm{Frob}_{L|\mathbb{Q}}(\mathfrak{P}|p) \arrow[dl] \arrow[dr] & \\
\mathrm{Frob}_{K|\mathbb{Q}}(\mathfrak{P}\cap K|p) & & \mathrm{Frob}(\mathfrak{P}\cap\mathbb{Q}(\zeta_n)|p)
\end{tikzcd}$$

Assume $K \not\subseteq \mathbb{Q}(\zeta_n)$. $\Rightarrow \mathrm{Gal}(L|K) \not\supseteq \mathrm{Gal}(L|\mathbb{Q}(\zeta_n))$.

$\Rightarrow \exists \sigma \in \mathrm{Gal}(L|\mathbb{Q}) : \sigma \notin \mathrm{Gal}(L|K)$, $\sigma \in \mathrm{Gal}(L|\mathbb{Q}(\zeta_n))$

$$\begin{array}{ccc}
\sigma \notin \mathrm{Gal}(L|K) & & \sigma \in \mathrm{Gal}(L|\mathbb{Q}(\zeta_n)) \\
\Updownarrow & & \Updownarrow \\
\sigma|_K \neq id & & \sigma|_{\mathbb{Q}(\zeta_n)} = id.
\end{array}$$

$$\begin{tikzcd}
 & id \arrow[dl] \arrow[dr] & \\
id & & id \arrow[d, phantom, "\parallel"] \\
 & & 1 \bmod p
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \sigma \arrow[dl] \arrow[dr] & \\
\neq id & & id \arrow[d, phantom, "\parallel"] \\
 & & 1 \bmod n
\end{tikzcd}$$

By Chebotarev's density theorem, there exist p, p' such that $\mathrm{Frob}_L(p) = \mathrm{id}$, $\mathrm{Frob}_L(p') =$ conjugacy class containing.

$\Downarrow$ p splits completely in K

$\Downarrow$ $p \equiv 1 \bmod n$

$\Downarrow$ p' doesn't split completely in K

$\Downarrow$ $p' \equiv 1 \bmod n$.

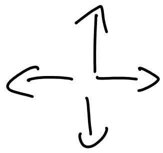
$↯$.

$\square$

<u>Ex of Thm 1</u> $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{|4n|})$, so the splitting behavior of p in $\mathbb{Q}(\sqrt{n})$ is determined by $p \bmod 4n$.

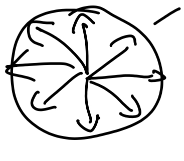
<u>Pf</u> It suffices to show this for primes $n = \ell$ and $n = -1$.

<u>Case $n = -1$:</u>



$$\sqrt{-1} = i = \zeta_4$$

<u>Case $n = \ell = 2$:</u>



$$\zeta_8 = \frac{\sqrt{2} + i \cdot \sqrt{2}}{2}$$

$$\zeta_8 + \zeta_8^{-1} = \sqrt{2}.$$

<u>Case $n = \ell$ odd:</u>

Quadr. subext. of $\mathbb{Q}(\zeta_\ell) \longleftrightarrow$ index two subgroups $H \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)|\mathbb{Q}) = (\mathbb{Z}/\ell\mathbb{Z})^\times$

$\exists$ only one such subgroup (because $(\mathbb{Z}/\ell\mathbb{Z})^\times = \mathbb{F}_\ell^\times$ is cyclic):

$$H = \{x \in (\mathbb{Z}/\ell\mathbb{Z})^\times \text{ quadr. res.}\}$$

Look at $\alpha = \sum_{x \in (\mathbb{Z}/l\mathbb{Z})^\times} \left(\frac{x}{l}\right) \zeta_l^x$ (Gaußsum).

$$\phi_y(\alpha) = \sum_x \left(\frac{x}{l}\right) \zeta_l^{xy} = \sum_x \left(\frac{x/y}{l}\right) \zeta_l^x = \left(\frac{y}{l}\right) \sum_x \left(\frac{x}{l}\right) \zeta_l^x$$

$$= \left(\frac{y}{l}\right) \cdot \alpha = \pm \alpha .$$

(In part., $\phi_y(\alpha^2) = \alpha^2 \ \forall y$, so $\alpha^2 \in \mathbb{Q}$.
That's why we look at the Gaußsum!)

$$\alpha^2 = \sum_{x_1, x_2} \left(\frac{x_1 x_2}{l}\right) \zeta_l^{x_1 + x_2}$$

$$= \sum_{x_1, x_2} \left(\frac{x_2/x_1}{l}\right) \zeta_l^{x_1 + x_2}$$

$$= \sum_{x_1, t} \left(\frac{t}{l}\right) \zeta_l^{x_1(1+t)}$$

$$= \sum_{t \in \mathbb{F}_l^\times} \left(\frac{t}{l}\right) \underbrace{\sum_{x_1 \in \mathbb{F}_l^\times} \zeta_l^{x_1(1+t)}}_{\substack{-1 \text{ if } t \neq -1 \\ l-1 \text{ if } t = -1}}$$

$$= \left(\frac{-1}{l}\right) \cdot l - \sum_t \left(\frac{t}{l}\right)$$

$$= \left(\frac{-1}{l}\right) \cdot l = \pm l .$$

$\Rightarrow \sqrt{c}$ or $\sqrt{-c} \in \mathbb{Q}(\zeta_c)$

$\overset{\uparrow}{\Rightarrow} \sqrt{c} \in \mathbb{Q}(\zeta_{4c})$. $\square$

$\sqrt{-1} \in \mathbb{Q}(\zeta_4)$