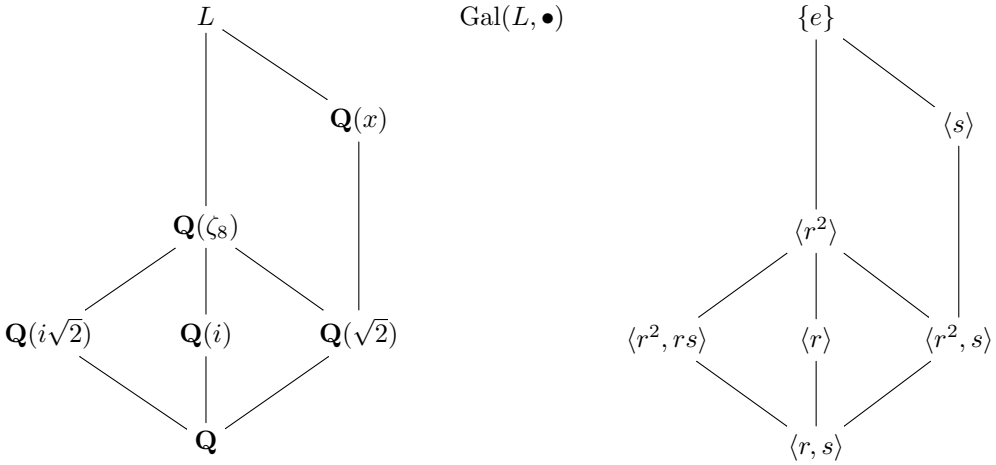
Soit $f = x^4 - 2$, on considère l'extension $E := \mathbf{Q}(x)$ du corps des nombres rationnels et sa clôture Galoisienne que l'on note L. Alors $L = \mathbf{Q}(\zeta_8, x)$ et $\mathrm{Gal}(L \mid \mathbf{Q})$ est isomorphe au groupe diédrale D_4 que l'on présente par $\langle r, s \mid r^4 = s^2 = 1\ srs = r^{-1}\rangle$. Un isomorphisme est donnée de la manière suivante :

$$r(\zeta_8) = \zeta_8^5 \qquad r(x) = ix \qquad s(\zeta_8) = \zeta_8^7 \qquad s(x) = x$$

Pour les calculs, on peut considérer le groupe diédrale comme le groupe d'isométrie du carré $\mathcal{C} := \{a, ia, -a, -ia\} \subset \mathbf{C}$ se groupe est engendré par la rotation r (multiplication par i) et s la conjugaison complexe. On obtient alors les diagrammes de correspondance de Galois (pas complet) :



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) :

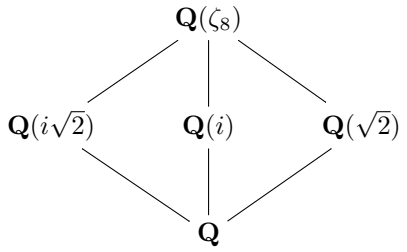
$$D(\mathfrak{P}; L \mid K) = D(\mathfrak{P}; L \mid \mathbf{Q}) \cap H$$

Démonstration Soit $\overline{\tau} \in D(\mathfrak{p}; K \mid \mathbf{Q})$, on commence par prolonger $\overline{\tau}$ en $\tau \in \mathrm{Gal}(L \mid \mathbf{Q})$, ensuite on applique le lemme de transitivité des idéaux premiers sur l'extension $L \mid K$. Il existe $\gamma \in \mathrm{Gal}(L \mid K)$ vérifiant $\gamma(\mathfrak{P}) = \tau(\mathfrak{P})$. Posons $\sigma := \gamma^{-1}\tau$. Alors $\sigma(\mathfrak{P}) = \mathfrak{P}$ et $forall x \in K$, $\sigma(x) = \tau(x)$. L'autre sens. si $\sigma \in D(\mathfrak{P}; L \mid \mathbf{Q})$, alors sa restriction fixe $\mathfrak{p}$.

La deuxième chose est a faire mais pas de soucis

■

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 :

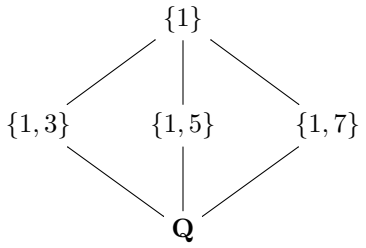
(i) Si $p = 1 \pmod 8$, alors $D(\mathfrak{P}; \mathbf{Q}(\zeta_8) \mid \mathbf{Q}) = \{1\}$.

(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 $\mathbf{Q}(\sqrt{2})$ Je me limite à l'étude de cette extension les autres étant similaire. D'une part, $\mathbf{Q}(\sqrt{2}) = \mathbf{Q}(\zeta_8)^{\{1,7\}}$ et son anneau d'entier est $\mathbf{Z}[\sqrt{2}]$ (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 $\mathfrak{p} := \mathfrak{P} \cap \mathbf{Z}[\sqrt{2}]$. Alors le lemme de réduction nous donne :

$$D(\mathfrak{p}; \mathbf{Q}(\sqrt{2}) \mid \mathbf{Q}) = D(\mathfrak{P}; \mathbf{Q}(\zeta_8) \mid \mathbf{Q}) \pmod{\{1, 7\}}$$

et en combinant les deux résultats :

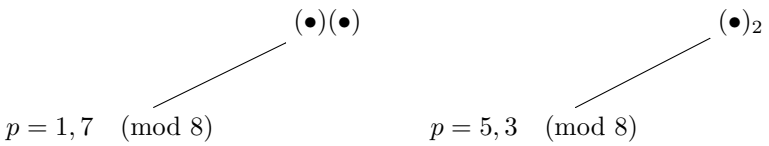
$$D(\mathfrak{p}; \mathbf{Q}(\sqrt{2}) \mid \mathbf{Q}) = \langle p \rangle \pmod{\{1, 7\}}$$

On en déduit :

(i) $p = 1, 7 \pmod 8$ si et seulement si $\#D(\mathfrak{p}; \mathbf{Q}(\sqrt{2}) \mid \mathbf{Q}) = 1$.

(ii) Si $p = 5, 3 \pmod 8$ si et seulement si $\#D(\mathfrak{p}; \mathbf{Q}(\sqrt{2}) \mid \mathbf{Q}) = 2$.

Ce qui veut dire en terme de diagramme :



En indice c'est le degré du corps de définition du point.

Combinatoire, fonction ζ et L Le p-facteur de L est obtenu de la manière suivante : je remplace dans la ligne du haut $(\bullet)_\star$ par $\frac{1}{1-T^\star}$:

$\frac{1}{1-T}\frac{1}{1-T}$ — $p = 1, 7 \pmod 8$ $\qquad$ $\frac{1}{1-T^2}$ — $p = 5, 3 \pmod 8$

Pour obtenir la fonction ζ de Dedekind, on fait le produit de la ligne du haut en remplaçant T par p^{-s} explicitement :

$$\begin{aligned}&\prod_{p=1,7 \pmod 8} \frac{1}{(1-p^{-s})(1-p^{-s})} \times \prod_{p=3,5 \pmod 8} \frac{1}{(1-p^{-s})(1+p^{-s})} \\ =&\prod_p \frac{1}{(1-p^{-s})} \times \prod_{p=1,7 \pmod 8} \frac{1}{(1-p^{-s})} \times \prod_{p=3,5 \pmod 8} \frac{1}{(1+p^{-s})}\end{aligned}$$

Introduisons la fonction

$$\chi_{\mathbf{Q}(\sqrt{2})}(p) = \begin{cases} 1, \text{ si } & p = 1, 7 \pmod 8 \\ -1, \text{ si } & p = 3, 5 \pmod 8 \end{cases}$$

Il s'agit d'un caractère et on fini le calcul :

$$\prod_p \frac{1}{(1-p^{-s})} \times \prod_{p=1,7 \pmod 8} \frac{1}{(1-p^{-s})} \times \prod_{p=3,5 \pmod 8} \frac{1}{(1+p^{-s})} = \zeta(s) \times \prod_p \frac{1}{(1-\chi_{\mathbf{Q}(\sqrt{2})}(p)p^{-s})} = \zeta_{\mathbf{Q}(\sqrt{2})}(s)$$

Comme on le voit on récupère la fonction ζ. Les fonctions L sont une généralisation des fonctions ζ. Il nous faut considérer la représentation

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. Et refaire avec l'inertie (toujours).

Retour sur l'exemple complet

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

Théorème 0.3 *On a :*

(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* $p = 3 \pmod 8$.

Complément On admet que (il s'agit d'un résultat fort):

(ia) $D(\mathfrak{P}; L \mid \mathbf{Q}) = \{e\}$ si et seulement si p est représenté par la forme binaire $x^2 + 64y^2$

(ib) $D(\mathfrak{P}; L \mid \mathbf{Q}) = \{e, r^2\}$ si et seulement si p est représenté par la forme binaire $4x^2 + 4xy + 17y^2$.

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).

■

Etude de E 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 : $\mathrm{Gal}(L \mid \mathbf{Q})$ sur $\mathrm{Hom}_{\mathbf{Q}}(E, L)$. Et on identifie :

$$\mathrm{Hom}_{\mathbf{Q}}(E, L) \equiv \{x, ix, -x, -ix\}$$

Théorème 0.4 *L'action de $Gal(L, K)$ sur $Hom_{\mathbf{Q}}(E, L)$ s'identifie avec le morphisme :*

$$\pi(r) = (x, ix, -x, -ix) \qquad \pi(s) = (x)(ix, -ix)(-x)$$

et la représentation par permutation est donnée par :

$$\rho(r) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \rho(s) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

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 $p = 1 \pmod 8$.

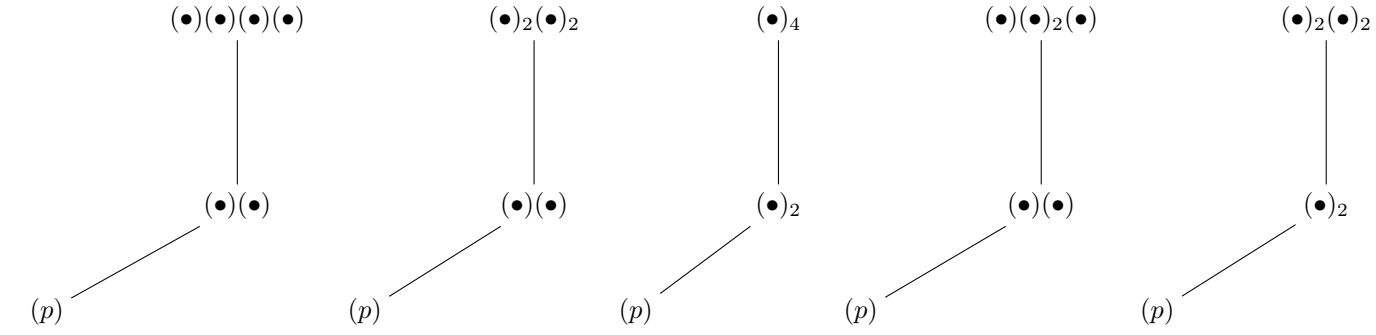
(ii) $(p) = (\bullet)_4$ si et seulement si $p = 5 \pmod 8$.

(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 $\Pi(rs) = (x\ ix)(-x\ -ix)$.

Les diagrammes de factorisation Je donne les diagrammes de factorisation d'un idéal p dans l'extension E et dans sa sous-extension $\mathbf{Q}(\sqrt{2})$.



cas (ia) cas (ib) cas (ii) cas (iii) cas (iv)

Retour sur la fonction L Ici nous nous proposons d'expliquer le calcul des fonctions L à partir de combinatoire sur les diagrammes.

Par la théorie des caractères la représentation se décompose en somme de trois représentations $\chi_1 \oplus \chi_3 \oplus \chi_5$. De plus, $L_{\chi_1} \times L_{\chi_3} = \zeta_{\mathbf{Q}(\sqrt{2})}$.

Pour tout nombre premier ce que l'on fait de manière combinatoire c'est que l'on compte le nombre d'idéaux premier avec groupe de décomposition trivial (i.e les points définies sur le corps premier) en haut et on enlève le nombre d'idéaux premier avec groupe de décomposition trivial sur l'étage du milieu. Ce qui donne :

$$2 \qquad -2 \qquad 0 \qquad 0 \qquad 0$$

(Exactement le ligne de caractère de la représentation de degré 2). Mais la on constate que si on multiplie par 2 cette ligne alors on trouve exactement le coefficient en p de Θ.

$$q_0(x,y) = x^2 + 64y^2 \qquad q_{\text{Gens}} = 4x^2 + 4xy + 17y^2$$

Alors

$$2L_3(s) = \Theta_0 - \Theta_{\text{Gens}^2}$$

Analyse des p-facteurs de $L_\rho(s)$. Pour chaque premier p, pour construire le p-facteur de L nous faisons le produit de la ligne du haut par la ligne intermédiaire en remplaçant $(\bullet)_f$ par $\frac{1}{1-T^f}$. On constate que pour les cas (ii) à (iv) le p-facteur est $\frac{1}{1-T^2}$ et que :

$$\frac{1}{(1-T)^2} \qquad \frac{1}{(1+T)^2}$$

D'autre part, dans le développement de L le coefficient a_p est exactement.

Par définition :

$$L(s) := \prod_{p_{ia}} \frac{1}{(1-T)^2} \prod_{p_{ib}} \frac{1}{(1+T)^2} \prod_{p} \frac{1}{(1-T^2)}$$

On en déduit que :

(ia) $a_{p^r} = 2$.

(ib) $a_{p^r} = -2$.

(p) $a_{p^r} = 1^r + (-1)^r$.

Et on constate que tous ses coefficients sont $\frac{1}{2}$ fois les coefficients de la série $\Theta_0 - \Theta_{\text{Gens}^2}$.

Introduisons la fonction $T(q) = \sum_{x,y \in \mathbf{Z}^2} q^{q_o(x,y)} - q^{q_{\text{Gens}}(x,y)}$.

0.1 Représentation

Etude du groupe D_4 On dispose des 4 représentation de degré 1 suivante :

$$\Phi_{\pm\pm} = \begin{bmatrix} r \mapsto \pm 1 \\ s \mapsto \pm 1 \end{bmatrix}$$

et d'un représentation de degré 2 :

$$r \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad \rho = s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

On obtient le tableau de caractère suivant :

	e	r^2	$\{r, r^3\}$	$\{s, r^2 s\}$	$\{rs, r^3 s\}$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Tentative pour comprendre la classe ambigüe On considère le diagramme suivant :

$$\begin{array}{ccc} \dfrac{\text{Bin}(-256)}{\text{SL}_2(\mathbf{Z})} & & \\ \uparrow & \searrow & \\ \dfrac{\text{Idéaux}(\mathbf{Z}[8i])}{P(\mathbf{Z}[8i])} & \longrightarrow & \text{Gal}(\mathcal{G}_8 \mid \mathbf{Q}(i)) \end{array}$$

Mon histoire de montagne et de caillou ... qui descent d'une montagne Prenons la lemniscate dont le graphe est

on dispose de i qui agit sur la lemniscate ∞, on trouve ... le conducteur est 8 ...

$$i \times \infty = 8$$