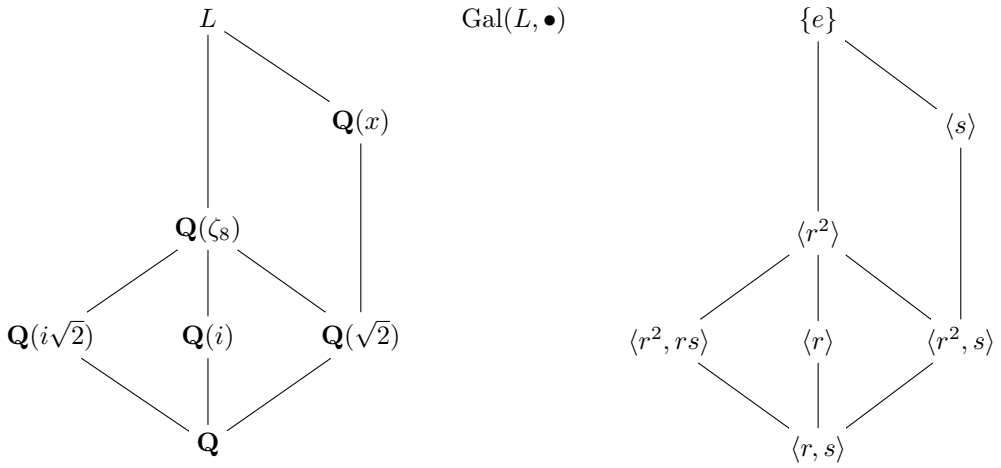
Nous allons étudier d'un point de vue arithmétique la situation suivante :



Le corps L est la clôture Galoisienne de $E := \mathbf{Q}(x)$ où x est une racine de $X^4 - 2$. (TODO expliquer proprement les deux diagrammes et la représentation de D_4 que l'on prend). Le résultat que l'on veut étudier est :

http://www.ams.org/journals/bull/2016-53-01/S0273-0979-2015-01515-6/S0273-0979-2015-01515-6.pdf

Où l'on trouve, à la page 10, une description explicite des Frobenius de $L \mid \mathbf{Q}$.

Le résultat

(i) $D(\mathfrak{P}; L \mid \mathbf{Q}) \subset \langle r^2 \rangle$ si et seulement si $p = 1 \pmod 8$.

(ii) $D(\mathfrak{P}; L \mid \mathbf{Q}) = \langle r \rangle$ si et seulement si $p = 5 \pmod 8$.

(iii) $D(\mathfrak{P}; L \mid \mathbf{Q}) \in \{\langle s \rangle, \langle r^2 s \rangle\}$ si et seulement si $p = 7 \pmod 8$.

(iv) $D(\mathfrak{P}; L \mid \mathbf{Q}) \in \{\langle rs \rangle, \langle r^3 s \rangle\}$ si et seulement si $p = 3 \pmod 8$.

Dans le texte en lien on trouve une distinction du cas (i) en deux sous-cas permettant d'identifier la classe de conjugaison du Frobenius pour tous les nombres premiers. Nous n'allons pas obtenir cette distinction qui constitue un résultat profond. Par contre, nous allons entreprendre l'étude arithmétique de l'extension $\mathbf{Q}(x) \mid \mathbf{Q}$ et mettant à profit l'action du groupe de Galois de $L \mid \mathbf{Q}$ sur les plongements de $\mathbf{Q}(x)$ dans L et les résultats obtenu dans ArtinLVsZetaE.pdf.

On souhaites comprendre les groupes de décomposition des idéaux premiers des différents anneaux d'entiers des extensions présentent dans ce diagramme. Nous allons utiliser deux ingrédients.

Lemma 0.1 (Cyclotomie) *Soit $\mathfrak{P}$ un idéal premier de l'anneau des entiers de $\mathbf{Q}(\zeta_8)$, alors :*

$$D(\mathfrak{P}; \mathbf{Q}(\zeta_8) \mid \mathbf{Q}) = \langle \mathfrak{P} \cap \mathbf{Z} \rangle$$

Et un résultat technique concernant les groupes de décompositions :

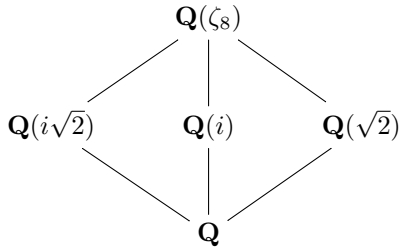
Lemma 0.2 (Lemme de réduction) *Soit $L \mid \mathbf{Q}$ une extension Galoisienne de groupe G et soit H un sous-groupe distingué de G et je note $K := L^H$. Soit $\mathfrak{P}$ un idéal de $\mathcal{O}_L$ et $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ et $p := \mathfrak{P} \cap \mathbf{Z}$. Alors :*

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

et (sans l'hypothèse que H est distingué) :

$$D(\mathfrak{P}; L \mid K) = D(\mathfrak{P}; L \mid \mathbf{Q}) \cap H$$

Etude préliminaire Nous allons commencer par examiner le pied du diagramme, pour mettre en pratique l'utilisation des deux lemmes. Une remarque importante, ici on oublie complètement le groupe D_4 et on considère la situation indépendante de la précédente (mauvaise idée ?):



Soit $p \in \mathbf{Z}$ un nombre premier $\neq 2$ et soit $\mathfrak{P}$ un idéal de l'anneau des entiers de $\mathbf{Q}(\zeta_8)$. Alors d'après le lemme cyclotomique :

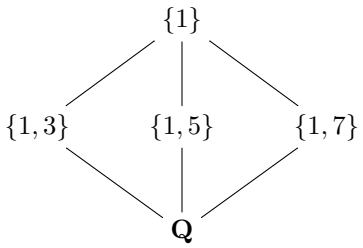
(i) Si $p = 1 \pmod 8$, alors $D(\mathfrak{P}; \mathbf{Q}(\zeta_8) \mid \mathbf{Q}) = \{1\}$.

(i) Si $p = 3 \pmod 8$, alors $D(\mathfrak{P}; \mathbf{Q}(\zeta_8) \mid \mathbf{Q}) = \{1, 3\}$.

(i) Si $p = 5 \pmod 8$, alors $D(\mathfrak{P}; \mathbf{Q}(\zeta_8) \mid \mathbf{Q}) = \{1, 5\}$.

(i) Si $p = 7 \pmod 8$, alors $D(\mathfrak{P}; \mathbf{Q}(\zeta_8) \mid \mathbf{Q}) = \{1, 7\}$.

Etude des sous-extensions Nous donnons le diagramme de la correspondance Galoisienne i.e utilisation de $\mathbf{Gal}(\mathbf{Q}(\zeta_8) \mid \bullet)$ à partir du diagramme des sous-extension.



L'extension $\mathbf{Q}(i\sqrt{2})$ Je me limite à l'étude de cette extension les autres étant similaire. D'une part, $\mathbf{Q}(i\sqrt{2}) = \mathbf{Q}(\zeta_8)^{\{1,3\}}$ et son anneau d'entier est $\mathbf{Z}[i\sqrt{2}]$ (juste pour fixé la notation).

Soit p un premier de $\mathbf{Z}$, $\mathfrak{P}$ un idéal de l'anneau des entiers de $\mathbf{Q}(\zeta_8)$ divisant p et $\mathfrak{p} := \mathfrak{P} \cap \mathbf{Z}[i\sqrt{2}]$. Alors le lemme de réduction nous donne :

$$D(\mathfrak{p}; \mathbf{Q}(i\sqrt{2}) \mid \mathbf{Q}) = D(\mathfrak{P}; \mathbf{Q}(\zeta_8) \mid \mathbf{Q}) \pmod{\{1, 3\}}$$

et en combinant les deux résultats :

$$D(\mathfrak{p}; \mathbf{Q}(i\sqrt{2}) \mid \mathbf{Q}) = \langle p \rangle \pmod{\{1, 3\}}$$

On en déduit :

(i) $p = 1, 3 \pmod 8$ si et seulement si $\#D(\mathfrak{p}; \mathbf{Q}(i\sqrt{2}) \mid \mathbf{Q}) = 1$.

(ii) Si $p = 5, 7 \pmod 8$ si et seulement si $\#D(\mathfrak{p}; \mathbf{Q}(i\sqrt{2}) \mid \mathbf{Q}) = 2$.

Remarque Bien faire attention a oeuf poule, car on retrouve la loi complémentaire de la réciprocité quadratique, c'est a reprendre complètement en particulier le lemme cyclotomique.

Retour sur l'exemple complet

Remarque Je ne suis pas complètement satisfait, donc je vais refaire quand j'aurais mieux compris.

Théorème 0.3 *(i)* $D(\mathfrak{P}; L \mid \mathbf{Q}) \subset \langle r^2 \rangle$ *si et seulement si* $p = 1 \pmod 8$.

(ii) $D(\mathfrak{P}; L \mid \mathbf{Q}) = \langle r \rangle$ *si et seulement si* $p = 5 \pmod 8$.

(iii) $D(\mathfrak{P}; L \mid \mathbf{Q}) \in \{\langle s \rangle, \langle r^2 s \rangle\}$ *si et seulement si* $p = 7 \pmod 8$.

(iv) $D(\mathfrak{P}; L \mid \mathbf{Q}) \in \{\langle rs \rangle, \langle r^3 s \rangle\}$ *si et seulement si* $p = 3 \pmod 8$.

Démonstration Pour le cas (i), on utilise le lemme de réduction avec le sous-groupe $\langle r^2 \rangle$ distingué dans D_4. Son corps des invariants est $\mathbf{Q}(\zeta_8)$. On a :

$$D(\mathfrak{P}; L \mid \mathbf{Q}) \subset \langle r^2 \rangle \iff D(\mathfrak{P} \cap \mathbf{Q}(\zeta_8); \mathbf{Q}(\zeta_8) \mid \mathbf{Q}) = \{e\} \iff p = 1 \pmod 8$$

Pour le cas (ii), on utilise le lemme de réduction avec le sous-groupe $\langle r \rangle$ distingué dans D_4. Son corps des invariants est $\mathbf{Q}(i)$. On a :

$$D(\mathfrak{P}; L \mid \mathbf{Q}) \subset \langle r \rangle \iff D(\mathfrak{P} \cap \mathbf{Q}(i); \mathbf{Q}(i) \mid \mathbf{Q}) = \{e\} \iff p = 1, 5 \pmod 8$$

Et le cas $p = 1 \pmod 8$ a déjà été discuté, on conclu le cas (ii).

Pour le cas (iii), on utilise le lemme de réduction avec le sous-groupe $\langle r^2, s \rangle$ distingué dans D_4. Son corps des invariants est $\mathbf{Q}(\sqrt{2})$. On a :

$$D(\mathfrak{P}; L \mid \mathbf{Q}) \subset \langle r^2, s \rangle \iff D(\mathfrak{P} \cap \mathbf{Q}(\sqrt{2}); \mathbf{Q}(\sqrt{2}) \mid \mathbf{Q}) = \{e\} \iff p = 1, 7 \pmod 8$$

De plus, le groupe $\langle r^2, s \rangle$ contient trois sous-groupe d'ordre 2, pour obtenir le résultat on utilise le cas (i).

Pour le cas (iv), on utilise le lemme de réduction avec le sous-groupe $\langle r^2, rs \rangle$ distingué dans D_4. Son corps des invariants est $\mathbf{Q}(i\sqrt{2})$. On a :

$$D(\mathfrak{P}; L \mid \mathbf{Q}) \subset \langle r^2, rs \rangle \iff D(\mathfrak{P} \cap \mathbf{Q}(i\sqrt{2}); \mathbf{Q}(i\sqrt{2}) \mid \mathbf{Q}) = \{e\} \iff p = 1, 3 \pmod 8$$

De plus, le groupe $\langle r^2, rs \rangle$ contient trois sous-groupe d'ordre 2, pour obtenir le résultat on utilise le cas (i).

■

A ce niveau là, nous allons obtenir la décomposition d'un premier p dans E en utilisant l'action de D_4 sur les plongements de $\mathbf{Q}(x)$ dans L. Elle est donnée de la manière suivante :

$$\Pi : r \mapsto (x, ix, -x, -ix) \qquad s \mapsto (x)(ix \ -ix)(-x)$$

On en déduit les décompositions dans E (ArtinLVsZetaE.pdf) :

(i) $(p) = (\bullet)(\bullet)(\bullet)(\bullet)$ ou $(p) = (\bullet)_2(\bullet)_2$ si et seulement si $p = 1 \pmod 8$.

(ii) $(p) = (\bullet)_4$ si et seulement si $p = 5 \pmod 8$.

(iii) $(p) = (\bullet)(\bullet)_2(\bullet)$ si et seulement si $p = 7 \pmod 8$.

(iv) $(p) = (\bullet)_2(\bullet)_2$ si et seulement si $p = 3 \pmod 8$.

En effet, pour le cas (iv), il nous suffit de calculer $\Pi(rs) = (x \ ix)(-x \ -ix)$.