$$
\begin{tikzcd}[column sep=small]
& L \arrow[dd, dash] \arrow[dr, dash] & \\
& & \mathbf{Q}(x) \arrow[dd, dash] \\
& \mathbf{Q}(\zeta_8) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbf{Q}(i\sqrt{2}) \arrow[dr, dash] & \mathbf{Q}(i) \arrow[d, dash] & \mathbf{Q}(\sqrt{2}) \arrow[dl, dash] \\
& \mathbf{Q} &
\end{tikzcd}
\qquad \mathrm{Gal}(L, \bullet) \qquad
\begin{tikzcd}[column sep=small]
& \{e\} \arrow[dd, dash] \arrow[dr, dash] & \\
& & \langle s \rangle \arrow[dd, dash] \\
& \langle r^2 \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle r^2, s' \rangle \arrow[dr, dash] & \langle r \rangle \arrow[d, dash] & \langle r^2, s \rangle \arrow[dl, dash] \\
& \langle r, s \rangle &
\end{tikzcd}
$$

Lemma 0.1 *Soit $L \mid \mathbf{Q}$ une extension Galoisienne de groupe G et soit H un sous-groupe distingué de G et je note $E := L^H$. Soit $\mathfrak{P}$ un idéal de $\mathcal{O}_L$ et $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_E$ et $p := \mathfrak{P} \cap \mathbf{Z}$. Alors :*

$$D(\mathfrak{p}; E \mid \mathbf{Q}) \equiv D(\mathfrak{P}; L \mid \mathbf{Q}) \pmod{H}$$

Nous allons utiliser ce lemme avec $H = \langle r \rangle$. Si $\chi_{-4}(p) = 1$ alors $D(\mathfrak{P}; L \mid \mathbf{Q}) \subset H$. Ensuite, nous allons séparé les différents cas.

Important Dans ce qui suit je me place sous l'hypothèse $\chi_{-4}(p) = 1$.

1. Dans ce cas, le groupe de décomposition $D(\mathfrak{P}; L \mid E) = D(\mathfrak{P}; L \mid \mathbf{Q}) \cap \langle s \rangle = \{e\}$ c'est-à-dire que l'extension résiduel $[\kappa(\mathfrak{P}) : \kappa(\mathfrak{P} \cap \mathcal{O}_E)]$ est triviale.

2. Nous allons regarder la situation sur $\mathbf{Q}(\sqrt{2})$. Alors

$$D(\mathfrak{P}; L \mid \mathbf{Q}(\sqrt{2})) \equiv D(\mathfrak{P}; L \mid \mathbf{Q}) \pmod{\langle r^2, s \rangle}$$

Ensuite, on peut séparer les différents cas :

(i) Si $D(\mathfrak{P}; L \mid \mathbf{Q}) = \{e\}$, alors

$$D(\mathfrak{P} \cap \mathcal{O}_{\mathbf{Q}(\sqrt{2})}; \mathbf{Q}(\sqrt{2}) \mid \mathbf{Q}) = \{e\} \qquad D(\mathfrak{P}; L \mid \mathbf{Q}(\sqrt{2})) = \{e\}$$

(ii) Si $D(\mathfrak{P}; L \mid \mathbf{Q}) = \{e, r^2\}$ alors

$$D(\mathfrak{P} \cap \mathcal{O}_{\mathbf{Q}(\sqrt{2})}; \mathbf{Q}(\sqrt{2}) \mid \mathbf{Q}) = \{e, r^2\} \qquad D(\mathfrak{P}; L \mid \mathbf{Q}(\sqrt{2})) = \{e\}$$

(iii) Si $D(\mathfrak{P}; L \mid \mathbf{Q}) = \{e, r, r^2, r^3\}$ alors

$$D(\mathfrak{P} \cap \mathcal{O}_{\mathbf{Q}(\sqrt{2})}; \mathbf{Q}(\sqrt{2}) \mid \mathbf{Q}) = \{e, r^2\} \qquad D(\mathfrak{P}; L \mid \mathbf{Q}(\sqrt{2})) = \{e, \overline{r}\}$$

On en déduit la loi de décomposition suivante selon les cas (en indice j'ai donné les indices résiduels):

$$
\begin{tikzcd}[column sep=small]
& (\bullet)(\bullet)(\bullet)(\bullet) \arrow[d, dash] \\
& (\bullet)(\bullet) \arrow[dl, dash] \\
(p) &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
& (\bullet)_2(\bullet)_2 \arrow[d, dash] \\
& (\bullet)_2 \arrow[dl, dash] \\
(p) &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
& (\bullet)_4 \arrow[d, dash] \\
& (\bullet)_2 \arrow[dl, dash] \\
(p) &
\end{tikzcd}
$$

cas (i) cas (ii) cas (iii)

3. Utilisation de la théorie des formes binaires quadratiques Il s'agit de donner un critère pour calculer les groupes de décomposition i.e séparation des 3 cas.

Important Pas de démonstration, je veux juste énoncé un truc qui semble fonctionner.

Enoncé Toujours sous l'hypothèse $\chi_{-4}(p) = 1$.

- p est représenté par $q_0(x, y) := x^2 + 64y^2$, alors $D(\mathfrak{P}; L \mid \mathbf{Q}) = \{e\}$ et la décomposition de p dans $\mathcal{O}_E$ est donné par le cas (i).
- p est représenté par $q_1(x, y) := 4x^2 + 4xy + 17y^2$ alors $D(\mathfrak{P}; L \mid \mathbf{Q}) = \{e, r\}$ et la décomposition de p dans $\mathcal{O}_E$ est donné par le cas (ii).
- p est représenté par $q_1(x, y) := 5x^2 + 2xy + 13y^2$ alors $D(\mathfrak{P}; L \mid \mathbf{Q}) = \{e, r, r^2, r^3\}$ et la décomposition de p dans $\mathcal{O}_E$ est donné par le cas (iii).