Université Bordeaux I
351 Cours de la Libération
33400 Talence

Mémoire

# « Qu'est que la loi de réciprocité d'Artin sur $\mathbb{Q}$ ? »

**Le 21 octobre 2009**

*Mademoiselle Sophie Marques*
*Tuteur : Monsieur Herr*

# Table des matières


**1 La loi de réciprocité quadratique sur $\mathbb{Z}$ 5**

1.1 Formulation usuelle de la loi de réciprocité quadratique à l'aide du symbole de Legendre . . . . . 5

1.2 Lien entre la loi de réciprocité et le morphisme de Kronecker . . . . . 9

**2 La loi de réciprocité d'Artin sur $\mathbb{Q}$ : 25**

2.1 Arithmétique des extensions quadratiques de $\mathbb{Q}$ . . . . . 25

2.1.1 Définition des corps quadratiques . . . . . 25

2.1.2 L'anneau des entiers d'un corps quadratique . . . . . 26

2.1.3 Discriminant et ramification . . . . . 26

2.1.4 Décomposition d'un premier dans un corps quadratique . . . . . 27

2.2 L'application d'Artin d'un corps quadratique sur $\mathbb{Q}$ . . . . . 28

2.2.1 Groupe de décomposition dans le cas d'un corps quadratique . . . . 28

2.2.2 Groupe de Galois du corps résiduel et morphisme de Frobénius . . 29

2.2.3 Construction de l'application d'Artin . . . . . 29

2.2.4 Lien avec le symbole de Legendre . . . . . 31

2.2.5 Réciprocité d'Artin . . . . . 32

2.3 Enoncé de la réciprocité d'Artin sur $\mathbb{Q}$ . . . . . 34

2.3.1 Rappels sur la décomposition des idéaux premier dans une extension galoisienne de corps de nombres . . . . . 34

2.3.2 Automorphisme de Frobénius . . . . . 34

2.3.3 Loi de réciprocité d'Artin sur $\mathbb{Q}$ . . . . . 36

**3 Conséquences sur la décompostion des nombres premiers dans une extension abélienne de $\mathbb{Q}$ 38**

3.1 Premiers totalements décomposés . . . . . 38

3.2 Polynômes totalement décomposés modulo un nombre premier . . . . . 40

3.3 Densité de $S(K)$ . . . . . 42

3.4 Lien avec le théorème de Kronecker-Weber . . . . . 43

**4 La réciprocités de Artin pour les extensions admissibles de $\mathbb{Q}$ 46**

4.1 Rappels sur les corps cyclotomiques . . . . . 46

4.2 Extensions admissibles de $\mathbb{Q}$ . . . . . 46

4.3 Théorie du corps des classes pour les extensions admissibles de $\mathbb{Q}$ . . . . . 50

**5 Un exemple : étude des sous corps de $K_7 = \mathbb{Q}(e^{\frac{2i\Pi}{7}})$ 53**

# Remerciements

Je tenais à remercier mon tuteur Monsieur Herr qui m'a permise de réaliser ce mémoire.
Il m'as aidé tout au long, conseiller, corriger, m'as fait découvrir la loi de réciprocité quadratique et étendre mes connaissances sur la théorie des nombres.
Je le remercie en particulier pour sa disponibilité et sa patience.
Ce mémoire m'a été très bénéfique, autant par les connaissances mathématiques que par le travail de recherche et de redaction.
C'est pour tout cela que j'adresse ici mes remerciements.

# Introduction

Le terme de "loi de réciprocité" est due à Legendre. Alors qu'il travaillait autour du petit théorème de Fermat et de ce qu'on l'on pourrait appeler la théorie des congruences, il énonce en 1785 la loi de réciprocité quadratique visant à rechercher les carrés modulo un premier.
Comprendre ce qu'est, au sens le plus général, une loi de réciprocité, est l'une des question qui a guidé et motivé tout le développement de la théorie algébrique des nombres, depuis les Disquisitiones Arithmeticae jusqu'aux recherches très actuelles qui s'inscrivent dans le programme des Langlands.
Nous nous proposons ici d'esquisser quelques éléments de réponse à la question suivante : "Qu'est que la loi de réciprocité d'Artin sur $\mathbb{Q}$ ?"
C'est ainsi, que nous commencerons par énoncer la réciprocité quadratique dans $\mathbb{Z}$ et les formules complémentaires en montrant de qu'elle manière elle vient répondre au problème des carrés modulo un premier.
En vue de l'étendre à des cas plus généraux, on montrera ensuite que cette loi est équivalente à la donnée d'un morphisme surjectif que l'on appellera le morphisme de Kronecker défini sur $\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times}$ à valeur $\{\pm 1\}$.
Nous introduisons alors pour les extensions quadratiques de $\mathbb{Q}$ l'application d'Artin construite à partir du morphisme de Frobénius en $p$ et définie sur un groupe de fractions particulier vers le groupe de Galois de l'extension. Nous verrons alors une nouvelle interprétation dans ce cas de la loi de réciprocité qui peut même s'étendre aux extensions abéliennes sous la forme du théorème de Artin que nous énoncerons sans le démontrer en toute généralité.
Cette traduction de la loi de réciprocité dans le cas abélien est très riche car elle aura des conséquences sur la décomposition des idéaux et sera même équivalente au théorème de Kronecker-Weber, ce qui constituera encore un aspect de la loi de réciprocité très intéressant.
Nous prouverons enfin la loi de réciporcité d'Artin pour les sous corps des extensions cyclotomiques de $\mathbb{Q}$.

# 1 La loi de réciprocité quadratique sur $\mathbb{Z}$

## 1.1 Formulation usuelle de la loi de réciprocité quadratique à l'aide du symbole de Legendre

Nous allons commencer par énoncer la loi de réciprocité quadratique sur $\mathbb{Z}$ suivie d'une de ses preuves.
On se donne un nombre premier $p$ et un entier $d$ premier à $p$.
Nous introduisons la locution **"d est un résidu quadratique mod p"** (resp. **"d un non-résidu mod p"**) comme signifiant que la classe de $d$ mod $p$ est un carré (resp. un non carré) dans $\mathbb{F}_p^*$.

**Nous allons introduire maintenant *le symbole de Legendre* $\left(\frac{d}{p}\right)$ défini comme suit :**

$$\begin{cases} \left(\frac{d}{p}\right) = +1 & \textbf{si } d \textbf{ est résidu quadratique mod } p \ . \\ \left(\frac{d}{p}\right) = -1 & \textbf{si } d \textbf{ est non-résidu mod } p \ . \end{cases} \tag{1}$$

Bien entendu $\left(\frac{d}{p}\right)$ n'est défini que pour $d$ premier avec $p$, c'est à dire que pour $d \in \mathbb{Z} - p\mathbb{Z}$.
Le groupe multiplicatif $\mathbb{F}_p^*$ étant cyclique d'ordre pair $p-1$, les carrés en forment un sous groupe $\mathbb{F}_p^{*2}$ d'indice 2, et $\frac{\mathbb{F}_p^*}{\mathbb{F}_p^{*2}}$ est isomorphe à $\{\pm 1\}$.
Ainsi le symbole de Legendre s'obtient en composant les homomorphisme :

$$\mathbb{Z} - p\mathbb{Z} \longrightarrow \mathbb{F}_p^* \longrightarrow \frac{\mathbb{F}_p^*}{\mathbb{F}_p^{2*}} \rightsquigarrow \{\pm 1\}$$

On en déduit donc la formule de multiplicativité suivante :

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{2}$$

**Proposition 1 (*"critère d'Euler"*)**

*Si $p$ est un nombre premier impair, et si $a \in \mathbb{Z} - p\mathbb{Z}$, on a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ mod\ p$*

**Démonstration :** :
Notons $\omega$ une racine primitive de l'unité mod $p$ ; on a $a \equiv \omega^j\ mod\ p$ avec $0 \leq j \leq p-2$ car la classe $\bar{\omega}$ de $\omega$ est un générateur de $\mathbb{F}_p^*$. Il est clair que "a résidu quadratique"' équivaut à "j pair" ; on a donc $\left(\frac{a}{p}\right) = (-1)^j$. D'autre part, $\mathbb{F}_p^*$ a un seul élément d'ordre 2, à savoir $\bar{\omega}^{\frac{p-1}{2}}$, et celui ci est égal à $-1$ car son carré est 1 ; donc dans $\mathbb{Z}$, on a $-1 \equiv \omega^{\frac{p-1}{2}}\ mod\ p$.
Ainsi :

$$\left(\frac{a}{p}\right) = (-1)^j \equiv \omega^{j\times\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}}\ modp$$

■

Nous arrivons alors au coeur du sujet, au célèbre résultat : la loi de réciprocité quadratique, qui montre que les propriétés de congruences modulo deux nombres premiers impairs distincts ne sont pas indépendantes.

**Théorème 1 (*"Loi de réciprocité quadratique d'Euler Legendre-Gauss"*)**

*Si $p$ et $q$ sont deux premiers impairs distincts, on a :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

**Démonstration :** :
Considérons, dans une extension convenable de $\mathbb{F}_q$,une racine primitive $p^{ième}$ de l'unité $\omega$. Comme $\omega^p = 1$, la notation $\omega^x$ a un sens pour $x \in \mathbb{F}_p$. Nous écrivons aussi le symbole de Legendre $\left(\frac{x}{p}\right)$ pour $x \in \mathbb{F}_p^*$, car $\left(\frac{d}{p}\right)$ ne dépend évidemment que de la classe de $d$ mod $p$. Pour $a \in \mathbb{F}_p^*$, considérons la "somme de Gauss" :

$$\tau(a) = \sum_{x\in\mathbb{F}_p^*} \left(\frac{x}{p}\right)\omega^{ax} \tag{3}$$

C'est un élément d'une extension de $\mathbb{F}_q$. Posant $ax = y$, on a :

$$\begin{aligned} \tau(a) &= \textstyle\sum_{y\in\mathbb{F}_p^*} \left(\frac{ya^{-1}}{p}\right)\omega^y \\ &= \left(\frac{a^{-1}}{p}\right)\textstyle\sum_{y\in\mathbb{F}_p^*} \left(\frac{y}{p}\right)\omega^y \end{aligned}$$

(par (2)), d'où

$$\tau(a) = \left(\frac{a}{p}\right)\tau(1). \tag{4}$$

D'autre part, comme on calcule en caractéristique $q$ et que $\left(\frac{x}{p}\right) \in \mathbb{F}_q$, on a $\tau(1)^q = \sum_{x\in\mathbb{F}_p^*} \left(\frac{x}{p}\right)^q \omega^{qx}$, d'où, en identifiant $q$ à sa classe mod $p$,

$$\tau(1)^q = \tau(q). \tag{5}$$

Calculons maintenant $\tau(1)^2$.
On a

$$\tau(1)^2 = \sum_{x,y\in\mathbb{F}_p^*} (\frac{x}{p})(\frac{y}{p})\omega^{x+y}.$$

Posant $y = tx$, il vient

$$\begin{aligned}
\tau(1)^2 &= \sum_{x,y\in\mathbb{F}_p^*} \left(\frac{x}{p}\right)^2 \left(\frac{t}{p}\right)\omega^{x(1+t)} \\
&= \sum_{x,t\in\mathbb{F}_p^*} \left(\frac{t}{p}\right)\omega^{x(1+t)} \\
&= \sum_{t\in\mathbb{F}_p^*} \left[\left(\frac{t}{p}\right)\sum_{x\in\mathbb{F}_p^*} \omega^{x(1+t)}\right].
\end{aligned}$$

Si $\omega^{1+t} \neq 1$, on a $\sum_{j=0}^{p-1}(\omega^{1+t})^j = 0$ par la formule de la progression géométrique, car $(\omega^{1+t})^p = 1$ ;
d'où $\sum_{x\in\mathbb{F}_p^*} \omega^{x(1+t)} = -1$.
Si $\omega^{1+t} = 1$, on a $\sum_{x\in\mathbb{F}_p^*} \omega^{x(1+t)} = p - 1$ ;
ce dernier cas n'a lieu que pour $t = -1$, car $\omega$ est une racine primitive $p - ème$ de l'unité.
On a donc

$$\tau(1)^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t\in\mathbb{F}_p^*, t\neq -1} \left(\frac{t}{p}\right).$$

Comme il y a autant de carré que de non carré dans $\mathbb{F}_p^*$, on a

$$\sum_{t\in\mathbb{F}_p^*} \left(\frac{t}{p}\right) = 0,$$

d'où

$$\tau(1)^2 = (\frac{-1}{p})(p-1) + (\frac{-1}{p}) = (\frac{-1}{p})p.$$

Par le critère d'Euler, on a donc

$$\tau(1)^2 = (-1)^{\frac{p-1}{2}} p. \tag{6}$$

Enfin, par (4) et (5), on a $\tau(1)^q = \tau(q) = \left(\frac{q}{p}\right)\tau(1)$.
Comme $\tau(1)$ est non nul par (6), on simplifie : $\tau(1)^{q-1} = \left(\frac{q}{p}\right)$.
Par (6) encore, on a :

$$\left(\frac{q}{p}\right) = (\tau(1)^2)^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}}.$$

Comme $p^{\frac{q-1}{2}} = \left(\frac{q}{p}\right)$ (proposition) et que $\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)^{-1}$, la loi de réciprocité est démontrée. ■

**Proposition 2 (*"formules complémentaires"*)**

*Si $p$ est un nombre premier impair on a :*
*a)* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
*b)* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

**Démonstration :** :
a) est un cas particulier du critère d'Euler.
Démontrons donc b). Notons d'abord que, comme les carrés de 1, 3, 5, 7, *mod.* 8 sont 1, 1, 1, 1, on a $p^2 \equiv 1$ *mod* 8, et la formule écrite a donc un sens.
Remarquons ensuite que, dans le groupe $H = 1,\ 3,\ 5,\ 7$ des éléments inversibles de $\frac{\mathbb{Z}}{8\mathbb{Z}}$, $1,\ 7$ est un sous-groupe $H'$ d'indice 2 ; posons $\theta(x) = 1$ pour $x \in H'$ et $\theta(x) = -1$ pour $x \in H - H'$, de sorte qu'on a $\theta(xy) = \theta(x)\theta(y)$ pour $x, y \in H$. Soit alors $\omega$ une racine primitive $8 - ième$ de l'unité dans une extension de $\mathbb{F}_p$. Comme dans le théorème, considérons, pour $a \in H$, la "somme de Gauss" :

$$\tau(a) = \sum_{x \in H} \theta(x)\omega^{ax}. \tag{7}$$

Comme dans le théorème, on a $\tau(a) = \theta(a)\tau(1)$ et $\tau(1)^p = \tau(p)$ (en identifiant $p$ à sa classe mod 8). D'après la définition de $\theta(x)$, on a :

$$\begin{aligned} \tau(1) &= \omega - \omega^3 - \omega^5 + \omega^7 = (1-\omega^2)(\omega - \omega^5) \\ &= \omega(1-\omega^2)(1-\omega^4) = 2\omega(1-\omega^2) \end{aligned}$$

(car $\omega^8 = 1$ et $\omega^4 = -1$) ; d'où

$$\tau(1)^2 = 4\omega^2(1 - 2\omega^2 + \omega^4) = -8\omega^4 = 8.$$

Comme dans le théorème, on en déduit $\tau(1)^p = \tau(p) = \theta(p)\tau(1)$ ; d'où, en simplifiant $\theta(p) = (\tau(1)^2)^{\frac{p-1}{2}} = 8^{\frac{p-1}{2}} = \left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right)$.
On a donc $\left(\frac{2}{p}\right) = \theta(p)$. Or on constate par calcul direct, qu'on a $\theta(x) = (-1)^{\frac{x^2-1}{8}}$ pour $x = 1,\ 3,\ 5,\ 7$ (ou, plus efficacement, pour $x = 1,\ 3,\ -3,\ -1$), et que $\frac{x^2-1}{8}$ ne dépend que de la classe de $x$ mod 8. ■

**Exemple 1**

*La loi de réciprocité et les formules complémentaires permettent de calculer le symbole de Legendre par réductions successives.*
*Calculons ainsi* $\left(\frac{23}{59}\right)$, *sans avoir à écrire la longue table des carrés modulo* 59. *On a :*

$$\begin{aligned} \left(\frac{23}{59}\right) &= (-1)^{11\times 29}\left(\frac{13}{23}\right) = -(-1)^{6\times 11}\left(\frac{23}{13}\right) = -\left(\frac{10}{13}\right) \\ &= -\left(\frac{-3}{13}\right) = -\left(\frac{-1}{13}\right)\left(\frac{3}{13}\right) = -(-1)^6\left(\frac{3}{13}\right) \\ &= -(-1)^{6\times 1}\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1. \end{aligned}$$

*Donc* 23 *n'est pas un carré modulo* 59.

Notre but ici est de bien comprendre la loi de réciprocité quadratique, de trouver des énoncés équivalents afin d'étudier les extensions possibles de cette loi. Dans son premier énoncé, la loi de réciprocité quadratique apparait comme le moyen de caractériser les carrés modulo un $p$ premier :
Pour $a \in \mathbb{Z}$, p un nombre premier impair tel que $p \not| a$, a est un carré modulo p est équivalent $\left(\frac{a}{p}\right) = 1$.
Nous allons voir une traduction en terme de morphisme de groupe qui nous conduira à l'étude du morphisme d'Artin et nous donnera des extensions intéressantes de la loi de réciprocité quadratique.

## 1.2 Lien entre la loi de réciprocité et le morphisme de Kronecker

On va commencer cette partie en introduisant **le symbole de Jacobi**.
Il est contruit à partir du symbole de Legendre :
Pour $M$, $m$ premiers entre eux $m \geq 3$ **impairs** admettant comme factorisation en produit de nombres premiers $m = p_1...p_r$, on pose :

$$\left(\frac{M}{m}\right) = \left(\frac{M}{p_1}\right)...\left(\frac{M}{p_r}\right)$$

Notons déjà que :

$$\left(\frac{M}{m}\right) = \left(\frac{N}{m}\right) \; quand \; M \equiv N \; mod \; m$$

On a alors la propriété suivante

**Propriété 1**

*Pour $M, N, m, n \in \mathbb{Z}$, avec $m, n \geq 3$ impairs, on a :*

$$\left(\frac{MN}{m}\right) = \left(\frac{M}{m}\right)\left(\frac{N}{m}\right) \tag{8}$$

$$\left(\frac{M}{nm}\right) = \left(\frac{M}{m}\right)\left(\frac{M}{n}\right)$$

**Démonstration :** :

La preuve de ces égalités réside en les propriétés du symbole de Legendre et la définition du symbole de Jacobi.
On écrit les décomposition $m = m_1...m_s$ et $n = n_1...n_r$ en produit de nombres premiers.
On a alors :

$$\left(\frac{MN}{m}\right) = \prod_{i=1}^{s}\left(\frac{MN}{m_i}\right) = \prod_{i=1}^{s}\left(\frac{M}{m_i}\right)\left(\frac{N}{m_i}\right) = \left(\frac{M}{m}\right)\left(\frac{N}{n}\right)$$

et

$$\left(\frac{M}{mn}\right)=\prod_{i=1}^{s}\prod_{j=1}^{r}\left(\frac{M}{m_i}\right)\left(\frac{M}{n_j}\right)=\prod_{i=1}^{s}\left(\frac{M}{m_i}\right)\prod_{j=1}^{r}\left(\frac{M}{n_j}\right)=\left(\frac{M}{m}\right)\left(\frac{M}{n}\right)$$ ■

## Propriété 2

*Le symbole de Jacobi satisfait aussi la version suivante de la loi de réciprocité quadratique, pour $m,\ M\geq 3$ impairs, on a :*

$$\begin{aligned} &1)\quad \left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}\\ &2)\quad \left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}\\ &3)\quad \left(\frac{M}{m}\right)=(-1)^{\frac{(M-1)(m-1)}{4}}\left(\frac{m}{M}\right)\end{aligned} \tag{9}$$

**Démonstration :** :

Ecrivons les décompositions $m=m_1..m_l$ et $M=M_1...M_r$ en produit de nombres premiers.
**1)**

$$\left(\frac{-1}{m}\right)=\prod_{i=1}^{l}(-1)^{\frac{m_i-1}{2}}=(-1)^{\sum_{i=1}^{l}\left(\frac{m_i-1}{2}\right)}=(-1)^{\frac{\prod_{i=1}^{l}m_i-1}{2}}=(-1)^{\frac{n+1}{2}}$$

car, par récurrence on montre que :

$$\sum_{i=1}^{l}\left(\frac{m_i-1}{2}\right)\equiv\frac{\prod_{i=1}^{l}m_i-1}{2}\ mod\ 2$$

Pour $l=1$, la propriété est clairement vérifiée.
Supposons que la propriété est vraie pour un $l\geq 1$ quelquonque ie

$$\sum_{i=1}^{l}\left(\frac{m_i-1}{2}\right)\equiv\frac{\prod_{i=1}^{l}m_i-1}{2}\ mod\ 2$$

Montrons que :

$$\sum_{i=1}^{l+1}\left(\frac{m_i-1}{2}\right)\equiv\frac{\prod_{i=1}^{l+1}m_i-1}{2}\ mod\ 2$$

Or, par hypothèse de récurrence :

$$\sum_{i=1}^{l+1}\left(\frac{m_i-1}{2}\right)\equiv\frac{\prod_{i=1}^{l}m_i-1}{2}+\frac{m_{l+1}-1}{2}\ mod\ 2$$

Posons $q=\prod_{i=1}^{l}m_i$ ; alors :

$$\begin{aligned}\frac{(qm_{l+1}-1)-(q-1)-(m_{l+1}-1)}{2} &= \frac{qm_{l+1}-q-m_l+1+2}{2}\\ &= \frac{(q-1)(m_{l+1}-1)}{2},\end{aligned}$$

Ce qui permet d'aboutir au résultat car $q$ est impair donc $q-1$ est pair et il en est de même pour $m_{l+1}-1$.

**2)**

Montrons que

$$(\frac{2}{m}) = (-1)^{\frac{m^2-1}{8}}$$

$$\left(\frac{2}{m}\right) = \prod_{i=1}^{l}(-1)^{\frac{m_i^2-1}{8}} = (-1)^{\sum_{i=1}^{l}\left(\frac{m_i^2-1}{8}\right)}$$

Montrons que

$$\sum_{i=1}^{l}(\frac{m_i^2-1}{8}) \equiv \frac{\prod_{i=1}^{l} m_i^2-1}{8} \ mod\ 2$$

Nous allons procéder par récurrence sur $l$. Pour $l=1$ c'est clair.
Supposons que :

$$\sum_{i=1}^{l}\frac{m_i^2-1}{8} \equiv \frac{\prod_{i=1}^{l} m_i^2-1}{8} \ mod\ 2$$

Montrons que :

$$\sum_{i=1}^{l+1}\frac{m_i^2-1}{8} \equiv \frac{\prod_{i=1}^{l+1} m_i^2-1}{8} \ mod\ 2$$

$$\sum_{i=1}^{l+1}\frac{m_i^2-1}{8} \equiv \sum_{i=1}^{l}\frac{m_i^2-1}{8} + \frac{m_{l+1}^2-1}{8} \equiv \frac{\prod_{i=1}^{l} m_i^2-1}{8} + \frac{m_{l+1}^2-1}{8} \ mod\ 2.$$

$$\begin{aligned}\frac{(\prod_{i=1}^{l+1} m_i^2-1)-(m_{l+1}^2-1)-(\prod_{i=1}^{l} m_i^2-1)}{8} &= \frac{\prod_{i=1}^{l} m_i^2-m_{l+1}^2-\prod_{i=1}^{l} m_l^2+2}{8} \\ &= \frac{(\prod_{i=1}^{l+1} m_i^2-1)(m_{s+1}^2-1)}{8} \equiv 0 \ mod\ 2\end{aligned}$$

En effet, on a $q := \prod_{i=1}^{l+1} m_i^2$ qui est un produit de nombres impairs donc impair et de la forme $2k+1$ où $k$ est un entier ;
comme

$$q^2 = (2k+1)^2 = 4k^2+4k+1 = 4(k+1)k+1 \equiv 1 mod 8$$

car $k$ ou $k+1$ est pair et $m_{l+1}^2-1$ est pair, on obtient la congruence voulue qui nous donne le résultat.

**3)**

$$\left(\frac{M}{m}\right) = \prod_{i=1}^{r}\prod_{j=r}^{l}\left(\frac{p_i}{q_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{l}(-1)^{\frac{(p_i-1)(q_j-1)}{4}} = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{(p_i-1)(q_j-1)}{4}}.$$

Montrons que :

$$(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{(p_i-1)(q_j-1)}{4}} = (-1)^{\frac{(M-1)(m-1)}{4}}.$$

ie :

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{(p_i-1)(q_j-1)}{4} \equiv \frac{(M-1)(m-1)}{4} \ mod\ 2$$

Or

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{(p_i-1)(q_j-1)}{4} = \left(\sum_{i=1}^{r}\frac{(p_i-1)}{2}\right)\left(\sum_{j=1}^{s}\frac{(q_j-1)}{2}\right)$$

De plus, par la preuve du 1), on a :

$$\left(\sum_{i=1}^{r}\frac{(p_i-1)}{2}\right) \equiv \frac{\prod_{i=1}^{r}p_i-1}{2} \ mod\ 2$$

et

$$\left(\sum_{i=1}^{r}\frac{(q_i-1)}{2}\right) \equiv \frac{\prod_{i=1}^{r}q_i-1}{2} \ mod\ 2$$

donc

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{(p_i-1)(q_j-1)}{4} \equiv \frac{\prod_{i=1}^{r}p_i-1}{2}\frac{\prod_{i=1}^{r}q_i-1}{2} \ mod\ 2.$$

C'est ce qu'il fallait démontrer.

■

Nous allons énoncer le théorème central de cette partie qui s'appuie sur les deux lemmes suivants.

**Lemme 1 (*Propriété remarquable du symbole de Jacobi*)**

*Si $m \equiv n\ mod\ D$ où $m,\ n$ sont* ***impairs*** *et $\geq 3$, et $D \equiv 0,\ 1 \mod 4$ alors :*

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right) \tag{10}$$

**Démonstration :** :

$1^{er}$ **cas :** $D > 0$
$1^{er}$ sous-cas : $D \equiv 1\ mod\ 4$

On a par la loi de réciprocité quadratique :

$$\begin{aligned}\left(\frac{D}{m}\right) &= (-1)^{\frac{(D-1)(m-1)}{4}}\left(\frac{m}{D}\right)\\ \left(\frac{D}{n}\right) &= (-1)^{\frac{(D-1)(n-1)}{4}}\left(\frac{n}{D}\right)\end{aligned}$$

Or, comme $m \equiv n\ mod\ D$, on a $\left(\frac{m}{D}\right) = \left(\frac{n}{D}\right)$.
On veut donc montrer que :

$$(-1)^{\frac{(D-1)(m-1)}{4}} = (-1)^{\frac{(D-1)(n-1)}{4}}$$

$$\iff \frac{(D-1)(m-1)}{4} \equiv \frac{(D-1)(n-1)}{4} \ mod\ 2$$

or comme $D \equiv 1\ mod\ 4 \implies D-1 \equiv 0\ mod\ 4$ et $m$ impair donc $m-1$ est pair (idem pour n). Ainsi,

$$\frac{(D-1)(m-1)}{4} \equiv \frac{(D-1)(n-1)}{4} \equiv 0\ mod\ 2.$$

C'est ce que l'on voulais montrer.

$2^{ème}$ **sous cas :** $D \equiv 0 mod\ 4$

Ecrivons alors $D$ sous la forme $D = 2^k d$ où $d > 0$ est impair et $k \geq 2$
On a :

$$\left(\frac{D}{m}\right) = \left(\frac{2}{m}\right)^k \left(\frac{d}{m}\right) = (-1)^{k\frac{m^2-1}{8}} (-1)^{\frac{m-1}{2}\frac{d-1}{2}} \left(\frac{m}{d}\right) \ (\textit{propriétés du symbole de Jacobi}).$$

De même, on obtient :

$$\left(\frac{D}{n}\right) = (-1)^{k\frac{n^2-1}{8}} (-1)^{\frac{n-1}{2}\frac{d-1}{2}} \left(\frac{n}{D}\right).$$

Comme

$$m \equiv n\ mod\ D \implies m \equiv n\ mod\ d \ \ car\ d\ divise\ n.$$

On a :

$$\left(\frac{m}{d}\right) = \left(\frac{n}{d}\right).$$

On veut donc montrer que :

$$(-1)^{k\left(\frac{m^2-1}{8}\right)+\frac{(m-1)(d-1)}{4}} = (-1)^{k\left(\frac{n^2-1}{8}\right)+\frac{(n-1)(d-1)}{4}}$$

ie :

$$k\left(\frac{m^2-1}{8}\right) + \frac{(m-1)(d-1)}{4} \equiv k\left(\frac{n^2-1}{8}\right) + \frac{(n-1)(d-1)}{4} mod\ 2$$

Commençons par montrer que :

$$\frac{(m-1)(d-1)}{4} \equiv \frac{(n-1)(d-1)}{4} \ mod\ 2$$

ie :

$$\frac{(m-1)(d-1)}{4} - \frac{(n-1)(d-1)}{4} = \frac{(m-n)(d-1)}{4} \equiv 0\ mod\ 2\ ]$$

Comme

$$m \equiv n\ mod\ D\ ie\ 4\ divise\ m-n\ car\ 4\ divise\ D$$

et $d-1$ est pair, on a la congruence voulue. Or $d$ est impair donc $d-1$ est pair.
ce qui montre l'équivalence souhaitée.

Reste à montrer que :

$$k\left(\frac{m^2-1}{8}\right) \equiv k\left(\frac{n^2-1}{8}\right) \ mod\ 2.$$

ie

$$k\left(\left(\frac{m^2-1}{8}\right) - \left(\frac{n^2-1}{8}\right)\right) = \frac{m^2-n^2}{8} = \frac{(m-n)(m+n)}{8} \equiv 0 \ mod\ 2$$

Si $k$ est pair c'est immédiat.
Supposons que $k$ est impair i.e. $k \geq 3$, puisque $k \geq 2$.
Or $m \equiv n \ mod\ D$ et 8 divise $D$ donc 8 divise $(m-n)$ et comme $m$ et $n$ sont impairs, on a $m+n$ pair.
Celà donne la congruence voulue.

**$2^{éme}$ cas : $D < 0$**

On va utiliser le résultat que l'on vient de montrer sur $-D > 0$.
**$1^{er}$ sous-cas :**

$$\begin{aligned}\left(\frac{D}{m}\right) &= \left(\frac{(-1)\times(-D)}{m}\right) \\ &= \left(\frac{-1}{m}\right) \times \left(\frac{-D}{m}\right) = (-1)^{\frac{m-1}{2}}\left(\frac{-D}{m}\right) \\ &= (-1)^{\frac{m-1}{2}}(-1)^{\frac{m-1}{2}\frac{-D-1}{2}}(-1)^{\frac{n-1}{2}}(-1)^{\frac{n-1}{2}\frac{-D-1}{2}}\left(\frac{D}{n}\right)\end{aligned}$$

Il s'agit de montrer que :

$$(-1)^{\frac{m-1}{2}}(-1)^{\frac{m-1}{2}\frac{-D-1}{2}}(-1)^{\frac{n-1}{2}}(-1)^{\frac{n-1}{2}\frac{-D-1}{2}} = 1$$

ie

$$\frac{m-1}{2} + \frac{m-1}{2}\frac{-D-1}{2} + \frac{n-1}{2} + \frac{n-1}{2}\frac{-D-1}{2} \equiv 0 \ mod\ 2$$

ou encore :

$$\left(\frac{m+n}{2} - 1\right) + \left(\frac{m+n}{2} - 1\right)\left(\frac{-D-1}{2}\right) \equiv 0 \ mod\ 2$$

qui se réécrit :

$$\left(\frac{m+n}{2} - 1\right)\left(\frac{-D+1}{2}\right) \equiv 0 \ mod\ 2$$

$$D \equiv 1 \ mod\ 4 \ ie \ -D \equiv 3 \ mod\ 4 \Leftrightarrow -D+1 \equiv 0 \ mod\ 4$$

Donc ici comme $m+n$ est pair car $m$ et $n$ sont impair.
On a l'équivalence.

**$2^{ème}$ sous cas :**

$$D \equiv 0 \ mod\ 4 \ ie \ -D \equiv 0 \ mod\ 4$$

$$\begin{aligned}\left(\frac{D}{m}\right) &= \left(\frac{-1}{m}\right)\times\left(\frac{-D}{m}\right)\\ &= (-1)^{\frac{m-1}{2}}\left(\frac{-D}{m}\right)\\ &= (-1)^{\frac{m-1}{2}}\left(\frac{-D}{n}\right)\ (car\ -D\ \equiv\ 0\ mod\ 4,\ cas\ positif)\\ &= (-1)^{\frac{m-1}{2}+\frac{n-1}{2}}\left(\frac{D}{n}\right)\\ &= (-1)^{\frac{m+n}{2}-1}\left(\frac{D}{n}\right)\end{aligned}$$

De plus

$$m \equiv n\ mod\ D$$

donc

$$\frac{m+n}{2} \equiv n\ mod\ D$$

ce qui implique que

$$\frac{m+n}{2} \equiv n\ mod\ 4$$

car 4 divise $D$.
Mais alors $\frac{m+n}{2} - 1 \equiv n - 1 \equiv 0\ mod\ 4$ car $n$ est impair
donc $n-1$ pair.
D'où $\frac{m+n-2}{4} \equiv 0\ mod\ 2$
Ce qui nous donne le résultat.
Donc, dans tous les cas, $m$, $n$ impairs positifs $\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right)$ pour $D \equiv 0,\ 1\ mod\ 4$ ■

**Lemme 2**

*Pour toute classe $a$ mod $D$ avec $(a, D) = 1$,*
*$\exists m \geq 3$ impair tel que $a$ mod $D = m$ mod $D$ et $(m, D) = 1$.*

**Démonstration :** :

**$1^{er}$ cas : $D$ pair**

Comme $(a, D) = 1$, on a donc $a$ impair.
Ce qui implique que, pour tout $\lambda \in \mathbb{Z}$, on a $a + \lambda D$ impair.
Bien entendu, on peut trouver $\lambda_0 \in \mathbb{Z}$ tel que $a + \lambda_0 D \geq 3$.
Donc, en posant $m = a + \lambda_0 D$, on a trouvé un $m$ qui convient.

**$2^{ème}$ cas : $D$ impair**
Il existe bien sur comme avant un $\lambda \in \mathbb{Z}$ tel que $a + \lambda D > 0$.
Si $a + \lambda D$ est impair, $m = a + \lambda D$ convient.
Sinon $m = a + \lambda D + signe(D)\ D$ convient car $D$ est impair. ■

**Théorème 2**

*Si $D \equiv 0,\ 1 \ mod\ 4$ est un entier non nul, alors il existe un unique homomorphisme*

$$\chi : \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^* \longrightarrow \{\pm 1\} \ tel\ que\ \chi(m \ mod\ D) = \left(\frac{D}{m}\right)$$

*pour $m \geq 3$ impair premier avec $D$.*
*De plus, $\chi$ est sujective si et seulement si $D$ n'est pas un carré dans $\mathbb{Z}$.*
*On appellera $\chi$ le* ***symbole de Kronecker ou morphisme de Kronecker*** *associé à $D$ noté aussi $\chi_D$ s'il y a une confusion possible.*
*En outre,*

$$\chi(-1 \ mod\ D) = \begin{cases} 1 & si\ D > 0, \\ -1 & si\ D < 0. \end{cases}$$

*et*

$$\chi(2 \ mod\ D) = \begin{cases} 1 & si\ D \equiv 1 \ mod\ 8, \\ -1 & si\ D \equiv 5 \ mod\ 8. \end{cases}$$

*(On remarque que le cas $D \equiv 0 \ mod\ 4$ disparait ici puisque on doit avoir $D$ et 2 premier entre eux).*

**Démonstration :** :

**Définition** :
Les deux lemmes que nous venons de démontrer montrent en fait que l'application $\chi$ est bien définie.
Le premier lemme montre que l'application $\chi$ qui est définie sur un ensemble quotient ne dépend pas du représentant choisi et le deuxième lemme montre que pour tout élément de $\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^*$, il existe un représentant comme dans le théorème.

On voit facilement que $\chi$ est un morphisme (en choisissant dans chaque classe un représentant $m \geq 3$, impair premier avec $D$ et en utilisant les propriétés du symbole de Jacobi).
**Unicité** :
Elle découle directement de la définition de $\chi$ et du lemme 2.

**Surjectivité** :
Il est clair que si $D$ est un carré dans $\mathbb{Z}$, alors $\chi$ est le morphisme trivial.

Nous voulons ensuite montrer que, si $D$ n'est pas un carré dans $\mathbb{Z}$, alors $\chi$ est surjectif, ie il existe $m$ impair tel que $(m \wedge D) = 1$ tel que $\left(\frac{D}{m}\right) = -1$.
Puisque on a déjà $\chi(1 \ mod\ D) = 1$ ($\chi$ est un morphisme).

On pose $D = \delta^2 2D'$ où $D'$ est impair sans facteurs carré et $\delta \in \mathbb{Z}$.

Supposons $D' \neq 1$. On impose $m \equiv 1 \ mod \ 8$ donc $\left(\frac{2}{m}\right) = 1$.
On a alors :

$$\left(\frac{D}{m}\right) = \left(\frac{D'}{m}\right) \times \left(\frac{2}{m}\right) = \left(\frac{m}{D'}\right) \times 1$$

car $m \equiv 1 \ mod \ 4$. On peut écrire $D' = p_1..p_r, \ avec \ des \ p_i \geq 3$ premier distincts car on a supposé que $D$ n'était pas un carré dans $\mathbb{Z}$.
On a :

$$\left(\frac{m}{D'}\right) = \left(\frac{m}{p_1}\right)...\left(\frac{m}{p_r}\right)$$

On cherche $m$ tel que :

$$\left(\frac{m}{p_1}\right) = -1$$

et

$$\left(\frac{m}{p_i}\right) = 1 \ \forall i \geq 2$$

Comme il existe toujours des carrés et des non carrés modulo tout nombre premier $\geq 3$ le lemme chinois nous donne l'existence d'un $\alpha$ déterminée modulo $(8p_1...p_r)$ :

$$\begin{array}{rcl} \alpha & \equiv & 1 \ mod \ 8 \\ \alpha & \equiv & non \ carré \ mod \ p_1 \\ \alpha & \equiv & carré \ mod \ p_2 \\ & ... & \\ & ... & \\ & ... & \\ \alpha & \equiv & carré \ mod \ p_r. \end{array}$$

Il existe $m \geq 3$ impair tel que $m \equiv \alpha \ mod \ (8p_1...p_r)$.
Il vérifie

$$\begin{array}{rcl} \left(\frac{D}{m}\right) = \left(\frac{m}{D'}\right) & = & \left(\frac{m}{p_1}\right)...\left(\frac{m}{p_r}\right) \\ & = & \left(\frac{\alpha}{p_1}\right)...\left(\frac{\alpha}{p_r}\right) \\ & = & (-1) \times 1 \times ... \times 1 \\ & = & -1 \end{array}$$

Si $D' = 1$ et $\left(\frac{D}{3}\right) = \left(\frac{2}{3}\right) = -1$ donc $m = 3$ convient.
$\chi$ est donc surjective.

**Montrons que :**

$$\chi(-1 \ mod \ D) = \begin{cases} 1 & si \ D > 0, \\ -1 & si \ D < 0. \end{cases}$$

Il faut toujours considérer les 4 cas.

**<u>$1^{er}$ cas :</u>**

$$D > 0 \ et \ D \equiv 1 \ mod \ 4$$

Soit $m$ impair $\geq 3$, $m \equiv -1 \ mod \ D$
On peut choisir $m = -1 + 4D$

$$\begin{aligned}\chi(-1\ mod\ D) &= \left(\frac{D}{-1+4D}\right)\\ &= \left(\frac{-1+4D}{D}\right)(-1)^{\frac{D-1}{2}\frac{-2+4D}{2}}\\ &= \left(\frac{-1}{D}\right)(-1)^{\frac{D-1}{2}\frac{-2+4D}{2}}\\ &= (-1)^{\frac{D-1}{2}}(-1)^{\frac{D-1}{2}\frac{-2+4D}{2}}\\ &= (-1)^{\frac{D-1}{2}\frac{4D}{2}}\end{aligned}$$

Donc

$$\chi(-1\ mod\ D) = 1$$

**$2^{ème}$ cas :**

$$D > 0\ et\ D \equiv 0\ mod\ 4$$

On écrit $D$ sous la forme $D = 2^k d$ où $d$ est impair.
On peut choisir $m = -1 + D$, où $m \geq 3$, impair.

$$\begin{aligned}\chi(-1\ mod\ D) &= \left(\frac{D}{-1+D}\right) = \left(\frac{2}{-1+D}\right)^k \left(\frac{d}{-1+D}\right)\\ &= \left(\frac{-1+D}{d}\right)(-1)^{\frac{d-1}{2}\frac{-2+D}{2}}(-1)^{\frac{(-D+1)^2-1}{8}k}\\ &= \left(\frac{-1}{d}\right)(-1)^{\frac{d-1}{2}\frac{-2+D}{2}}(-1)^{\frac{(D-1)^2-1}{8}k}\\ &= (-1)^{\frac{d-1}{2}\frac{-2+D}{2}+\frac{d-1}{2}}(-1)^{\frac{(D-1)^2-1}{8}k}\\ &= (-1)^{\frac{d-1}{2}\frac{D}{2}}(-1)^{\frac{(D-1)^2-1}{8}k}\end{aligned}$$

Comme

$$D \equiv 0\ mod\ 4$$

on a $\frac{D}{2}$ pair et $d$ impair implique $d-1$ pair
donc $\frac{d-1}{2}\frac{D}{2}$ est pair
Ainsi

$$(-1)^{\frac{d-1}{2}\frac{D}{2}} = 1.$$

Si $k$ pair, on a $\frac{(D-1)^2-1}{8}k$ pair
et donc

$$(-1)^{\frac{(D-1)^2-1}{8}k} = 1.$$

Si $k$ est impair comme $k \geq 2$, on a $k \geq 3$
donc 8 divise $D$
ie

$$\exists \lambda \in \mathbb{Z}\ tel\ que\ D = 8\lambda$$

et alors

$$(D-1)^2 - 1 = (8\lambda - 1)^2 - 1 = 64\lambda^2 - 16\lambda \equiv 0\ mod\ 16$$

donc

$$(-1)^{\frac{(D-1)^2-1}{8}k} = 1.$$

Ce qui montre que

$$\chi(-1 \ mod \ D) = 1.$$

**3$^{ème}$ cas :**

$$D < 0 \ et \ D \equiv 1 \ mod \ 4$$

On peut choisir $m = -1 - 4D$ où $m \geq 3$, impair.

$$\begin{aligned}
\chi(-1 \ mod \ D) &= \left(\frac{D}{-1-4D}\right) \\
&= \left(\frac{-1}{-1+4D}\right)\left(\frac{-D}{-1-4D}\right) \\
&= (-1)^{(-1-2D)}(-1)^{\frac{-1-D}{2}(-1-2D)}\left(\frac{-1-4D}{-D}\right) \\
&= (-1)^{\frac{1-D}{2}(-1-2D)}\left(\frac{-1}{-D}\right) \\
&= (-1)^{\frac{1-D}{2}(-1-2D)}(-1)^{\frac{-1-D}{2}}
\end{aligned}$$

On a

$$D \equiv 1 \ mod \ 4$$

donc

$$D - 1 \equiv 0 \ mod \ 4$$

d'où

$$\frac{1-D}{2}(-1-2D) \ est \ pair$$

ainsi

$$(-1)^{\frac{1-D}{2}(-1-2D)} = 1$$

. De plus,

$$-D \equiv -1 \ mod \ 4$$

donc

$$-D - 1 \equiv -2 \ mod \ 4$$

D'où

$$\frac{-D-1}{2} \equiv -1 \ mod \ 4.$$

Donc c'est un nombre impair
Par suite,

$$\chi(-1 \ mod \ D) = -1$$

**4$^{ème}$ cas :**

$$D < 0 \ et \ D \equiv 0 \ mod \ 4$$

On peut choisir $m = -1 - D$ $m \geq 3$, impair.

On écrit $D$ sous la forme $D = 2^k d$ où $d$ est impair.

$$\begin{aligned}
\chi(-1\ mod\ D) &= \left(\frac{D}{-1-D}\right) \\
&= \left(\frac{2}{-1-D}\right)^k \left(\frac{d}{-1-D}\right) \\
&= \left(\frac{2}{-1-D}\right)^k \left(\frac{-1}{-1-D}\right)\left(\frac{-d}{-1-D}\right) \\
&= (-1)^{\left(\frac{-2-D}{2}\right)}(-1)^{\frac{-2-D}{2}\frac{-1-d}{2}}\left(\frac{-1-D}{-d}\right)(-1)^{\left(\frac{(-1-D)^2-1}{8}\right)k} \\
&= (-1)^{\left(\frac{-2-D}{2}\right)}(-1)^{\frac{-D}{2}\frac{-1-d}{2}}(-1)^{\left(\frac{(-1-D)^2-1}{8}\right)k}
\end{aligned}$$

Comme $D \equiv 0\ mod$ , on a que $\frac{-2-D}{2}$ est impair donc $-1)^{\left(\frac{-2-D}{2}\right)} = -1$ et $\frac{-D}{2}$ est pair donc $(-1)^{\frac{-D}{2}\frac{-1-d}{2}} = 1$.
Reste à étudier la parité de $\left(\frac{(-1-D)^2-1}{8}\right)k$.
Si $k$ est pair on a que $\left(\frac{(-1-D)^2-1}{8}\right)k$ est pair et par suite $(-1)^{\left(\frac{(-1-D)^2-1}{8}\right)k} = 1$.
Si $k$ est impair, alors $k \geq 3$ donc $D$ est divisible par 8 i.e. il existe $\lambda \in \mathbb{Z}$ tel que $-D-1 = -1-8\lambda$ et par suite $(-1-D)^2 - 1 = (-1-8\lambda)^2 - 1 = 64\lambda^2 - 16\lambda = 16 \times (3\lambda^3 - 1)$ ainsi $\frac{(-1-D)^2-1}{2}$ est pair d'où on a aussi dans ce cas $(-1)^{\left(\frac{(-1-D)^2-1}{8}\right)k} = 1$.
C'est ainsi que l'on obtient que $\chi(-1\ mod\ D) = -1$ lorsque $D < 0$ et $D \equiv 0\ mod\ 4$.

**Montrons que :**

$$\chi(2\ mod\ D) = \begin{cases} 1 & si\ D \equiv 1\ mod\ 8, \\ -1 & si\ D \equiv 5\ mod\ 8. \end{cases}$$

**1$^{er}$ cas :**

$$D > 0\ et\ D \equiv 1\ mod\ 4$$

Soit $m$ impair, $m \equiv 2\ mod\ D$ et $m \geq 3$.
On peut choisir $m = 2 + D$

$$\begin{aligned}
\chi(2\ mod\ D) &= \left(\frac{D}{2+D}\right) \\
&= \left(\frac{2+D}{D}\right)(-1)^{\frac{D-1}{2}\frac{D+1}{2}} \\
&= \left(\frac{2}{D}\right)(-1)^{\frac{D-1}{2}\frac{D+1}{2}} \\
&= (-1)^{\frac{D^2-1}{8}}(-1)^{\frac{D-1}{2}\frac{D+1}{2}}
\end{aligned}$$

Ici, si

$$D \equiv 1\ mod\ 8\ ou\ D \equiv\ 5\ mod\ 8$$

On a

$$D - 1 \equiv 0\ mod\ 4$$

Donc

$$(-1)^{\frac{D-1}{2}\frac{D+1}{2}} = 1$$

Maintenant, si

$$D \equiv 1 \ mod \ 8$$

on a que

$$\exists \lambda \in \mathbb{Z} \ tel \ que \ D = 1 + 8\lambda$$

et

$$D^2 - 1 = 64\lambda^2 + 16\lambda$$

Par suite, $\frac{D^2-1}{8}$ est pair.
Mais alors,

$$(-1)^{\frac{D^2-1}{8}} = 1$$

Enfin,

$$\chi(2 \ mod \ D) = 1$$

Si

$$D \equiv 5 \ mod \ 8$$

on a que

$$\exists \lambda \in \mathbb{Z} \ tel \ que \ D = 5 + 8\lambda$$

et

$$D^2 - 1 = 64\lambda^2 + 80\lambda + 24$$

donc

$$\frac{D^2 - 1}{8} = 8\lambda^2 + 10\lambda + 3 \ est \ impair$$

Mais alors,

$$(-1)^{\frac{D^2-1}{8}} = -1$$

Enfin,

$$\chi(2 \ mod \ D) = -1$$

**$2^{ème}$ cas :**

$$D < 0 \ et \ D \equiv 1 \ mod \ 4$$

Soit $m$ impair, $m \equiv 2 \ mod \ D$, $m \geq 3$.
On peut choisir $m = 2 - D$

$$\begin{aligned}
\chi(2 \ mod \ D) &= \left(\frac{D}{2-D}\right) \\
&= \left(\frac{-1}{2-D}\right)\left(\frac{-D}{2-D}\right) \\
&= (-1)^{\frac{1-D}{2}}\left(\frac{2-D}{-D}\right)(-1)^{\frac{-D-1}{2}\frac{1-D}{2}} \\
&= (-1)^{\frac{1-D}{2}}\left(\frac{2}{-D}\right)(-1)^{\frac{-D-1}{2}\frac{1-D}{2}} \\
&= (-1)^{\frac{D^2-1}{8}}(-1)^{\frac{1-D}{2}}(-1)^{\frac{-D-1}{2}\frac{1-D}{2}} \\
&= (-1)^{\frac{D^2-1}{8}}(-1)^{\frac{-D+1}{2}\frac{1-D}{2}}
\end{aligned}$$

Ici, si

$$D \equiv 1 \ mod\ 8 \ ou \ D \equiv \ 5 \ mod\ 8$$

On a

$$-D + 1 \equiv 0 \ mod\ 4$$

Donc

$$(-1)^{\frac{-D+1}{2}\frac{1-D}{2}} = 1$$

Comme dans le premier cas, si

$$D \equiv 1 \ mod\ 8$$

on a que

$$(-1)^{\frac{D^2-1}{8}} = 1$$

Donc,

$$\chi(2 \ mod\ D) = 1$$

et si

$$D \equiv 5 \ mod\ 8$$

on a que

$$(-1)^{\frac{D^2-1}{8}} = -1$$

Enfin,

$$\chi(2 \ mod\ D) = -1$$

■

On va montrer la "réciproque" c'est à dire le résultat suivant :

**Théorème 3**

*On suppose que le théorème 2 est satisfait pour tout $D \equiv 0$ ou $1 \ mod\ 4$. Alors la loi de réciprocité quadratique et les lois complémentaires sont vraies.*

**Démonstration :** :

Soient $p$ et $q$ des premiers disctincts impairs.
Posons

$$p^* = (-1)^{\frac{p-1}{2}} p.$$

De sorte que,

$$p^* \equiv 1 \ mod\ 4$$

en effet,
comme $p$ est impair, on a que $p \equiv 1 \ mod\ 4$ ou $p \equiv 3 \ mod\ 4$
Si $p \equiv 1 \ mod\ 4$, on a $\frac{p-1}{2}$ pair
Donc $p^* = p \equiv 1 \ mod\ 4$
Si $p \equiv \ 3 \ mod\ 4$, on a $\frac{p-1}{2}$ impair

Donc $p^* = -p \equiv 1 \ mod \ 4$.
Donc on peut considérer $\chi = \chi_D$ où $D = p^*$.
Le but ici est de montrer que :

$$\chi(q) = \left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

Car

$$\begin{aligned}\left(\tfrac{p^*}{q}\right) &= \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\tfrac{p}{q}\right) \\ &= \left(\tfrac{(-1)}{q}\right)^{\frac{p-1}{2}}\left(\tfrac{p}{q}\right) \\ &= (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\tfrac{p}{q}\right).\end{aligned}$$

On a que $\chi$ est l'unique homomorphisme du groupe cyclique $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ vers $\{\pm 1\}$ qui est surjectif puisque ici $D$ n'est pas un carré dans $\mathbb{Z}$.
Or, l'application $\left(\frac{\cdot}{q}\right) : \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \longrightarrow \{\pm 1\}$ est elle aussi clairement un morphisme par définition du symbole de Legendre. De plus il est facile de voir qu'il est surjectif (car il y a toujours des carrés et des non carrés modulo un nombre premier impair) donc les deux morphismes sont égaux, ce qui montre l'égalité souhaitée.

On va établir maintenant les formules complémentaires. Pour la première formule concernant la valeur $-1$ :

Etant donné qu'elle fait intervenir les congruences modulo 4, il est naturel de considérer l'application $\chi$ pour $D = -4$. On veut montrer que :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

ie :

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & si \quad p \equiv 1 \ mod \ 4 \\ -1 & si \quad p \equiv 3 \ mod \ 4 \end{cases}$$

Soit $p$ un premier impair tel que $p \equiv 1 \ mod \ 4$.
On a donc :

$$\chi(p \ mod \ 4) = \chi(1 \ mod \ 4) = 1$$

Ainsi

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = 1 \ si \ p \equiv 1 \ mod \ 4.$$

Soit $p$ un premier impair tel que $p \equiv 3 \ mod \ 4$.
On a donc :

$$\chi(p \ mod \ 4) = \chi(3 \ mod \ 4) = \left(\frac{-4}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

Ainsi

$$\left(\frac{-1}{p}\right) = -1 \ si \ p \equiv 3 \ mod \ 4.$$

Pour la seconde formule concernant la valeur 2 :
Etant donné qu'elle fait intervenir les congruences modulo 8, il est naturel de considérer l'application $\chi$ pour $D = 8$.

On veut montrer que :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

ie :

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & si \quad p \equiv 1 \ mod \ 8 \\ -1 & si \quad p \equiv 3 \ mod \ 8 \\ -1 & si \quad p \equiv 5 \ mod \ 8 \\ 1 & si \quad p \equiv 7 \ mod \ 8 \end{cases}$$

Soit $p$ un premier impair tel que $p \equiv 1 \ mod \ 8$.
On a donc :

$$(\frac{2}{p}) = (\frac{8}{p}) = \chi(p \ mod \ 8) = \chi(1 \ mod \ 8) = 1$$

Ainsi $\left(\frac{2}{p}\right) = 1 \ si \ p \equiv 1 \ mod \ 8$

Soit $p$ un premier impair tel que $p \equiv 3 \ mod \ 8$.
On a donc :

$$(\frac{2}{p}) = \chi(p \ mod \ 8) = \chi(3 \ mod \ 8) = \left(\frac{2}{3}\right) = -1$$

car 2 n'est pas un carré modulo 3.
Ainsi $\left(\frac{2}{p}\right) = -1 \ si \ p \equiv 3 \ mod \ 8$

Soit $p$ un premier impair tel que $p \equiv 5 \ mod \ 8$
On a donc :

$$(\frac{2}{p}) = \chi(p \ mod \ 8) = \chi(5 \ mod \ 8) = \left(\frac{2}{5}\right) = -1$$

car 2 n'est pas un carré modulo 5.
Ainsi $\left(\frac{2}{p}\right) = -1 \ si \ p \equiv 5 \ mod \ 8$
Soit $p$ un premier impair tel que $p \equiv 7 \ mod \ 8$.
On a donc :

$$(\frac{2}{8}) = \chi(p \ mod \ 8) = \chi(7 \ mod \ 8) = \left(\frac{2}{7}\right) = 1$$

car 2 est un carré modulo 3.
Ainsi $\left(\frac{2}{p}\right) = 1 \ si \ p \equiv 7 \ mod \ 8$.

# 2 La loi de réciprocité d'Artin sur $\mathbb{Q}$ :

## 2.1 Arithmétique des extensions quadratiques de $\mathbb{Q}$

L'objet de cette partie est de faire des rappels concernant les extensions quadratiques dont nous aurons besoin pour la suite.
Elle ne comportera donc pas les démonstrations des résultats énoncés (si le lecteur désire les consulter il poura se reporter au livre "Samuel Théorie algébrique des nombres".

### 2.1.1 Définition des corps quadratiques

**Définition 1**

*On appelle corps quadratique toute extension de degré 2 du corps $\mathbb{Q}$ des nombres rationnels.*

Si $K$ est un corps quadratique, tout élément $x$ de $K - \mathbb{Q}$ est de degré 2 sur $\mathbb{Q}$, donc est un élément primitif de $K$ (i.e. $K = \mathbb{Q}[x]$, et $(1,\ x)$ est une base de $K$ sur $\mathbb{Q}$).
Soit $F(X) = X^2 + bX + c$ $(b,\ c \in \mathbb{Q})$, le polynôme minimal d'un tel élément $x \in K$. La résolution de l'équation du second degré $x^2 + bx + c = 0$ donne $2x = -b \pm \sqrt{b^2 - 4c}$.
Ainsi $K = \mathbb{Q}(\sqrt{b^2 - 4c})$.
Or $b^2 - 4c$ est un nombre rationnel $\frac{u}{v} = \frac{uv}{v^2}$ avec $u, v \in \mathbb{Z}$ ; on a donc aussi $K = \mathbb{Q}(\sqrt{uv})$ avec $uv \in \mathbb{Z}$.
Par le même procédé on voit qu'on peut enfin écrire $K = \mathbb{Q}(\sqrt{d})$ où $d$ est un entier sans facteurs carrés.

**Proposition 3**

*Tout corps quadratique est de la forme $\mathbb{Q}(\sqrt{d})$, où $d$ est un entier sans facteur carrés.*

L'élément $\sqrt{d}$ est racine du polynôme irréductible $X^2 - d$.
Il admet un *conjugué* dans $K$, à savoir $-\sqrt{d}$. Il existe donc un automorphisme $\sigma$ de $K$ qui applique $\sqrt{d}$ sur $-\sqrt{d}$.

L'élément général de $K$ est de la forme $a + b\sqrt{d}$ avec $a,\ b \in \mathbb{Q}$, et on a

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d} \tag{11}$$

Ainsi $Gal(K/Q) = \{id, \sigma\}$ est abélien.

### 2.1.2 L'anneau des entiers d'un corps quadratique

Nous noterons $O_K$ l'anneau des entiers de $K$.
La structure de cet anneau dépendant de la valeur de $d$ modulo 4.

**Théorème 4**

*Soit $K = \mathbb{Q}[\sqrt{d}]$ un corps quadratique, avec $d \in \mathbb{Z}$, sans facteur carré (et donc $\not\equiv 0$ mod 4).*
*a) Si $d \equiv 2$ ou 3 mod 4, l'anneau $O_K$ des entier de $K$ est l'ensemble des $a + b\sqrt{d}$, avec $a, b \in \mathbb{Z}$.*
*b) Si $d \equiv 1$ mod 4, l'anneau $O_K$ des entier de $K$ est l'ensemble des $\frac{1}{2}(u + v\sqrt{d})$, avec $u, v \in \mathbb{Z}$ de même parité.*
*Dans le cas où $d \equiv 2$ ou 3 mod.4, une base du $\mathbb{Z}-$module $O_K$ est évidemment $(1, \sqrt{d})$.*
*Dans le cas $d \equiv 1 \mod 4$, une base du $\mathbb{Z}-$module $O_K$ est $(1, \frac{1}{2}(1+\sqrt{d}))$.*
*On notera $\omega_d$ :*

$$\begin{cases} \sqrt{d} & \text{dans le cas où} d \equiv 2 \text{ ou } 3 \text{ mod } 4. \\ \frac{1+\sqrt{d}}{2} & \text{dans le cas où} d \equiv 1 \text{ mod } 4. \end{cases}$$

*Ainsi, on aura $O_K = \mathbb{Z}[\omega_d]$ dans les deux cas. Pour finir un peu de terminologie :*
*Si $d > 0$ , on dit que $\mathbb{Q}(\sqrt{d})$ est **un corps quadratique réel** (car il existe un sous-corps de $\mathbb{R}$ conjugué de $\mathbb{Q}(\sqrt{d})$).*
*Si $d < 0$, on dit que $\mathbb{Q}(\sqrt{d})$ est **un corps quadratique imaginaire**.*

### 2.1.3 Discriminant et ramification

Prenons $K = \mathbb{Q}[\sqrt{d}]$ où $d$ est un entier sans facteurs carrés.
a) Si $d \equiv 2$ *ou* 3 *mod* 4, $(1, \sqrt{d})$ est une base de l'anneau des entiers de $K$. Comme $Tr(1) = 2$, $Tr(d) = 2d$, on a $D(1, \sqrt{d}) = 4d$.
Les nombres premiers qui se ramifient dans $L$ sont donc 2 et les diviseurs premiers de $d$.
b) Si $d \equiv 1$ *mod* 4, $\left(1, \frac{1+\sqrt{d}}{2}\right)$ est une base de l'anneau des entiers de $K$.
On a

$$Tr(1) = 2,\ Tr\left(\frac{1+\sqrt{d}}{2}\right) = 1 \tag{12}$$

et

$$Tr\left(\left(\frac{1+\sqrt{d}}{2}\right)^2\right) = Tr\left(\frac{d+1}{4} + \frac{1}{2}\sqrt{d}\right) = \frac{d+1}{2} \tag{13}$$

D'où,

$$D\left(1, \frac{1+\sqrt{d}}{2}\right) = 2.\frac{d+1}{2} - 1 = d.$$

Les nombres premiers qui se ramifient dans $K$ sont donc les diviseur de $d$.
On remarque qu'un corps quadratique $\mathbb{Q}[\sqrt{d}]$ est uniquement déterminé par son discriminant $D_K$. On notera aussi que le discriminant d'un corps quadratique n'est pas un entier arbitraire.

### 2.1.4 Décomposition d'un premier dans un corps quadratique

Soient $d \in \mathbb{Z}$ un entier sans facteur carrés, $K$ le corps quadratique $\mathbb{Q}[\sqrt{d}]$ et $p$ un nombre premier.
La proposition qui suit donne la décomposition en idéaux premiers de l'idéal $p\mathbb{Z}$ dans $O_K$.

**Proposition 4**

*Soit $K = \mathbb{Q}[\sqrt{d}]$ un corps quadratique, où $d \in \mathbb{Z}$ est sans facteurs carrés.*
*a) Sont décomposés dans $K$ i.e. $pO_K = \mathfrak{p}_1\mathfrak{p}_2$ où $\mathfrak{p}_1$, $\mathfrak{p}_2$ sont des idéaux premier dans $O_K$ tels que $\mathfrak{p}_1 = \sigma(\mathfrak{p}_2)$, les nombres premiers impairs $p$ tels que $d$ est résidu quadratique mod $p$, et 2 si $d \equiv 1$ mod 8 ;*
*b) Sont inertes dans $K$ i.e. $pO_K = \mathfrak{p}$ où $\mathfrak{p}$ est un idéal premier dans $O_K$, les nombres premiers impairs $p$ tels que $d$ est non-résidu mod $p$, et 2 si $d \equiv 5$ mod 8 ;*
*c) Se ramifient dans $K$ i.e. $pO_K = \mathfrak{p}^2$ où $\mathfrak{p}$ est un idéal premier dans $O_K$, les diviseurs premiers impairs de $d$, et 2 si $d \equiv 2$ ou 3 (mod 4)*

## 2.2 L'application d'Artin d'un corps quadratique sur $\mathbb{Q}$

Soit $K$ un corps quadratique et $p$ un premier non ramifié dans $K$. Notons $G = Gal(K\backslash\mathbb{Q}) = \{Id,\ \sigma\}$. Soit $\mathfrak{p}$ idéal premier tel que $p \in \mathfrak{p}$.

### 2.2.1 Groupe de décomposition dans le cas d'un corps quadratique

Le groupe de décomposition en $p$, que l'on notera $G_p$ est défini par :

$$G_p = \{f \in G \mid f(\mathfrak{p}) = \mathfrak{p}\}$$

La notation ne prend pas en compte l'idéal $\mathfrak{p}$ au dessus de $p$ choisi car ce groupe est indépendant de celui-ci.
On va déterminer à la main **le groupe de décomposition en** $p$ en séparant les cas inerte et totalement décomposé pour $p$ non ramifié.

$1^{er}$ **cas :** Supposons que $p$ est inerte, donc que $pO_K = \mathfrak{p}$.
Soit $f \in G$, on a $f(\mathfrak{p}) = f(pO_K) = pf(O_K) = pO_K = \mathfrak{p}$.
On a donc $G_p = G$

$2^{ème}$ **cas :** Supposons que $p$ est totalement décomposé i.e. il y a exactement deux idéaux premiers distincts au-dessus de $p$ et si l'un d'eux est noté $\mathfrak{p}$ l'autre sera $\sigma(\mathfrak{p})$.
Soit $f \in G$, on a $f(\sigma(\mathfrak{p})) = \sigma(\mathfrak{p}) \iff \sigma^{-1}f\sigma(\mathfrak{p}) = f(\mathfrak{p}) = \mathfrak{p}$ car $G$ est abélien.
On retrouve bien que $G_p$ est indépendant de l'idéal choisi.
Soit $f \in G$.

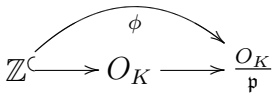
$$f(\mathfrak{p}) = \begin{cases} \mathfrak{p} & si\ f = id \\ \sigma(\mathfrak{p}) & sif = \sigma \end{cases}$$

Or comme $p$ est totalement décomposé, on a $\mathfrak{p}$ et $\sigma(\mathfrak{p})$ distincts.
Donc $G_p = Id$.

**En résumé**
**- si $p$ est inerte alors $G_p = G$.**
**- si $p$ est totalement décomposé alors $G_p = \{Id\}$.**

### 2.2.2 Groupe de Galois du corps résiduel et morphisme de Frobénius

On a les applications suivantes :




et

$$ker\phi = \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$$

Ainsi, on a

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \hookrightarrow \frac{O_K}{\mathfrak{p}}$$

Le corps résiduel en $\mathfrak{p}$ est un corps fini de cardinal $\mathcal{N}(\mathfrak{p})$ et $Gal\big(\frac{O_K}{\mathfrak{p}}, \mathbb{F}_p\big)$ est un groupe cyclique engendré par le Frobénius $Fr : x \mapsto x^p$.

**Propriété 3 (*Description du groupe de Galois résiduel*)**

*Dans le cas, $p$ totalement décomposé $\frac{O_K}{\mathfrak{p}} = \frac{\mathbb{Z}}{p\mathbb{Z}}$, donc le groupe de galois est trivial i.e. $Fr = id$.*
*Dans le cas où $p$ est inerte, on a $\frac{O_K}{\mathfrak{p}} = \frac{O_K}{pO_K}$ qui est de cardinal $p^2$ et $Fr$ est d'ordre 2 égal à $[\frac{O_K}{\mathfrak{p}} : \frac{\mathbb{Z}}{p\mathbb{Z}}]$.*

**Démonstration :** :
La preuve se base sur le résultat suivant :

$$pO_K = \mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r} \text{ où } \mathfrak{p}_i \text{sont des idéaux premiers distincts de} O_K$$

Pour $i \in \{1, .., r\}$, $e_i$ désigne l'indice de ramification de p en $\mathfrak{p}_i$ et $\left[\frac{O_K}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{p\mathbb{Z}}\right] = f_i$ est le degré résiduel de $p$ en $\mathfrak{P}_i$.
On a alors :

$$[K : \mathbb{Q}] = \sum_{i=1}^{r} e_i f_i$$

■

### 2.2.3 Construction de l'application d'Artin

Soit $f \in G_p$ comme $f(\mathfrak{p}) = \mathfrak{p}$, on voit que $\bar{f}$ induit un automorphisme de $\frac{O_K}{\mathfrak{p}}$ qui vérifie

$$\bar{f}(x \ mod \ \mathfrak{p}) = f(x) \ mod \ \mathfrak{p}$$

De plus, $\bar{f} \in \ Gal\big(\frac{O_K}{\mathfrak{p}}, \frac{\mathbb{Z}}{p\mathbb{Z}}\big)$.

**Proposition 5**

*Pour $p$ non ramifié dans $K$ l'application :*

$$\begin{array}{rccc} \gamma : & G_p & \to & Gal\left(\frac{O_K}{\mathfrak{p}}, \frac{\mathbb{Z}}{p\mathbb{Z}}\right) \\ & f & \mapsto & \bar{f} \end{array}$$

*est un isomorphisme de groupes.*

**Démonstration :** :

Si $p$ est totalement décomposé, il s'agit clairement du morphisme trivial qui est évidemment un isomorphisme dans ce cas là.
Supposons maintenant que $p$ est inerte.
On a :

$$ker(\gamma) := \{f \in G_p \backslash \bar{f} = Id\}$$

On veut montrer que $ker\ \gamma$ est trivial.
Soit $f \in ker(\gamma)$, donc tel que :

$$f(x) \equiv x\ mod\ \mathfrak{p} = pO_K\ \forall x \in O_K$$

Supposons que : $f = \sigma$
On aurait donc :

$$\sigma(x) - x \in pO_K = p\mathbb{Z} + p\mathbb{Z}\omega_d\ \ \forall x \in O_K$$

En posant $x = a + b\ \omega_d$, $a, b \in \mathbb{Z}$, on a $\sigma(x) = a + b\ \sigma(\omega_d)$.

on aurait alors :

$$\sigma(x) - x = b\ (\sigma(\omega_d) - \omega_d) \in pO_K$$

**Dans le cas où** $\omega_d = \sqrt{d}$ i.e. $d \equiv 2\ ou\ 3\ mod\ 4$,
on a $\sigma(x) - x = -2b\sqrt{d}$.
De $\sigma(x) - x \in p\mathbb{Z} + p\mathbb{Z}\omega_d$, il découle en particulier des calculs précédents que $p$ divise $2b\ \forall b \in \mathbb{Z}$ ce qui implique, que la seule possibilité est que $p = 2$.
Or 2 est inerte si et seulement si $d \equiv 5\ mod\ 8$ ce qui entraîne que $d \equiv 1\ mod\ 4$.
Ceci étant impossible, $f$ ne peut être égal à $\sigma$, donc $f$ est l'identité.

**Dans le cas où** $\omega_d = \frac{1+\sqrt{d}}{2}$ i.e. $d \equiv 1\ mod\ 4$,
on a $\sigma(x) - x = -b\sqrt{d}$. Pour $b = -1$, $\sqrt{d} \in pO_K$ implique qu'il existe $a', b' \in \mathbb{Z}$ tels que

$$\begin{array}{rcl} \sqrt{d} & = & pa' + pb'\left(\frac{1+\sqrt{d}}{2}\right) \\ & = & \left(pa' + \frac{pb'}{2}\right) + pb'\frac{\sqrt{d}}{2} \end{array}$$

Donc $pb' = 2$ et $pa' + 1 = 0$, ce qui est impossible. Donc $f = id$.
Donc $\gamma$ est une injection.

On a montre que :

$$|G_p| = |Gal(\frac{O_K}{\mathfrak{p}}, \mathbb{F}_p)| = 2 \text{ } si \text{ } p \text{ } est \text{ } inerte.$$

$\gamma$ est donc un isomorphisme.

■

Voici un résumé de ce que l'on vient d'établir :

**Soit $p$ non ramifié.**
**Il existe un unique automorphisme $f \in G$ tel que**

$$\forall x \in O_K, \ f(x) \equiv x^p \ mod \ p$$

**(car $pO_K$ est le produit des idéaux premiers au-dessus de p).**
**On le note $\left(\frac{K\backslash\mathbb{Q}}{p}\right)$, c'est le Frobénius en p.**
**On a :**

$$\left(\frac{K\backslash\mathbb{Q}}{p}\right) = Id \quad \Leftrightarrow \quad p \ totalement \ décomposé$$
$$\left(\frac{K\backslash\mathbb{Q}}{p}\right) = \sigma \quad \Leftrightarrow \quad p \ inerte$$

### 2.2.4 Lien avec le symbole de Legendre

On a en fait que :

$$\left(\frac{K\backslash\mathbb{Q}}{p}\right)(\sqrt{d}) = \epsilon_p\sqrt{d} \ avec \ \epsilon_p \in \{\pm 1\}$$

où

$$\epsilon_p = 1 \quad si \ p \ est \ totalement \ décomposé \quad \Leftrightarrow \quad \chi_{D_K}(p \ mod \ D_K) = 1$$
$$\epsilon_p = -1 \quad si \ p \ est \ inerte \quad \Leftrightarrow \quad \chi_{D_K}(p \ mod \ D_K) = -1$$

(ceci par le théorème 2).
Ceci met en évidence le lien avec $\left(\frac{\cdot}{p}\right)$.
On a :

$$\epsilon_p = \chi_{D_K}(p \ mod \ D_K) \ \forall p \nmid D_K$$

### 2.2.5 Réciprocité d'Artin

On se donne un $D \equiv 0$ *ou* $1$ *mod* $4$ qui n'est pas un carré.
$D$ peut alors être considéré comme le discriminant d'un polynôme irrédutible unitaire $P$ de degré 2 dans $\mathbb{Z}[X]$
En effet,
si $D \equiv 0$ *mod* $4$ alors on peut choisir $P = X^2 - \frac{D}{4}$.
si $D \equiv 1$ *mod* $4$ alors on peut choisir $X^2 + X + \frac{1-D}{4}$.
Soit $K$ le corps de rupture de $P$ sur $\mathbb{Q}$.
En fait, on a $D = carré \times D_K$. Le carré est égal à $[O_K : \mathbb{Z}[\theta]]^2$, où $\theta$ est une racine de $P$ dans $K$.
On pose alors :

$$\boldsymbol{I_D = \{\frac{a}{b};\ a,\ b \in \mathbb{Z}\ a,\ b > 0\ et\ a,\ b\ premier\ avec\ D\}}$$

On définit alors un morphisme de groupes appelé **application d'Artin associée à $D$** :

$$\begin{array}{rccc} \left(\frac{K\backslash\mathbb{Q}}{\cdot}\right) : & I_D & \longrightarrow & Gal(K\backslash\mathbb{Q}) \\ & \prod_{i=1}^{r} p_i^{\alpha_i} & \mapsto & \prod_i \left(\frac{K\backslash\mathbb{Q}}{p_i}\right)^{\alpha_i} \end{array}$$

où les $p_i$ ne divisent pas $D$ donc pas $D_K$ i.e. les $p_i$ ne sont pas ramifié dans $K$ et $\alpha_i \in \mathbb{Z}$.
On définit :

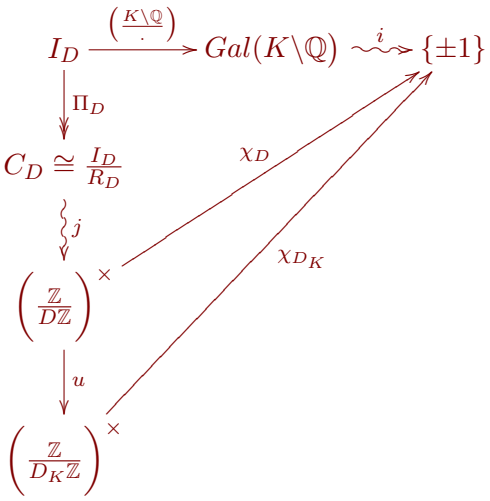
$$\boldsymbol{R_D = \{\frac{a}{b} \mid a,\ b \in \mathbb{Z}\ a > 0,\ b > 0,\ a,\ b\ premier\ avec\ p, a \equiv b\ mod\ D\}}$$

C'est un sous groupe de $I_D$.
On peut alors réécrire le théorème 2. de la manière suivante.

**Théorème 5**

*Le théorème 2 pour $D$ est équivalent à dire que l'application d'Artin est un morphisme de groupes surjectif dont le noyau contient $R_D$.*

**Démonstration :** :
On pose $C_D := \frac{I_D}{R_D}$ On a alors le diagramme suivant :




où les applications sont définies comme suit :

1. $$\left(\frac{K\backslash\mathbb{Q}}{\cdot}\right) \textit{ définie plus haut}$$
2. $$i = \begin{cases} Id & \longrightarrow & 1 \\ \sigma & \longrightarrow & -1 \end{cases}$$
3. $$\Pi_D : \begin{array}{ccc} I_D & \longrightarrow & C_D \\ \frac{a}{b} & \mapsto & \frac{a}{b} R_D \end{array}$$
4. $$j : \begin{array}{ccc} C_D & \longrightarrow & \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^\times \\ \frac{a}{b} R_D & \mapsto & (a \bmod D)(b \bmod D)^{-1} \end{array}$$
5. $$u : \begin{array}{ccc} \left(\frac{\mathbb{Z}}{D_K\mathbb{Z}}\right)^\times & \longrightarrow & \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^\times \\ a \bmod D & \mapsto & a \bmod D_K \end{array}$$
6. $$\chi_D \textit{ et } \chi_{D_K} \textit{ définie plus haut}$$

On a $\chi_D = \chi_{D_K} \circ u$ car $D/D_K$ et j est un isomorphisme de groupes.
L'assertion sur l'application d'Artin pour D et le théorème 2 sont alors équivalentes tous les deux à dire que le diagramme est un diagramme commutatif de morphismes de groupes surjectifs. ■

## 2.3 Enoncé de la réciprocité d'Artin sur $\mathbb{Q}$

### 2.3.1 Rappels sur la décomposition des idéaux premier dans une extension galoisienne de corps de nombres

Soit $K$ une extension galoisienne de $\mathbb{Q}$, $p$ un premier.
On rappelle ici quelques propriétés sur la décomposition des idéaux dans une extension Galoisienne.

$$On\ a\ :\ pO_K = (\mathfrak{p}_1...\mathfrak{p}_g)^e$$

pour des idéaux premiers distincts de $O_K$ ayant tous le même degré résiduel $f$ et

$$efg = [K : \mathbb{Q}]$$

De plus, l'action de $G$ sur les $\{\mathfrak{p}_i\}$ est transitive.

**Démonstration :** -Voir le livre de Samuel- ■

### 2.3.2 Automorphisme de Frobénius

Soit $K/\mathbb{Q}$ est une extension abélienne du groupe de Galois $G$.
Soit $p$ un nombre premier.
On a donc :

$$pO_K = (\mathfrak{p}_1...\mathfrak{p}_g)^e\ où\ \mathfrak{p}_i \text{ sont des idéaux premiers distincts } de\ O_K$$

Soit $G_p := \{f \in G / f(\mathfrak{p}_i) = \mathfrak{p}_i\}$ le stabilisateur de $\mathfrak{p}_i$ pour l'action de $G$ sur les $\{\mathfrak{p}_i\}$ qui est transitive : il ne dépend pas de $i$ car G est abélien.
En effet, $i \neq j$, il existe $\sigma \in G$ tel que $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$ car l'action de $G$ sur $\mathfrak{p}_i$ est transitive.
On a donc :

$$G_{\mathfrak{p}_j} = \sigma G_{\mathfrak{p}_i} \sigma^{-1} = G_{\mathfrak{p}_i}$$

car $G$ est abélien.
Ainsi, on pose $G_p = G_{\mathfrak{P}_i}$ : c'est le groupe de décomposition en $p$.
On a $card\ (G_p) = ef$ et $|Gal\big(\frac{O_K}{\mathfrak{p}},\ \frac{\mathbb{Z}}{p\mathbb{Z}}\big)| = f$.
Pour un idéal premier $\mathfrak{p}$ contenant $p$, on peut définir :

$$\begin{array}{ccc} G_p & \longrightarrow & Gal\big(\frac{O_K}{\mathfrak{p}}, \big(\frac{\mathbb{Z}}{p\mathbb{Z}}\big)\big) \\ f & \mapsto & (\bar{f} :\ x\ mod\ \mathfrak{p} \mapsto f(x)\ mod\ \mathfrak{p}) \end{array}$$

Il s'agit d'un morphisme surjectif (pour la preuve de ce résultat voir le livre de Samuel).
Il n'est pas injectif en général. Le noyau est de cardinal $\frac{ef}{f} = e$.

On a en fait que $p$ non ramifié est équivalent à $e = 1$ i.e. à $G_p \cong Gal\left(\frac{O_K}{\mathfrak{p}}, \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$ ou encore $|G_p| = f$.
De plus, $Gal\left(\frac{O_K}{\mathfrak{p}}, \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$ est cyclique engendré par $F \ : \ x \to x^p$.
Si $^p$ non ramifié, il existe donc un unique élèment $\left(\frac{K/\mathbb{Q}}{p}\right)$ de $G_p$ qui s'envoie sur $F$.
C'est l'unique automorphisme $f$ dans $G$ tel que

$$\forall x \in O_K, \ f(x) \equiv x^p \ mod \ pO_K$$

$$(\bar{f} \ : \ x \mapsto x^p).$$

Il s'agit du Frobénius en $p$.

**Propriété 4**

*Soit $K/\mathbb{Q}$ une extension abélienne et $p$ non ramifié dans $K$.*

1. *$\left(\frac{K/\mathbb{Q}}{p}\right)$ engendre $G_p$ et est d'ordre $f$.*
2. *Si $L$ est un sous corps de $K$, alors $L/\mathbb{Q}$ est aussi galoisienne donc abélienne. De plus, $p$ est non ramifié dans $L$ et $\left(\frac{L/\mathbb{Q}}{p}\right)$ est la restriction à $L$ de $\left(\frac{K/\mathbb{Q}}{p}\right)$.*

**Démonstration :** :

1. clair par ce qui a été fait précédemment, car l'isomorphisme $G_p \to Gal\left(\frac{O_K}{\mathfrak{p}}, \mathbb{F}_p\right) \cong \left(\frac{\mathbb{Z}}{f\mathbb{Z}}\right)$ envoie $\left(\frac{K/\mathbb{Q}}{p}\right)$ sur $(x \mapsto x^p)$.
2. $L/\mathbb{Q}$ galoisienne implique que $L$ est stable par $\left(\frac{K/\mathbb{Q}}{p}\right)$.
   Ceci entraine que la restriction $\sigma$ existe et est dans $Gal(L/\mathbb{Q})$.
   $\forall x \in O_L, \ \frac{(\sigma(x) - x^p)}{p} \in O_K \cap L$ par construction de $\left(\frac{K/\mathbb{Q}}{p}\right)$.
   Or $O_K \cap L = O_L$.
   Donc $\forall x \in O_L, \ \sigma(x) \equiv x^p \ mod \ pO_L$,
   d'où $\sigma = \left(\frac{L/\mathbb{Q}}{p}\right)$.

■

### 2.3.3 Loi de réciprocité d'Artin sur $\mathbb{Q}$

Par analogie avec le cas de corps quadratique sur $\mathbb{Q}$, on peut conjecturer les généralisations suivantes du théorème 5 :

**Théorème 6 (*Version faible*)**

*Soit $K/\mathbb{Q}$ une extension abélienne de groupe de Galois $G$. La forme faible de la réciprocité d'Artin dit qu'il existe $D \in \mathbb{N}$ divisible par les premiers ramifiés dans $K$ (ceux qui divise le discriminant $D_K$) tel que l'application d'Artin :*

$$\begin{array}{rccc} \left(\frac{K\backslash\mathbb{Q}}{\cdot}\right) : & I_D & \longrightarrow & Gal(K\backslash\mathbb{Q}) \\ & \prod_{i=1}^{r} p_i^{\alpha_i} & \mapsto & \prod_i \left(\frac{K\backslash\mathbb{Q}}{p_i}\right)^{\alpha_i} \end{array}$$

*où les $p_i$ ne divisent pas $D$ et les $\alpha_i \in \mathbb{Z}$, est un morphisme de groupe dont le noyau contient $R_D$.*
*Un tel $D$ est dit* ***"admissible"*** *pour le corps $K$.*
*La réciprocité d'Artin pour $D$ est équivalente à l'existence d'un morphisme surjectif de $\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times} \cong \frac{I_D}{R_D}$ sur $G$ qui envoie $p$ mod $D$ (où $p$ est un premier ne divisant pas $D$) sur $\left(\frac{K/\mathbb{Q}}{p}\right)$.*

**Théorème 7 (*Version forte*)**

*La version forte précise $D$ : par exemple tel que les facteurs premiers de $D$ soit exactement les premiers ramifiés dans $K$ ou $D = D_K$.*

**Remarque 1**

*Nous n'allons pas démontrer ces résultats subtils en toute généralité mais étudier dans la suite quelques unes de leurs conséquences et voir en quoi ils constituent une généralisation de la loi de réciprocité quadratique.*

**Exemple 2**

1. *Si $K/\mathbb{Q}$ est une* ***extension quadratique****, c'est fait avant.*
   *Dans ce cas le discriminant est admissible.*
2. ***Extension cyclotomique*** *$K = \mathbb{Q}(\zeta_n)$ où $\zeta_n = e^{\frac{2i\Pi}{n}}$*
   *On définit le morphisme de groupe :*

$$\begin{array}{rccc} \Lambda_n : & \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times} & \longrightarrow & G \\ & a \text{ mod } n & \longrightarrow & \phi_a \end{array}$$

   *où $\phi_a$ est l'unique automorphisme $K$ tel que $\zeta_n \longrightarrow \zeta_n^a$ où $a \wedge n = 1$.*
   *On a $\Lambda_n$ est injective et par l'égalité des cardinaux, c'est donc un isomorphisme*

*de groupes.*
*On a*

$$p\ ramifié \Rightarrow p/n$$

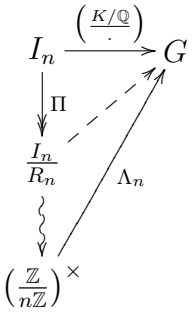
*Si* $p \nmid n$ *alors* $\left(\frac{K/\mathbb{Q}}{p}\right) = \phi_p$ *où* $\phi_p$ *est l'automorphisme qui envoie* $\zeta_n$ *sur* $\zeta_n^p$
*Pour le corps cyclotomique* $K$, *on a* $O_K = \mathbb{Z}[\zeta_n]$.
*Pour* $x \in O_K$, *on a* $x = a_0 + a_1\zeta_n^p + ... + a_{n-1}\zeta_n^{p^{n-1}}$ *avec* $a_i \in \mathbb{Z}$
*Donc*

$$\phi_p(x) \equiv a_0 + a_1\zeta_n^p + ... + a_{n-1}\zeta_n^{p^{n-1}} \equiv (a_0 + ... + a_{n-1}\zeta^{n-1})^p \ mod\ pO_K$$

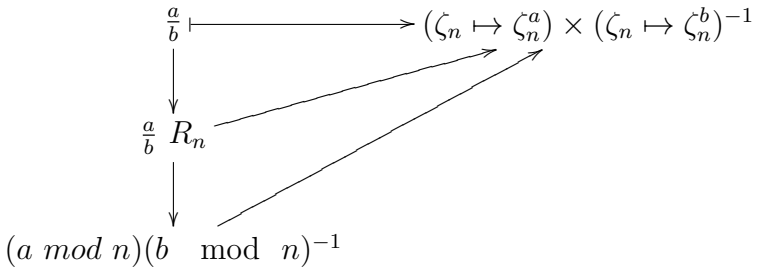
*où* $a_i \in \mathbb{Z}$ *(par le petit théorème de Fermat).*

$$\phi_p(x) \equiv x^p \ mod\ p\mathbb{Z}[\zeta_n] \Rightarrow \phi_p = \left(\frac{K/\mathbb{Q}}{p}\right)$$

*On a le diagramme commutatif suivant :*




*défini par :*




*Ainsi* $R_n \subset ker(\left(\frac{K/\mathbb{Q}}{\cdot}\right))$ *en d'autres termes la réciprocité de Artin est vraie pour* $D = n$ *c'est à dire dans le cas cyclotomique.*
*En général* $n \nmid D_K$ *mais c'est vrai si* $n$ *est minimal tel que* $K = \mathbb{Q}(\zeta_n)$. *On en déduit que la réciprocité d'Artin forte est vraie pour* $K$ *un corps cyclotomique avec* $D = D_K$ *: on compose simplement* $\Lambda_n$ *avec l'application naturelle* $\left(\frac{\mathbb{Q}}{D_K\mathbb{Z}}\right)^\times \longrightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$.

# 3 Conséquences sur la décompostion des nombres premiers dans une extension abélienne de $\mathbb{Q}$

## 3.1 Premiers totalements décomposés

**Définition 2**

*Soit $K/\mathbb{Q}$ une extension galoisienne finie de degré $n$.*
*On dit que* ***p nombre premier est totalement décomposé*** *dans $K$ si et seulement si $p$ $O_k$ est produit de $n$ idéaux premiers distincts,*
*c'est-à-dire si $e = f = 1$ où*

$$\begin{cases} e = \text{indice de ramification de } p \\ f = \text{degré résiduel} \end{cases}$$

On note $S(K)$ l'ensemble défini par :

$$\boldsymbol{S(K) = \{p \text{ premier totalement décomposé dans } K\}}$$

Si $p$ est non ramifié, l'ordre de $\left(\frac{K/\mathbb{Q}}{p}\right)$ est $f$. Donc la réciproque d'Artin donne immédiatement le résultat suivant :

**Théorème 8**

*On suppose que $K$ est une extension finie abélienne de $\mathbb{Q}$.*

1. *Un nombre premier $p$ est totalement décomposé dans $K$ si et seulement $p$ est non ramifié (i.e. $p \nmid D_k$) dans $K$ et $\left(\frac{K/\mathbb{Q}}{p}\right) = id$.*
2. *Soit $D$ un entier admissible pour $K$.*
   *Alors $p \in S(K)$ si et seulement $p \nmid D$ et $p$ appartient au noyau de l'application d'Artin associé à $D$.*
3. *Soit $D$ un entier admissible pour $K$.*
   *Alors il existe un sous groupe $H$ de $\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^\times$ tel que $S(K)$ soit l'ensemble des nombres premiers dont la classe modulo $D$ appartient à $H$.*
   *En particulier $S(K)$ peut se décrire à l'aide de conditions de congruences.*

**Remarque 2**

*La propriété 3) caractérise en fait les extensions abéliennes de $\mathbb{Q}$ :*
*on peut montrer que si $K/\mathbb{Q}$ est finie galoisienne et s'il existe $D \in \mathbb{N}$ tel que $p \in S(K)$ si et seulement si $p$ mod $D$ est dans un sous-groupe de $\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^\times$, alors $K/\mathbb{Q}$ est abélienne.*

**Exemple 3**

1. *Soit $K$* ***quadratique*** *et $D = D_K$.*

$$\begin{array}{rccc} \chi_{D_K} : & \left(\frac{\mathbb{Z}}{D_K\mathbb{Z}}\right)^{\times} & \longrightarrow & G \\ & p \ mod \ D_K & \mapsto & \left(\frac{D_K}{p}\right) \end{array}$$

*Ainsi,*

$$ker\ (\chi_{D_K}) = \{p \ mod \ K \mid \left(\frac{D_K}{p}\right) = 1\}$$

*On a que ici*

$$S(K) = \{p \mid p \nmid D_K \ tel \ que \ \left(\frac{D_K}{p}\right) = 1\}$$

*Soit $K = \mathbb{Q}(\sqrt{2})$ et $D_K = 8$.*

$$\begin{array}{rccc} \chi_8 \ : & \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^{\times} & \longrightarrow & \{\pm 1\} \\ & 1 \ ou \ 7 \ mod \ 8 & \mapsto & 1 \\ & 3 \ ou \ 5 \ mod \ 8 & \mapsto & -1 \end{array}$$

$$\left(\frac{8}{p}\right) \Longleftrightarrow \left(\frac{2}{p}\right) = 2 \Longleftrightarrow p \equiv 1 \ ou \ 7 \ mod \ 8$$

*On a alors*

$$Ker\ (\chi_8) = \{1 \ mod \ 8, 7 \ mod \ 8\}$$

*et*

$$S(K) := \{p \mid p \equiv 1 \ mod \ 8 \ ou \ p \equiv 7 \ mod \ 8\}$$

2. *Soit $K = \mathbb{Q}(\zeta_n)$ et $D = n$.*

$$\begin{array}{rccc} lambda_n : & \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times} & \longrightarrow & G \\ & a \ mod \ n & \mapsto & (\zeta_n \mapsto \zeta_n^a) \end{array}$$

*Ici,*

$$Ker\ (\lambda_n) = \{1 \ mod \ n\}$$

*et*

$$S(K) := \{p \mid p \equiv 1 mod n\}$$

## 3.2 Polynômes totalement décomposés modulo un nombre premier

Soit $P$ un polynôme unitaire irréductible dans $\mathbb{Z}[X]$.
On suppose que le corps de décomposition $K$ de $P$ sur $\mathbb{Q}$ est aussi un corps de rupture (ie $[K:\mathbb{Q}] = deg\ P = n$) et que $K/\mathbb{Q}$ est abélienne.

**Définition 3**

*On note $S(p)$ l'ensemble des premiers $p$ tels que $P$ est totalement décomposé modulo $p$.*
*On dit que $P$ est totalement décomposé modulo un nombre premier $p$ si $P$ mod $p \in \mathbb{F}_p[X]$ admet $n$ racines différents dans $\mathbb{F}_p$.*
*On dit que $P$ est non ramifié modulo $p$ si $P$ mod $p \in \mathbb{F}_p[X]$ est sans facteur carré : cela équivaut à dire que $p$ ne divise pas le discriminant $D(P) \in \mathbb{Z}$ de $P$.*

**Théorème 9 (*Kummer-Dedekind*)**

*Soit $K/\mathbb{Q}$ une extension finie galoisienne. Soit $P$ irrédutible dans $\mathbb{Z}[X]$ unitaire et $\theta$ une racine de $P$ dans $K$ tel que $K = \mathbb{Q}(\theta)$.*
*Alors $\mathbb{Z}[\theta] \subset O_K$ est $\mathbb{Z}$-libre de rang $n$ et alors,*

$$D(P) = [O_K\ : \mathbb{Z}[\theta]]^2 \times D_K.$$

*Si $p \nmid [O_K : \mathbb{Z}[\theta]]$, alors on a $P$ mod $p = \bar{P}_1^e..\bar{P}_2^e$ où les $\bar{P}_i \in \mathbb{F}_p[X]$ sont irréductibles unitaires distincts de même degré $f$ et $pO_K := \mathfrak{p}_1^e...\mathfrak{p}_g^e$ où les $\mathfrak{p}_i$ sont les idéaux premiers distincts définis par $\mathfrak{p}_i = (p,\ P_i(\theta))$ (où $P_i$ relèvement de $\bar{P}_i$ dans $\mathbb{Z}[X]$), de même degré résiduel $f$.*

**Démonstration :** :
Admise ( voir [N], Théorème 4.33 ) ■

**Remarque 3**

*Pour un polynôme $P \in \mathbb{Z}[X]$ vérifiant les hypothèse précédente, le théorème 9. dit que si $p \nmid D(P)$, alors $P$ mod $p$ admet une racine dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ équivaut à $p \in S(P)$.*

**Définition 4**

*On dit que $p$ **est exeptionnel** si $p \mid [O_K : \mathbb{Z}(\theta)]$ (Cette définition est indépendante du choix de $\theta$).*

**Théorème 10**

*On a :*

$$S(K) = S(P) + \text{un nombre fini de premier exceptionnels.}$$

*De plus, si $D_K$ est admissible pour $K$ alors il existe $H$ sous groupe de $\left(\frac{\mathbb{Z}}{D(P)\mathbb{Z}}\right)^\times$ tel que $S(P) := \{p \mid p \bmod D(P) \in H\}$.*

**Démonstration :** :
La preuve s'appuie sur la version forte du théorème de Artin qui nous dit que :

$$\begin{array}{rccccc} \lambda : & \left(\frac{\mathbb{Z}}{D(P)\mathbb{Z}}\right)^\times & \twoheadrightarrow & \left(\frac{\mathbb{Z}}{D_K\mathbb{Z}}\right)^\times & \twoheadrightarrow & Gal(K/\mathbb{Q}) \\ & p \bmod D(P) & \mapsto & p \bmod D_K & \mapsto & \left(\frac{K/\mathbb{Q}}{p}\right) \end{array}$$

est un morphisme de groupes bien défini car :

$$p \wedge D(P) = 1 \Rightarrow p \wedge D_K = 1.$$

$$p \nmid D(P) \Rightarrow p \nmid D_K$$

On peut prendre $H = ker(\lambda)$.

■

**Exemple 4**

***Cas cyclotomique :***

*On a dans ce cas $P = \varphi_n$, $K = \mathbb{Q}(\zeta_n)$, $O_K = \mathbb{Z}[\zeta_n]$*

$$S(P) = S(K) = \{p \mid \ p \equiv 1 \ [n]\}$$

*Ce qui implique que l'on a pas de premier exeptionnel.*

***Cas quadratique :***

*Soit $P = X^2 - 2q^2$ où $q$ est premier différent de 1.*
*Soit*

$$K = \mathbb{Q}(\sqrt{2q^2}) = \mathbb{Q}(\sqrt{2})$$

*On a que*

$$\theta = (\sqrt{2q^2}) = q\sqrt{2}$$

*On a :*

$$\mathbb{Z}[\theta] := \mathbb{Z} \bigoplus q\mathbb{Z}\sqrt{2} \subseteq \mathbb{Z}[\sqrt{2}] = O_K$$

*et*

$$[O_K : \mathbb{Z}[\theta]] = q$$

$$D(P) = 8 \times q^2 = [O_K : \mathbb{Z}[\theta]]^2 D_K$$

*En fait $D_K = 8$ et $q$ est exeptionnel.*

$$q \in S(K) \Longleftrightarrow q \equiv 1 \text{ ou } 7 \text{ mod } 8$$

$$q \equiv 3 \text{ ou } 5 \text{ mod } 8 \Rightarrow S(K) = S(P) = \{p | p \equiv 1 ou 7 \text{ mod } 8\} \text{ car } q \notin S(K)$$

*Si $q \equiv 1$ ou $7$ mod $8$ alors $S(P) = S(K) \backslash \{q\}$.*
*On pourait envisager des cas où $S(P) = S(K)$ privé de plusieurs premiers, le principe serait le même.*

## 3.3 Densité de $S(K)$

Rappelons le résultat classique suivant :

**Théorème 11 (*Théorème de Dirichlet*)**

*Si $a,\ b \in \mathbb{Z}$ sont premiers entre eux, donc il existe une infinité de premiers congrus à $a$ modulo $b$.*

Ce théorème et le théorème de Artin entrainent que $S(K)$ et $S(P)$ sont des ensembles infinis.

On peut même aller au delà de celà et utiliser une version plus forte :

**Théorème 12 (*Théorème de Dirichlet, version forte*)**

*Supposons que $a,\ b$ sont des entiers premiers entre eux. Alors :*

$$\sharp\{p \leq x (p \text{ premier}) | p \equiv a \text{ mod } b\} \sim \frac{1}{\varphi(b)} \times \frac{x}{log\ x} \text{ lorsque } x \mapsto +\infty$$

*Ceci entraine le théorème des nombres premiers (en faisant bouger $a$) :*

$$\sharp\{p \leq x (p \text{ premier})\} \sim \frac{x}{log\ x} \text{ lorsque } x \longrightarrow +\infty$$

*Ainsi le rapport $\frac{\sharp\{p \leq x (p \text{ premier}) | p \equiv a \text{ mod } b\}}{\sharp\{p \leq x (p \text{ premier})\}}$ vers $\frac{1}{\varphi(b)}$ quand $x \to +\infty$.*

**Démonstration :** :
voir Descombes [D], chapitre 8, théorème 8.8.2 et 8.8.3. ■

**Théorème 13 (*Théorème de densité*)**

*Soit $K/\mathbb{Q}$ une extension abélienne, $D$ admissible.*

$$\frac{\sharp\{p \leq x (p \text{ premier}) | p \in S(K)\}}{\sharp\{p \leq x (p \text{ premier})\}} \to \frac{1}{[K : \mathbb{Q}]} \text{ quand } x \to +\infty$$

**Démonstration :** :
Soit $H$ le noyau de l'application $\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^\times \to G$ On a donc :

$$\frac{\sharp\{p \leq x (p \text{ premier}) | p \in S(K)\}}{\sharp\{p \leq x \ (p \text{ premier})\}} = \sum_{a \bmod D \in H} \frac{\sharp\{p \leq x | p \equiv a \bmod D}{\sharp\{p \leq x \ (p\text{premier})\}}$$

Or $\frac{\sharp\{p \leq x | p \equiv a \bmod D}{\sharp\{p \leq x \ (p\text{premier})\}} \to \frac{1}{\psi(D)}$ quand $x \to +\infty$.
Par suite

$$\frac{\sharp\{p \leq x (p \text{ premier}) | p \in S(K)\}}{\sharp\{p \leq x (p \text{ premier})\}} \to \frac{|H|}{\varphi(D)} = \frac{|H|}{\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^\times} = \frac{1}{|G|} = \frac{1}{[K : \mathbb{Q}]}$$

car $\frac{\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^\times}{H} \cong G$ ■

## 3.4 Lien avec le théorème de Kronecker-Weber

**Théorème 14**

*On suppose que la réciprocité d'Artin vraie pour des extensions abéliennes $K$, $L$, et $K.L$ de $\mathbb{Q}$. Alors :*

1. *$S(K) \subset S(L)$ à un nombre fini de premiers près $\Leftrightarrow L \subset K$.*
2. *$S(K) = S(L)$ à un nombre fini de premier près $\Leftrightarrow L = K$*

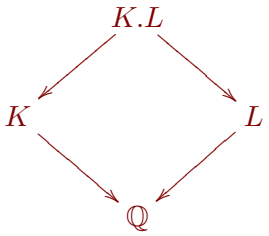
**Démonstration :** :
Il est clair que 1. $\Rightarrow$ 2. double inclusion.
Preuve du 1.

$$L \subset K \Leftrightarrow K.L = K$$

**Lemme 3**

$$S(K.L) = S(K) \cap S(L)$$

**Démonstration :** :
Comme $K$ et $L$ extensions galoisiennes de $\mathbb{Q}$ (corps de décomposition d'un polynôme de $\mathbb{Q}[X]$), on a donc que $K.L$ est une extension galoisienne de $\mathbb{Q}$.




$$\begin{array}{lcl} Gal(K.L,\mathbb{Q}) & \to & Gal(K,\ \mathbb{Q}) \times Gal(L,\ \mathbb{Q}) \\ g & \mapsto & (g|K, g|L) \end{array}$$

où $g|K$ est la restriction de $g$ à $K$ et $g|L$ est la restriction de $g$ à $L$.
Cette application est injective car $g$ est déterminé par ses restrictions à $K$ et à $L$.

On a d'abord le résultat suivant :
**Résultat 1**

*$p$ premier non ramifié dans $L$ et $K \Leftrightarrow p$ non ramifié dans $K.L$.*

**Démonstration :** :
$\Leftarrow$ clair par la mutiplicativité des indices de ramifications.
$\Rightarrow$ voir : [N], Proposition 4.25, Corollaire 1.

■

$p$ est totalement décomposé dans $K$ et $L \Rightarrow p$ est non ramifié dans $K.L$ et $\left(\frac{KL/\mathbb{Q}}{p}\right) = id$ car ses restrictions à $K$ et $L$ sont triviales ce qui implique que $p$ est totalement décomposé dans $K.L$.
On a donc que :

$$S(K) \cap S(L) \subset S(KL)$$

Réciproquement, considérons un $p$ totalement décomposé dans $K.L$ alors $p$ est totalement décomposé dans $K$ et $L$.
car

$$\begin{cases} e_K/e_{K.L} = 1 \\ f_K/f_{K.L} = 1 \end{cases}$$

De même pour $L$.
Donc $S(K.L) \subset S(K) \cap S(L)$.

■

Supposons que $S(K) \subset S(L)$ à un nombre fini de premier près : on a donc $S(K.L) = S(K)$ par le lemme 3.
Le théorème de densité des premiers totalement décomposés appliqué à $K.L$, nous donne une densité de $\frac{1}{[K.L:\ \mathbb{Q}]}$ pour $S(K.L)$.
Le théorème de densité des premiers totalement décomposés appliqué à $K$, nous donne une densité de $\frac{1}{[K:\ \mathbb{Q}]}$ pour $S(K)$.
Comme les ensembles sont les mêmes, on a égalité des densités.

Ce qui implique que $[K.L : \mathbb{Q}] = [K : \mathbb{Q}]$
Or $K \subset K.L \Rightarrow K.L = K \Rightarrow L \subset K$
Si $L \subset K$, $p$ est totalement décomposé dans $K \Rightarrow p$ est totalement décomposé dans $L$ car $e_L/e_K$ et $f_L/f_K$.
Autrement dit, $L \subset K$ entraîne que $S(K) \subset S(L)$.

■

**Conséquence 1**

*Soit $K/\mathbb{Q}$ finie abélienne et $D$ admissible pour $K$.*
*La réciprocité de Artin entraîne que $S(K)$ contient les premiers congrus à 1 modulo $D$, d'où $S(K) \supset S(\mathbb{Q}(e^{\frac{2i\Pi}{D}}))$.*
*Le théorème 2. implique que $K \subset \mathbb{Q}(e^{\frac{2i\Pi}{D}})$.*

Ainsi le théorème de Artin entraine le théorème de Kronecker-Weber :

**Théorème 15 (*Théorème de Kronecker-Weber*)**

*Toute extension abélienne de $\mathbb{Q}$ est contenue dans une extension cyclotomique $\mathbb{Q}$.*

**Exemple 5 (*Etude du cas quadratique à la main*)**

*On peut vérifier que dans le cas d'un corps quadratique, on a bien le théorème de Kronecker-Weber sans utiliser la réciprocité de Artin :*
*Soit $p$ un nombre premier avec $p \geq 3$. On pose $p^* = (-1)^{\frac{p-1}{2}} p$.*
*On a que $\sqrt{p^*} \in \mathbb{Q}(e^{\frac{2i\Pi}{p}})$ car $\left(\sum_{1 \leq a \leq p-1} \left(\frac{a}{p}\right) e^{\frac{2i\Pi}{p}a}\right)^2 = p^*$ (calcul identique à celui dans la preuve de la réciprocité quadratique).*
*Donc*

$$\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(e^{\frac{2i\Pi}{p}})$$

*Or $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(e^{\frac{2i\Pi}{8}})$.*
*On en déduit alors facilement que pour $p$ nombre premier $\mathbb{Q}(\sqrt{p})$ et $\mathbb{Q}(\sqrt{-1})$ sont inclus dans une extension cyclotomique de $\mathbb{Q}$, puis que c'est vrai pour $\mathbb{Q}(\sqrt{d})$.*
*On peut même montrer que $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(e^{\frac{2i\Pi}{|D_K|}})$.*

# 4 La réciprocités de Artin pour les extensions admissibles de $\mathbb{Q}$

## 4.1 Rappels sur les corps cyclotomiques

**Théorème 16 (*admis*)**

*Soit $n \geq 1$ un entier et $\zeta_n = e^{\frac{2i\pi}{n}} \in \mathbb{C}$, $K_n = \mathbb{Q}(\zeta_n) \subset \mathbb{D}$.*

- *$K_n \cap K_m = K_{pgcd(m,n)}$ et $K_n K_m = K_{ppcmm,n}$ pour $m, n \geq 1$.*
- *$O_{K_n} = \mathbb{Z}[\zeta_n]$.*
- *Discriminant de $K_n$ vaut*
$$(-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p \mid n} p^{\frac{\varphi(n)}{p-1}}}$$
*où $\phi$ est l'indicatrice d'euler.*
- *$p$ est ramifié dans $K_n \Leftrightarrow p \mid n$ sauf si $n \equiv 2 \ mod \ 4$ ($K_n = K_{\frac{n}{2}}$ dans ce cas).*
- *$p$ totalement décomposé dans $K \Leftrightarrow p \equiv 1 \ (n)$.*
- $$\begin{array}{ccccc} \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times} & & \to & & Gal\left(K_n/\mathbb{Q}\right) \\ a \pmod n & & \mapsto & \varphi_a : & \zeta_n \mapsto \zeta_n^a \end{array}$$
*est un isomorphisme*

**Démonstration :** :
Voir [N] théorème 4.27 ■

## 4.2 Extensions admissibles de $\mathbb{Q}$

**Définition 5**

*Une extension $K$ de $\mathbb{Q}$ contenue dans $\mathbb{C}$ est dite **admissible** s'il existe un $n \geq 1$ tel que $K \subset K_n = \mathbb{Q}(\zeta_n)$.*
*Le plus petit entier $n \geq 1$ tel que $K \subset k_n$ est alors appelé le **conducteur** de $K$, noté $\delta_K$.*
*Notons **$\mathcal{A}$ l'ensemble des extensions admissibles de $\mathbb{Q}$ contenues dans $\mathbb{C}$.***
*$\mathcal{A}$ est stable par intersection et compositum.*

**Proposition 6 (*Propriétés du conducteur*)**

*Soit $K/\mathbb{Q}$ et $L/\mathbb{Q}$ admissibles.*

1. *Si $K \subset K_n$ alors $\delta_K \mid n$.*
2. *$\delta_{K\cap L} | pgcd\,(\delta_K,\ \delta_L)$ et $\delta_{K.L} = ppcm\,(\delta_K, \delta_L)$.*
3. *Un nombre premier $p$ est ramifié dans $k \Leftrightarrow p|\delta_K$.*

**Démonstration :** :
1. et 2. découle facilemenent du théorème 16.
Prouvons le 3.
**Rappel** :
Considérons $K_n = \mathbb{Q}(e^{\frac{2i\Pi}{n}})$
Le conducteur de $K_n$ varie suivant $n$.

On a $p$ ramifié dans $K_n \Leftrightarrow \begin{cases} p \mid n & si\ n \neq 2\ mod\ 4 \\ & (\text{ Dans ce cas, n est le conducteur de} K_n) \\ p \mid \frac{n}{2} & si\ n \equiv 2\ mod 4 \\ & (\text{ Dans ce cas,} K_n = K_{\frac{n}{2}} \text{et le conducteur de} K_n \text{est égal à} \frac{n}{2}) \end{cases}$

$$\begin{array}{c} K_{\delta_K} = \mathbb{Q}(e^{\frac{2i\Pi}{\delta_K}}) \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$$

Le conducteur de $K_{\delta_K}$ est $\delta_K$ par définition du conducteur de $K$.
$\Rightarrow$ Supposons que $p$ est ramifié dans $K$.
On a donc que $p$ est ramifié dans $K_{\delta_K}$. Ce qui implique que $p \mid \delta_K$ (théorème 16).
$\Leftarrow$ Supposons que $p$ est tel que $p \mid \delta_K$ : $\delta_K = p^a m$ avec $m$ premier à $p$, $a \geq 1$ et si $p = 2$ alors $a \geq 2$ ($\delta_K \neq 2\ mod\ 4$).
Supposons $p$ non ramifié dans $K_m$ : on a donc que $p$ est non ramifié dans $K.K_m$.

$$\begin{array}{ccccccc} \mathbb{Q} & \subset & K & \subset & K.K_m & \subset & K_{\delta_K} \\ & & & & & & \cup \\ & & & & & & K_{p^a} \end{array}$$

$\mathbb{Q} \subset K_{p^a}$. On cherche l'indice de ramification en $p$.
Il est en fait égal à $\phi(p^a)$.

$$p\ O_{K_{p^a}} = \mathfrak{p}_1^e ... \mathfrak{p}_g^e$$

En fait, ici

$$p\ O_{K_{p^a}} = \mathfrak{p}^{\phi(p^a)}$$

où

$$\mathfrak{p} = (p,\ e^{\frac{2i\Pi}{p^a}} - 1) = (e^{\frac{2i\Pi}{p^a}} - 1)$$

On peut appliquer ici le théorème de Dédekind à $K_{p^a}$ avec $\Phi_{p^a}$.
L'anneau des entiers de $K_{p^a}$ est $\mathbb{Z}[e^{\frac{2i\Pi}{p^a}}]$ ( ceci implique que il n'y a pas de premier exeptionnel dans ce cas).

$$p\ O_{K_{p^a}} = \mathfrak{p}_1^e ... \mathfrak{p}_g^e \ et\ \Phi_{p^a}\ mod\ p = (f_1\ mod\ p)^e ... (f_g\ mod\ p)^e$$

où $f_i \in \mathbb{Z}[X]$ unitaire tel que $f_i\ mod\ p$ irréductibles distincts dans $\mathbb{F}_p[X]$ et $\mathfrak{p}_i = (p,\ f_i(e^{\frac{2i\Pi}{p}}))$
On a

$$\Phi_{p^a} = X^{p^{a-1}(p-1)} + .... + X^{p^a} + 1 = \Phi_p(X^{p^{a-1}})$$

Si on regarde $\Phi_{p^a}$ modulo $p$, on a par le petit théorème de Fermat :

$$\Phi_{p^a}\ mod\ p \equiv (\Phi_p\ mod\ p)^{p^{a-1}}$$

$$\Phi_p\ mod\ p = (X-1)^{p-1}\ dans\ \mathbb{F}_p[X]$$

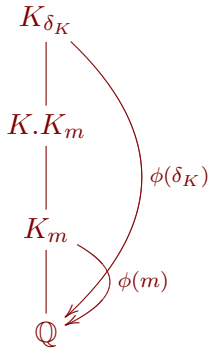
car

$$X^p - 1 = (X-1)\Phi_p dans\ \mathbb{Z}[X] et\ modulo\ p,\ X^p - 1 = (X-1)^p.$$

Donc $\Phi_{p^a}\ mod\ p = (X-1)^{\phi(p^a)}$ dans $\mathbb{F}_p[X]$
On a donc $e = \varphi(p^a)$ et $g = 1$.
De plus, $\mathfrak{p}_1 = (p,\ e^{\frac{2i\Pi}{p^a}} - 1) = (e^{\frac{2i\Pi}{p^a}} - 1)$
car

$$p = \Phi_{p^a}(1) = \prod_{1 \leq k \leq p^a p \nmid k} (1 - e^{\frac{2i\Pi}{p^a}}) = (1 - e^{\frac{2i\Pi}{p}}) \prod_{1 \leq k \leq p^a p \nmid k k \neq 1} (1 - e^{\frac{2i\Pi \times k}{p^a}})$$

Donc $(e^{\frac{2i\Pi}{p^a}} - 1) \mid p$ dans $\mathbb{Z}[e^{\frac{2i\Pi}{p^a}}]$
On en déduit que $\varphi(p^a)$ divise l'indice de ramification de $p$ dans $K_{\delta_K}$




Si $\mathfrak{p}$ est un idéal premier au dessus de $p$ dans $K.K_m$ alors l'indice de ramification de $\mathfrak{p}$ dans $K_{\delta_K}$ est l'indice de ramification de $p$ dans $K_{\delta_K}$ car $p$ non ramifié dans $K.K_m$.
On a : $\varphi(p^a) \leq [K_{\delta_K} :\ K.K_m] = \frac{[K_{\delta_K} :\ K_m]}{[K.K_m :\ K_m]} = \frac{\frac{\varphi(\delta)}{\varphi(m)}}{[K.K_m :\ K_m]} = \frac{\varphi(p^a)}{[K.K_m :\ K_m]}$
Donc $[K.K_m :\ K_m] = 1 \Rightarrow K.K_m = K_m \Rightarrow K \subset K_m$.
On aboutit à une contradiction de la définition de $\delta_K$.
Donc $p$ est ramifié dans $K$.
C'est ce qu'il fallait démontrer.

■

**Exemple 6**

*Soit $p$ nombre premier, avec $p \geq 3$, et $K = \mathbb{Q}(\sqrt{p^*})$*
*Donc $K \subset K_p$.*
*$\delta_K \mid p \Rightarrow \delta_K = 1$ ou $p$*
*donc $\delta_K = p$ car $\sqrt{p*} \notin \mathbb{Q}$.*

$\mathbb{Q}(\sqrt{p})$
*Si $p^* = p$ et $p \equiv 1 \ mod\ 4 \Rightarrow \delta_K = p$*
*Si $p^* = -p$ et $p \equiv 3 \ mod\ 4$*
$K = \mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(i,\ \sqrt{p^*}) \subset \mathbb{Q}(i, e^{\frac{2i\Pi}{p}}) \subset K_{4p}$
$\delta_K \mid 4p$
$D_K = 4p$, $\delta_K \mid 4p \Rightarrow \delta_K = 2p$ ou $4p$
$K_{2p} = K_p$ car $K_2 = \mathbb{Q}$, doù $K_2 K_p = K_{2p} = K_p$.
$\Rightarrow \delta_K \neq 2p$ car $p$ est plus petit que $2p$.
donc $\delta_K = 4p = D_K$.
$\delta_{\mathbb{Q}(i)} = 4$ et $\delta_{\mathbb{Q}(\sqrt{2})} = 8$
*On peut montrer, plus généralement, que si $K$ est quadratique sur $\mathbb{Q}$, alors $\delta_K = |D_K|$ (le raisonnement de la fin de la partie 3, montre que $\delta_K / D_K$).*

$K = K_n$ : $\delta_K = \begin{cases} n & si\ n \neq 2 \ mod\ 4 \\ \frac{n}{2} & si\ n \equiv 2 \ mod\ 4 \end{cases}$
*Considérons $n = p^\alpha$, $p \geq 3$ et $m = p^\beta$, $\beta \leq \alpha$ et $\phi(p^\beta) = \phi(p^\alpha) \Rightarrow \alpha = \beta$*
*Si $p = 2$, $\varphi(2^\beta) = \varphi(2^\alpha) \Rightarrow \begin{cases} \alpha = \beta ou \\ \alpha = 1 \ et\ \beta = 0. \end{cases}$*
*Ceci implique la formule pour $\delta_K$, si $n = p^\alpha$ avec $p$ premier.*
*Dans le cas général : $K_n = K_{p_1^{\alpha_1}} ... K_{p_r}^{\alpha_r}$ où $n = p_1^{\alpha_1} ... p_r^{\alpha_r}$ (théorème 16), puis on utilise le fait que $\delta_K = ppcm(\delta_{K_{p_i^{\alpha_i}}}) = \prod \delta_{K_{p_i^{\alpha_i}}} = n$ ou $\frac{n}{2}$.*
*On voit dans cet exemple que $\delta_K / D_K$ si $K = K_n$, en utilisant la formule sur le discriminant de $K_n$.*
*C'est vrai pour $K$ admissible quelconque (pas évident).*
*Le lecteur intéressé par une preuve pourra se référer à [N], Proposition 8.7.*

## 4.3 Théorie du corps des classes pour les extensions admissibles de $\mathbb{Q}$

**But :**
*Soit $K/\mathbb{Q}$ est une extension admissible contenue dans $\mathbb{C}$*
*Décrire l'arithmétique de $K$ à l'aide de notions venant de $\mathbb{Z}$ en l'occurence des congruences modulo des nombres premiers.*
*La théorie du corps de classes pour les extensions admissibles de $\mathbb{Q}$ (en fait abéliennes de $\mathbb{Q}$ par Kronecher-Weber) constitue le résultat suivant :*

**Théorème 17**

*Soit $K$ une extension admissible de $\mathbb{Q}$ contenue dans $\mathbb{C}$ et $D$ un entier $\geq 1$ tel que $\mathbb{Q}\left(e^{\frac{2i\pi}{D}}\right) \supset K$.*
*L'entier $D$ est donc divisible par les premiers ramifiés dans $K$ et exactement par eux si on prend pour $D$ le conducteur de $K$.*

1. *Réciprocité d'Artin :*
   *$D$ est admissible pour $K$ et l'application d'Artin $I_D \to Gal\,(K/Q)$ induit donc un morphisme surjectif de $\Phi_D : \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times} \to Gal\,(K/\mathbb{Q})$ envoyant $p$ mod $D$ sur $\left(\frac{K/\mathbb{Q}}{p}\right)$ pour $p \nmid D$.*
2. *Loi de décomposition des premiers non ramifiés dans $K$.*
   *Soit $p \in \mathbb{P}$ premier avec $D$ et notons $\Gamma_D(K) = Ker\Phi_D$.*
   *$pO_K = \mathfrak{p}_1..\mathfrak{p}_g$ avec $\mathfrak{p}_i$ des idéaux premiers différents de $O_K$.*
   *Soit $f$ le degré résiduel commun des $\mathfrak{p}_i$.*
   *Alors*
   $$\begin{cases} f = + \text{ petit entier } k \geq 1 \text{ tel que } p^k \bmod D \in \Gamma_D(K) \\ g = \frac{[K:\,\mathbb{Q}]}{f} \end{cases}$$
   *En particulier, $p$ premier totalement dcompos dans $K \Leftrightarrow p$ mod $D \in \Gamma_D(K)$ et pour $D =$ conducteur $\delta_K$ : $p \in S(K) \Leftrightarrow p$ mod $\delta_K \in \Gamma_{\delta_K}(K)$.*
3. *Théorème d'existence :*
   *Soit $D \geq 1$ entier quelquonque $H$ sous groupe de $\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times}$, il existe une unique extension admissible de $K$ contenue dans $\mathbb{C}$ telle que $D$ est admissible pour $K$ (en fait $K \subset K_D$) et $\Gamma_D(K) = H$.*

**Démonstration :** :
1.

$$\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times} \overset{\Lambda_D}{\rightsquigarrow} Gal(K_D,\ \mathbb{Q})$$
$$\left(\frac{K_D/\mathbb{Q}}{\cdot}\right)$$
$$I_D$$

où $\Lambda_D$ est un isomorphisme et $\chi$ est l'application de Artin pour $K_D$ est surjective, de noyau $R_D$.
Soit

$$\begin{array}{ccccc} I_D & & & & \\ \downarrow & \searrow & & & \\ \frac{I_D}{R_D} & & & & \\ \wr & & & & \\ \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times} & \rightsquigarrow & Gal(K_D/\mathbb{Q}) & \longrightarrow\!\!\!\!\rightarrow & Gal(K/\mathbb{Q}) \end{array}$$

défini par :

$$\begin{array}{ccccc} p & & & & \\ \downarrow & \searrow & & & \\ p\ R_D & & & & \\ \wr & & & & \\ p\ mod\ D & \longrightarrow & \left(\frac{K_D/\mathbb{Q}}{p}\right) & \longrightarrow\!\!\!\!\rightarrow & \left(\frac{K/\mathbb{Q}}{p}\right) \end{array}$$

$$\begin{array}{lcl} Gal(K_D/\mathbb{Q}) & \to & Gal(K/\mathbb{Q}) \\ g & \mapsto & g|K(restriction\ g\ à\ K) \end{array}$$

$K \in K_D$
L'application $\Phi_D$ : $\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times} \twoheadrightarrow Gal(K_D/\mathbb{Q}) \twoheadrightarrow Gal(K/\mathbb{Q})$ est surjective mais pas injective.
Le noyau de cette application $\Phi_D$ est le sous-groupe de $\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times}$ qui correspond à $Gal(K_D, K)$ par l'isomorphisme $\Lambda_D$ et $R_D \subset \tilde{H} := ker(I_D \to Gal(K/\mathbb{Q})$.

$$\frac{\tilde{H}}{R_D} \cong ker\left[\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times} \to Gal(K/\mathbb{Q}]$$

L'application d'Artin pour $K$ et $D$ : $I_D \to Gal(K/\mathbb{Q})$ est surjective comme composée de surjections et le noyau contient $R_D$.
Donc, $D$ est edmissible pour $K$.

2. $f$ = ordre de $\left(\frac{K/\mathbb{Q}}{p}\right)$ dans $Gal(K/\mathbb{Q}) \Leftrightarrow f$ = ordre de la classe de $p\ mod\ D$ dans $\frac{\left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)}{\Gamma_D(K)} \cong Gal(K/\mathbb{Q})$. L'isomorphisme découle de 1.

Preuve du 3.

$$D \to K_D$$

Ecrire Artin pour $K_D$.

$$\begin{array}{lll} \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^\times & \rightsquigarrow^{\Lambda_D} & Gal(K/\mathbb{Q}) \\ \cup & & \\ H & \rightsquigarrow & H' \text{ sous groupe de } Gal(K_D/\mathbb{Q}) \end{array}$$

Posons $K := K_D^{H'}$ : on a $Gal(K_D/K) = H' \cong_{\Lambda_D} H$.
par la preuve du 1., ce corps convient : $K \subset K_D \Rightarrow D$ admissible pour $K$ et on a $\Gamma_D(K) = H$.
Unicité de K :
On a $S(K) = \{p \text{ premier}/p \text{ mod } D \in H\}$ à un nombre fini de premiers près.
Or le théorème 14. est vraie pour les extensions admissible de $\mathbb{Q}$ car $\mathcal{A}$ est stable par compositum et la réciprocité d'Artin est vraie pour les extensions admissible de $\mathbb{Q}$.

■

**Remarque 4**

*Le conducteur de $K$ est le pgcd des entiers $D \geq 1$ qui sont admissibles pour $K$.*

**Conséquence 2**

*Le théorème de Kronecker-Weber implique la réciprocité d'Artin.*
*Ces deux théorème sont donc équivalent.*

Pour une preuve du théorème de Kronecker-Weber (n'utilisant pas la réciprocité d'Artin), on pourra consulter [N], théorème 6.18.

# 5 Un exemple : étude des sous corps de $K_7 = \mathbb{Q}(e^{\frac{2i\Pi}{7}})$

On notera dans la suite $\zeta_7 := e^{\frac{2i\Pi}{7}}$.

$$\begin{array}{rccc} \Lambda_7 : & \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times \cong \frac{\mathbb{Z}}{6\mathbb{Z}} & \rightsquigarrow & Gal(K_7/\mathbb{Q}) \\ & a \ mod \ 7 & \mapsto & (\zeta \mapsto \zeta^a) = \Phi_a \end{array}$$

On a que $\frac{\mathbb{Z}}{6\mathbb{Z}}$ a exactement 4 sous-groupes cycliques d'ordre 1, 2, 3, 6) qui induisent, par la théorie de Galois, les 4 sous extensions $K$ de $K_7/\mathbb{Q}$ de degré sur $\mathbb{Q}$ : 6, 3, 2, 1.

Si $[K : \mathbb{Q}] = 1$ alors $K = \mathbb{Q}$ (rien à faire).
Si $[K : \mathbb{Q}] = 6$ alors $K = K_7$ (déjà étudier, cas cyclotomique).
Si $[K : \mathbb{Q}] = 3$ alors $K = \mathbb{Q}(cos\ \frac{2\Pi}{7})$ (déjà étudier, cas cyclotomique).
On pose $\alpha := 2cos\ \frac{2\Pi}{7} = \zeta_7 + \zeta_7^{-1}$ On a alors que le polynôme minimal de $\alpha$ sur $\mathbb{Q}$ est :

$$\mu_{\alpha,\mathbb{Q}} = X^3 + X^2 - 2X - 1 = P$$

Les autres racines de $P$ sont les images de $\alpha$ par les différents automorphismes de $K_7$. On a ainsi que les deux autres racines sont :

$$\left\{ \begin{array}{rcl} \zeta_7^2 + \zeta_7^{-2} & = & \alpha^2 - 2 \\ \zeta_7^3 + \zeta_7^{-3} & = & \alpha^3 - 3\alpha \end{array} \right.$$

On a que :

$$D(P) = [O_K : \ \mathbb{Z}[\alpha]]^2 D_K = D(P) = 49 = D_K \Rightarrow O_K = \mathbb{Z}[\alpha]$$

(en effet, les $D_K$ ne peut être égal à un car sinon on aurait $K = \mathbb{Q}$) Donc il n'y a pas de premier exceptionnel par $P$.
i.e. $S(K) = S(P)$.
Pour $p \neq 7$ : $p$ non ramifié dans $K$.
On a :

$$\left(\frac{K/\mathbb{Q}}{p}\right) = \ restriction\ à K\ de\ \left(\frac{K_7/\mathbb{Q}}{p}\right) = \ restriction\ de\ \varphi_p\ à\ K.$$

On a que $\alpha$ engendre $K/\mathbb{Q}$ donc $\left(\frac{K/\mathbb{Q}}{p}\right)$ est déterminé par sa valeur en $\alpha$ donc par $\Phi_p(\alpha)$

$$\left\{ \begin{array}{lll} p \equiv \pm 1 \ mod \ 7 \ : & \Phi(\alpha) = \alpha : & \left(\frac{K/\mathbb{Q}}{p}\right) = id \\ p \equiv \pm 2 \ mod \ 7 \ : & \Phi(\alpha) = \alpha^2 - 2 : & \left(\frac{K/\mathbb{Q}}{p}\right) = \sigma \\ p \equiv \pm 3 \ mod \ 7 \ : & \Phi(\alpha) = \alpha^3 - 3\alpha : & \left(\frac{K/\mathbb{Q}}{p}\right) = \sigma^2 \end{array} \right.$$

Avec $Gal(K/\mathbb{Q}) =< \sigma > \cong \frac{\mathbb{Z}}{3\mathbb{Z}}$ où $\sigma \ : \ \alpha \mapsto \alpha^2 - 2$ et $\sigma^2 \ : \ \alpha \mapsto \alpha^3 - 3\alpha$.
On retrouve la surjectivité de l'application $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times \to Gal(K/\mathbb{Q})$ induite par la réciprocité d'Artin. Le noyau de cette application est : $\{\pm 1 \ mod \ 7\}$.
On a :

$$S(K) = \{p \ premier / \ p \equiv \pm 1 \ mod \ 7\} = S(P)$$

De plus,

$$\{p \text{ premier } / \ P \text{ mod } p \text{ admet une racine dans } \frac{\mathbb{Z}}{p\mathbb{Z}}\} := \{7\} \cup S(P).$$

Si $p = 7$ alors par Dedekind, comme dans ce cas là p est non exceptionnel, on a 2 *mod* 7 est une racine triple du polynôme.
Si $[K : \mathbb{Q}] = 2$ alors $K = \mathbb{Q}(\sqrt{7^*}) = \mathbb{Q}(\sqrt{-7}) \subset K_7$.
On a $D_K = -7$. Pour $p \neq 7$, on a :

$$(\frac{K/\mathbb{Q}}{p}) = (\frac{-7}{p}) \text{ } et \text{ } \varphi_p(\sqrt{-7}) = (\frac{-7}{p})\sqrt{-7}.$$

On cherche à exprimer $\sqrt{-7}$ en fonction de $\zeta_7$.
On a a nouveau à l'aide des sommes de Gauss :

$$\sqrt{-7} = \pm \sum_{1 \leq a \leq 6} (\frac{a}{p}) e^{\frac{2i\Pi}{7}}$$

Posons $S = \sum_{1 \leq a \leq 6} \left(\frac{a}{p}\right) e^{\frac{2i\Pi}{7}}$.
On a : $\varphi_p(S) = \sum_a \left(\frac{a}{7}\right) \zeta_7^{ap} = \left(\frac{p}{7}\right) S$ et $\phi_p(S) = \left(\frac{-7}{p}\right) S$.

$$Donc \ (\frac{p}{7}) = (\frac{7^*}{p}) = (\frac{-7}{p}) \ :$$

c'est le cas particulier de la réciprocité quadratique. Et $\varphi_p = \left(\frac{p}{7}\right)$ :

$$\varphi_p = 1 \ ssi \ p \equiv 1, \ 4, \ 6 \ mod \ 7.$$

# Conclusion

La loi de réciprocité quadratique comme nous l'avons vu peut prendre différentes formes toutes aussi intéressantes et pleines d'intéret.
Nous avons pu voir comment à partir d'une loi de réciprocité pour résoudre le problème d'existence de carré modulo un nombre premier, c'est à dire le problème de résolution d'équation du type $X^2 - a = 0$ dans $\mathbb{F}_p$, on pouvait s'interressait à un polynôme plus général et établir s'il avait des racines ou même mieux s'il était totalement décomposé. Sans oublier que l'on a pu montrer que la réciprocité d'Artin i.e. la traduction en termes de morphisme de la loi de réciprocité de départ étendu à des extension abélienne était équivalente au théorème de Kronecker-Weber qui, je rappelle, dit que toute extension abélienne de $\mathbb{Q}$ est inclue dans une extension cyclotomique.
Nous avons ici trois aspect de la loi de réciprocité quadratique :
– la recherche des carrés modulo un premier.
– la donnée d'un morphisme en lien avec la décomposition des idéaux et des polynômes.
– le théorème de Kronecker-Weber.

# Bibliographie

[$Sa$] Pierre Samuel, La théorie algébrique des nombres (Hermann, 1971)

[$Se$] Serre Cours d'arithmétique (Mann)

[$N$] Narkiewicz "Elementary and analytic theory of algebraic numbers" (Springer Monographs in mathematics).

[$LS$] H.W Lenstra J.A et P. Stevenhagen, Artin reciprocity and Mersenne primes(article)

[$W$] B.F Wynam, What is a reciprocity law ? (Stanford university, article, 1972)

[$D$] Descombes, Eléments de théories des nombres (PUF)