الجمهوريـــة الجزائـــريـــة الديمقراطيـــة الشعبيـــة
République Algérienne Démocratique et Populaire
وزارة التعليـــــم العالـــي والبحـــث العلمـــي
Ministère de lôEnseignement Supérieur et de la Recherche Scientifique

N° Ref :é é é é é

Centre Universitaire de Mila

Institut des sciences et de la technologie **Département de Mathématiques et Informatique**

La loi de réciprocité quadratique

Mémoire préparé en vue de lôobtention du diplôme de licence en Mathématiques

Préparé par : Bouguebina Saliha
Guessoum Imen

Encadré par : Bouguebina Mounir

Filière : **Mathématique**

Année universitaire : 2012 /2013

La loi de réciprocité quadratique

Bouguebina Saliha et Guessoum Imen

Table des matières

Remerciements

Avant tout nous tenons à remercier ALLAH pour nous avoir aidé à acomplir ce travail.

Nous tenons aussi à remercier notre encadreur, Mounir Bouguebina, pour ces conseils, ainsi que tout les enseignants du département de Mathématiques et Informatique.

Enfin nous remercions vivement nos parents et tous les membres de nos familles respectives.

Introduction

La loi de réciprocité quadratique peut être considérée comme un joyau de l'Arithmétique. La simplicité et l'élégance de son énoncé n'ont d'égales que la difficulté et la profondeur de sa démonstration. Mêmes les preuves dites élémentaires de cette loi demeurent plus ou moins compliquées et ceci la rend encore plus attrayante. On peut la voir comme un théorème concernat les congruences de Gauss puisqu'elle s'occupe de donner les conditions de résolubilité de certaines équations quadratiques modulo des nombres premiers et comme son nom l'indique, il y a une certaine réciprocité entre les solutions concernant deux nombres premiers p et q distincts : déterminer le problème concernant l'un permet de résoudre le problème concernat l'autre et vice versa. Conjecturée par Euler et enfin démontrée par Gauss, elle n'a cessé d'occuper l'esprit des plus brillants mathématiciens. Son importance (pour elle-même et pour ses généralisations) a été encore plus accentuée dans les années 1970, quand Tate et d'autres ont découvetrt une relation mystérieuse entre cette loi et une théorie mathématique encore naissante à l'époque : La K-théorie algébrique.

Dans ce mémoire, nous allons essayer de donner un enoncé et une preuve aussi élémentaires que possible de la loi de réciprocité quadratique et on touchera à peine au lien avec la K-théorie qui reste un peu difficle. Il est organisé de la manière suivante : le premier chapitre est un résumé de quelques notions d'Arithmétique indispensables pour la compréhension des chapitres suivants. On y définit notamment ce qu'est une racine primitive de l'unité modulo un nombre premier. Le second chapitre constitue le coeur de ce travail et c'est ici qu'on donne une formulation de la loi en utilisant les symboles de Legendre ainsi que des exemples de son application pour enfin la démontrer à la fin du chapitre. Dans le troisième et dernier chapitre, on explique comment la K-thórie permet de reinterpréter la loi de réciprocité en utilisant certains symboles et le K_2 d'un corps (qui sera ici $\mathbb{Q}$).

Chapitre 1

Arithmétique élémentaire

Dans ce premièr chapitre, on présente quelques notions d'Arithmétique qui nous serviront par la suite. Dans la première section, on commence par rappeler la theorie de la divisibilité qui est à la base de la définition des nombres premiers et du plus grand commun diviseur de deux entiers. On énonce également ici le lemme de Gauss ainsi que le théorème fondamental de l'Arithmétique. Les congruences de Gauss sont abordées dans la seconde section dans laquelle, outre les définitions principales, on présente en particulier l'étude de l'équation linéaire $ax = b$ modulo n et le petit théorème de Fermat. Le contenu de la troisième section est trés important pour l'étude de la loi de réciprocité. On y définit les racines primitives de l'unité modulo un nombre premier p et on montre l'existence de telles racines.

1.1 Divisibilité

Soient a, b deux éléments de $\mathbb{Z}$. On dit que a est divisible 'par b ou encore que a est un multiple de b ou encore que b divise a s'il existe un élément $c \in \mathbb{Z}$ tel que :

$$a = bc.$$

Remarquer que si $a \neq 0$ et si b divise a, alors $b \neq 0$ et c est unique. c est appelé le quotient de a par b

Exemple : 2 divise 12 ; -5 divise 15 ; 6 ne divise pas 29.

La division euclidienne dans $\mathbb{Z}$ est à la base de la notion de congruence qu'on verra un peu plus loin. Depuis Euclide, on sait que si a un entier et si b un entier non nul, alors il existe un unique entier q et un unique entier r

tels que :

$$a = qb + r$$

avec

$$0 \leq r <\mid b \mid$$

q est le quotient de la division de a par b et r est son reste.

Nous allons étudier les diviseurs d'un ou plusieurs entiers. Comme les diviseurs de a sont les mêmes que ceux de $-a$ et que si d est un diviseur de a, il en est de même de $-d$, on peut restreindre dans un premier temps l'étude à $\mathbb{N}$. Elle s'étendra naturellement à $\mathbb{Z}$.

Soient a, b deux nombres entiers. Le plus grand commun diviseur de a et b est le plus grand entier non nul qui les divise tous les deux. On le note $pgcd(a, b)$.

On a donc :

$$pgcd(a, b) = max\{d : d \mid a \wedge d \mid b\}$$

Par convention $pgcd(0, 0) = 0$.

Definition 1 *: Les nombres entiers a, b sont dits premiers entre eux si $pgcd(a, b) = 1$.*

Par exemple $a = 325$ et $b = 145$ sont premiers entre eux. L'algorithme d'Euclide étendu permet de préciser la relation entre deux entiers a et b et leur plus grand commun diviseur d : Il existe deux entiers u et v tels que $au + bv = d$. En particulier si a et b sont premiers entre eux, les deux entiers u et v vérifient $au + bv = 1$. Nous allons l'utiliser pour montrer le résultat suivant appelé lemme de Gauss :

Proposition 1 *(lemme de Gauss) : Si c divise ab et si c est premier avec b, alors il divise a.*

Preuve : Si c est premier avec b, on peut trouver u, v tels que $cu + bv = 1$. On aura alors $acu + abv = a$. Mais acu est divisible par c ainsi que abv. Donc a est divisible par c.

Definition 2 *: Un nombre entier $p > 1$ est dit premier si les seuls diviseurs de p sont 1 et p lui-même. Autrement dit :*

$$a \mid p \Longrightarrow a = 1 \vee a = p.$$

Par exemple 2, 5 et 7 sont des nombres premiers, mais 10, 12 et 15 ne le sont pas. On dit que ce sont des nombres composés. Remarquer que si un nombre premier p divise un produit ab, il doit diviser l'un des facteurs a ou b. En effet supposons que p ne divise pas a. Il est alors premier avec a et d'aprés le lemme de Gauss, il divise b.

Si un nombre entier n'est pas premier on peut montrer qu'il est toujours produit de nombres premiers :

Théorème 1 *(théorème fondamental de l'arithmétique) : Tout nombre entier positif s'écrit comme un produit de nombres premiers et ce de manière unique à l'ordre des facteurs prés.*

Preuve : Soit n un entier positif. Pour montrer la première partie du théorème utilisons une récurrence sur n. Si n est premier, on a fini. Sinon on a $n = ab$ avec $a, b < n$. Par hypothèse de récurrence a et b sont produits de nombres premiers et donc n aussi. Passons à l'unicité. Supposons qu'on ait deux factorisations :

$$n = p_1.p_2 \dots p_m$$

et

$$n = q_1.q_2 \dots q_l,$$

avec les p_i et les q_i des nombres premiers. Comme p_1 divise $n = q_1.(q_2 \dots q_l)$, on doit avoir $p_1 = q_1$ ou $p_1 \mid q_2 \dots q_m$. Par induction on a $p_1 = q_i$ pour un certain i. En simplifiant par p_1 et q_i et en répetant l'argument précédent pour les nombres premiers qui restent, on arrive au resultat.

Exemple : On a :

$$666 = 2.3^2.37.$$

$$2001 = 3.23.29.$$

$$12 = 22.3.$$

On peut montrer qu'il y a une infinité de nombres premiers. En effet supposons que non et soient $p_1 = 2, p_2 = 3, \dots, p_n$ tous les nombres premiers et posons :

$$N = 2.3.5 \dots p_n + 1.$$

Alors N est un entier qui n'est divisible par aucun nombre premier, ce qui contredit le théorème fondamental de l'arithmétique.

1.2 Congruences

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$. On dit que a est congru à b modulo n si n divise $a - b$. Autrement dit il existe $k \in \mathbb{Z}$ tel que :

$$a - b = nk.$$

On note $a \equiv b \pmod{n}$. On vérifie facilement que la relation de congruence est une relation d'équivalence sur $\mathbb{Z}$ (elle est reflexive, symétrique et transitive). La classe d'équivalence de a sera notée $\overline{a}$:

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

L'ensemble quotient est :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{a}, a \in \mathbb{Z}\}.$$

On l'appelle l'ensemble des congruences modulo n.
Exemple : Pour $n = 3$, on obtient :

$$\overline{0} = \{\ldots, -3, 0, 3, \ldots\},$$

$$\overline{1} = \{\ldots, -2, 1, 4, \ldots\},$$

$$\overline{2} = \{\ldots, -1, 2, 5, \ldots\},$$

et

$$\frac{\mathbb{Z}}{3\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}\}.$$

De manière générale l'ensemble des congruences modulo n contient exactement n éléments :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, on a (vérification facile) :

$$a + b \equiv a' + b' \pmod{n},$$

et

$$ab \equiv a'b' \pmod{n}.$$

Ceci nous permet de définir une addition et une multiplication sur l'ensemble des congruences et ainsi faire de l'arithmétique modulo n :

$$\overline{a} + \overline{b} = \overline{a+b}$$

et

$$\overline{a}.\overline{b} = \overline{a.b}$$

Ces deux opérations font de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ un anneau commutatif unitaire : l'addition en fait un groupe abélien (l'élément neutre de l'addition est $\overline{0}$ et le symétrique de $\overline{a}$ est $\overline{-a}$) et la multiplication est associative, commutative et distributive par rapport à l'addition et d'élément neutre $\overline{1}$. Notons aussi que dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ on peut simplifier par les éléments m qui sont premiers avec n. Plus exactement si $am \equiv bm \pmod{n}$ et si $pgcd(m,n) = 1$ alors $a \equiv b \pmod{n}$. En effet si n divise $am - bm$, alors il doit diviser $a - b$ s'il est premier avec m. En particulier si $n = p$ est un nombre premier, on peut simplifier par tous les éléments de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ non nuls.

Definition 3 *: Un ensemble complet R de résidus modulo n est le choix d'un représentant de chaque classe de congruences modulo n.*

En général le choix le plus simple est :

$$R = \{0, 1, 2, \ldots, n-1\}$$

mais d'autres choix sont possibles. Par exemple pour $n = 3$ on peut prendre

$$R = \{0, 1, -1\}.$$

Proposition 2 *: Si R est un ensemble complet de résidus modulo n, il en est de même de $mR = \{mx, x \in R\}$ pour tout entier m premier avec n.*

Preuve : Il suffit de montrer que les éléments de mR sont tous distincts. En effet on aura alors $\#mR = \#R = n$ et donc mR est un ensemble complet de résidus. Supposons que $mx \equiv mx' \pmod{n}$ pour $x \neq x'$ dans R. Comme m est premier avec n, on peut simplifier par m et donc $x \equiv x' \pmod{n}$. Contradiction.

En utilisant ces ensembles R, on va montrer que l'equation $ax \equiv b \pmod{n}$ a toujours une solution en x si a est premier avec n.

Proposition 3 *: Si* $pgcd(a, n) = 1$ *alors l'équation linéaire* $ax \equiv b \pmod{n}$ *admet une solution.*

Preuve : Soit R un ensemble complet de résidus modulo n. Alors aR est aussi un ensemble complet de résidus. Cela veut dire qu'il existe un x dans R tel que $ax \equiv b \pmod{n}$.
Exemple : Soit l'équation $2x \equiv 3 \pmod{5}$. Comme 2 est premier avec 5, cette équation doit avoir une solution. Soit $R = \{0, 1, 2, 3, 4\}$ un ensemble complet de résidus modulo 5. On a :

$$2R = \{2.0, 2.1, 2.2, 2.3, 2.4\} = \{0, 2, 4, 6, 8\}$$

donc

$$2.4 = 8 \equiv 3 \pmod{5}$$

et la solution cherchée est $x = 4$.

En particuliersi $n = p$ est un nombre premier, l'equation $ax \equiv 1 \pmod{p}$ a une solution pour tout $a \neq 0$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$. Autrement dit tout élément non nul modulo p a un inverse pour la multiplication. Ainsi

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

est un groupe pour la multiplication modulo p. Comme l'ordre de ce groupe est $p - 1$, on obtient le petit théorème de Fermat :

Proposition 4 *: Si* p *est un nombre premier, on a :*

$$a^{p-1} \equiv 1 \pmod{p}$$

pour tout $a \in \mathbb{Z}$ *non congru à* 0 *modulo* p.

Preuve : L'ordre de tout élément d'un groupe fini divise l'ordre du groupe.

1.3 Racines de l'unité

Definition 4 *: Une racine primitive de l'unité modulo* p *est un élément de* $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$ *d'ordre exactement* $p - 1$.

Autrement dit une racine primitive ζ modulo p est un générateur de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$. Tout élément $a \in (\frac{\mathbb{Z}}{p\mathbb{Z}})^*$ s'écrit alors :

$$a = \zeta^r$$

pour un entier r compris entre 1 et $p-1$.

Dans ce numéro, nous allons montrer qu'une racine primitive modulo p existe toujours, ce qui fait de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$ un groupe cyclique d'ordre $p-1$. Pour cela remarquons d'abord que si d divise $p-1$, alors l'équation $x^d = 1$ modulo p a exactement d solutions. En effet soit e un entier tel que $de = p-1$. On a alors $x^{p-1} - 1 = (x^d)^e - 1 = (x^d - 1)((x^d)^{e-1} + (x^d)^{e-2} + ... + 1) = (x^d - 1)g(x)$ avec g un polynôme de degré $p - 1 - d$. Par le petit théorème de Fermat, on sait que l'equation $x^{p-1} = 1$ a exactement $p-1$ solutions modulo p. Comme g a au plus $p-1-d$ racines et que $x^d - 1$ a au plus d racines (par le théorème de Lagrange), on en déduit le résultat.

Proposition 5 *: Pour tout nombre premier p, il existe une racine primitive modulo p.*

Preuve : Soit

$$p - 1 = q_1^{n_1} ... q_k^{n_k}$$

la décomposition de $p-1$ en facteurs premiers. L'equation $x^{q_i^{n_i}} - 1$ a exactement $q_i^{n_i}$ solutions et l'équation $x^{q_i^{n_i - 1}} - 1$ a exactement $q_i^{n_i - 1}$ solutions. Il existe donc un élément a_i modulo p qui vérifie la première mais pas la seconde. Cet élément a_i est donc forcément d'ordre $q_i^{n_i}$. En répétant ce raisonnement pour $i = 1, ..., k$, posons

$$a = a_1 a_2 ... a_k$$

qui est un élément d'ordre $q_1^{n_1} ... q_k^{n_k} = p - 1$. C'est donc une racine primitive modulo p.

Chapitre 2

La loi de réciprocité quadratique

Dans ce second chapitre, nous énoncons et démontrons la loi de réciprocité quadratique. Dans la premiére section, on définit le symbole de legendre et nous étudions quelques unes de ces proprietés. La deuxieme section a pour théme le lemme de Gausse qui est essentiel dans la démonstration de la loi de réciprocité dans la troisieme section, on énonce la loi proprement dite que l'on démontre dans la dernière section

2.1 Le symbole de Legendre

Soit p un nombre premier. Un entier a non divisible par p est un résidu quadratique modulo p si a est un carré modulo p i.e s'il existe un entier x tel que

$$x^2 \equiv a \pmod{p}$$

Exemple : pour $p = 7$, on a $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 2$, $5^2 \equiv 4$ et $6^2 \equiv 1$. Donc $1, 2$ et 4 sont des résidus quadratiques modulo 7, mais $3, 5$ et 6 ne le sont pas.

Definition 5 *: Soit p un nombre premier impair et soit a un entier. On définit le symbole de Legendre $(\frac{a}{p})$ par $(\frac{a}{p}) = 0$ si p divise a, $(\frac{a}{p}) = 1$ si a est résidu quadratique modulo p et $(\frac{a}{p}) = -1$ si a n'est pas résidu quadratique modulo p.*

Le symbole de Legendre est égal au nombre de solutions de l'équation $x^2 = a$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ moins 1 :

$$(\frac{a}{p}) = \#\{x/x^2 \equiv a \pmod{p}\} - 1$$

Exemple : Toujours pour $p = 7$, on a $(\frac{1}{7}) = 1$, $(\frac{2}{7}) = 1$ et $(\frac{6}{7}) = -1$.
Le symbole de Legendre est multiplicatif comme le montre la :

Proposition 6 *: On a*

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$$

Preuve : Si $(\frac{a}{p}) = 0$ ou $(\frac{b}{p}) = 0$ alors p divise a ou p divise b et donc p divise ab, ce qui implique par définition que $(\frac{ab}{p}) = 0$. Supposons donc que $(\frac{a}{p}) \neq 0$ et $(\frac{a}{p}) \neq 0$. Donc p ne divise ni a ni b. Ainsi les classes de a et b modulo p sont non nulles. Ce sont donc des éléments de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^* = \{1, ..., p-1\}$. Soit ζ une racine primitive de l'unité modulo p i.e un générateur de ce dernier groupe. On peut écrire $a = \zeta^k$ et $b = \zeta^l$ pour k et l deux entiers. Donc $ab = \zeta^{k+l}$. Si on remarque que ζ^i est un carré si et seulement si i est pair, on en déduit le résultat en notant que la somme de deux entiers pairs est un entier pair, que la somme de deux entiers impairs est un entier pair et que la somme d'un entier pair et d'un entier impair est un entier impair.
Remarque : En termes de groupes cette proposition veut dire que l'application

$$\psi : (\frac{\mathbb{Z}}{p\mathbb{Z}})^* \longrightarrow \{+1, -1\}$$

donnée par $\psi(a) = (\frac{a}{p})$ est un morphisme de groupes :

$$\psi(ab) = \psi(a)\psi(b)$$

Le résultat suivant du à Euler permet de déterminer le symbole de Legendre :

Proposition 7 *(Euler) : Soit p un nombre premier impair et soit $a \in (\frac{\mathbb{Z}}{p\mathbb{Z}})^*$. Alors on a*

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

Preuve : La condition sur a implique que $(\frac{a}{p}) = +1$ ou $(\frac{a}{p}) = -1$. Si $(\frac{a}{p}) = 1$, cela veut dire que a est résidu quadratique modulo p. Il existe donc x tel que $x^2 \equiv a \pmod{p}$. Soit ζ une racine primitive de l'unité modulo p. On sait que $x = \zeta^r$ pour un entier r. Donc $a \equiv (\zeta^r)^2 \equiv \zeta^{2r} \pmod{p}$. Ceci donne $a^{\frac{p-1}{2}} \equiv \zeta^{2r\frac{p-1}{2}} \equiv \zeta^{r(p-1)} \equiv 1 \pmod{p}$ par le petit théorème de Fermat ($\zeta^{p-1} \equiv 1 \pmod{p}$). Inversement supposons que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. On a $q = \zeta^k$ pour un certain entier k. Donc $\zeta^{k\frac{p-1}{2}} \equiv 1 \pmod{p}$ et donc $p-1$ divise $k\frac{p-1}{2}$. Ceci montre que k est un entier pair. On peut donc écrire $a = (\zeta^{\frac{k}{2}})^2 = x^2$ avec $x = \zeta^{\frac{k}{2}}$ et donc $(\frac{a}{p}) = 1$. Si $(\frac{a}{p}) = -1$, cela veut dire que l'équation $x^2 \equiv a \pmod{p}$ n'a pas de solutions et donc $a^{\frac{p-1}{2}} \neq 1$ modulo p. Mais $a^{\frac{p-1}{2}}$ est racine du polynôme $x^2 - 1$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ (par le petit théorème de Fermat) qui n'a que deux racines : $+1$ et -1. On doit donc avoir $a^{\frac{p-1}{2}} \equiv -1 \pmod{p} = (\frac{a}{p})$.
On obtient ainsi un critère simple pour voir si l'equation $x^2 \equiv a \pmod{p}$ a une solution ou non :
Critère d'Euler : $x^2 \equiv a \pmod{p}$ (p premier impair et a non divisible par p) a une solution si et seulement si :

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Exemple : Soit $p = 7$. On a $1^2 = 1$, $2^2 = 4$, $3^2 = 2$, $4^2 = 2$, $5^2 = 4$, $6^2 = 1$. Les carrés dans $\frac{\mathbb{Z}}{7\mathbb{Z}}$ sont donc $1, 2$ et 4. Calculons $a^{\frac{p-1}{2}}$ pour $a \in (\frac{\mathbb{Z}}{7\mathbb{Z}})^*$. On a $1^3 = 1$, $2^3 = 1$, $3^3 = -1$, $4^3 = 1$, $5^3 = -1$ et $6^3 = -1$. L'ensemble des a avec $a^3 = 1$ est donc égal à l'ensemble des résidus quadratiques modulo 7.

La proposition précédente peut être reformulée en termes de groupes : l'application

$$\psi : (\frac{\mathbb{Z}}{p\mathbb{Z}})^* \longrightarrow \{+1, -1\}$$

donnée par $\psi(a) = a^{\frac{p-1}{2}} \pmod{p}$ est un morphisme de groupes, de noyau l'ensemble des carrés modulo p.
D'aprés le résultat d'Euler, pour calculer le symbole de Legendre $(\frac{a}{p})$, il suffit de calculer $a^{\frac{p-1}{2}}$ modulo p. Dans certains cas ce calcul est assez simple. Par exemple on a toujours

$$(\frac{1}{p}) = 1$$

et

$$(\frac{-1}{p}) = \pm 1$$

selon que $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$. La première formule est claire. Expliquons la deuxième. On a $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. Comme p est un nombre impair il ne peut prendre que deux valeurs modulo 4 : 1 et 3. Si $p \equiv 1 \pmod 4$, cela veut dire que $p = 4k + 1$. Donc $\frac{p-1}{2} = 2k$ est un entier pair et $(-)^{\frac{p-1}{2}} = 1$. Si $p \equiv 3 \pmod 4$, alors on doit avoir $p = 4k + 3$ et donc $\frac{p-1}{2} = 2k + 1$ est un entier impair, ce qui donne $(-1)^{\frac{p-1}{2}} = -1$.

2.2 Le lemme de Gauss

Le résultat d'Euler permet de donner une expression au symbole de Legendre, mais ne permet pas de le calculer effectivement. Le lemme de Gauss est une première tentative dans cette direction. Soit R l'ensemble suivant :

$$R = \{a, 2a, ..., (\frac{p-1}{2})a\}$$

avec p un nombre premier impair et $a \in (\frac{\mathbb{Z}}{p\mathbb{Z}})^*$. Soit r le nombre d'éléments de R qui sont dans l'ensemble :

$$\{\frac{p+1}{2}, ..., p-1\}$$

Proposition 8 *: On a*

$$(\frac{a}{p}) = (-1)^r$$

Preuve : Remarquons que $(\frac{\mathbb{Z}}{p\mathbb{Z}})^* = \{1, ..., p-1\} = \{1, ..., \frac{p-1}{2}\} \cup \{\frac{p+1}{2}, ..., p-1\}$ et que $R = a.\{1, ..., \frac{p-1}{2}\} \subset (\frac{\mathbb{Z}}{p\mathbb{Z}})^*$. Les éléments de R se répartissent donc entre les deux sous-ensembles de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$. Notons que si $x \neq x'$ dans R, alors on a forcément $x \neq \pm x'$ (Ceci est vrai pour les éléments de $\{1, ..., \frac{p-1}{2}\}$ et donc $ax \neq \pm ax'$). Soient $x_1, ..., x_s$ les éléments de R qui sont dans $\{1, ..., \frac{p-1}{2}\}$ et soient $x_1', ..., x_r'$ ceux qui sont dans $\{\frac{p+1}{2}, ..., p-1\}$. On a l'égalité d'ensembles :

$$\{x_1, ..., x_s, p - x_1', ..., p - x_r'\} = \{1, 2, ..., \frac{p-1}{2}\}$$

En prenant le produit des éléments de R, on obtient :

$$a.2a.3a...\frac{p-1}{2}a = x_1...x_s.x_1^{'}...x_r^{'}$$

Comme $p - x_i^{'} \equiv -x_i^{'} \pmod{p}$, on a donc

$$a.2a.3a...\frac{p-1}{2}a = (-1)^r x_1...x_s.(p-x_1^{'})...(p-x_r^{'})$$

$$= (-1)^r 1.2.3...\frac{p-1}{2}$$

ce qui donne

$$a^{\frac{p-1}{2}}(\frac{p-1}{2})! = (-1)^r(\frac{p-1}{2})!$$

i.e

$$a^{\frac{p-1}{2}} = (-1)^r$$

Pour illustrer ce lemme essayons par exemple de calculer $(\frac{2}{p})$. Ici $a = 2$ et donc $R = \{2, 4, ..., p-1\}$. Nous devons trouver la parité du nombre r d'éléments de R qui sont dans $\{\frac{p+1}{2}, ..., p-1\}$ ou de manière équivalente qui sont dans l'intervalle ouvert $I = \left]\frac{p}{2}, p\right[$. Mais on a

$$\#(I \cap R) = \#(\frac{1}{2}I \cap \mathbb{Z}) = \#(\left]\frac{p}{4}, \frac{p}{2}\right[\cap \mathbb{Z})$$

Si $p = 8k + s$, ce cardinal est égal à

$$\#(\left]2k + \frac{s}{4}, 4k + \frac{s}{2}\right[\cap \mathbb{Z}) \equiv \#(\left]\frac{s}{4}, \frac{s}{2}\right[\cap \mathbb{Z}) \pmod{2}$$

Les possibilités pour s sont $1, 3, 5, 7$ (puisque p est un nombre premier impair). Si $s = 1$, le cardinal est 0, si $s = 3, 5$ le cardinal est 1 et si $s = 7$ le cardinal est 2. Donc $(\frac{2}{p}) = 1$ si $p \equiv 1$ ou $7 \pmod{8}$ et $(\frac{2}{p}) = -1$ si $p \equiv 3$ ou$5 \pmod{8}$. Comme $7 \equiv -1 \pmod{8}$ et $5 \equiv -3 \pmod{8}$ cela donne aussi $(\frac{2}{p}) = 1$ si $p \equiv \pm 1 \pmod{8}$ et $(\frac{2}{p}) = -1$ si $p \equiv \pm 3 \pmod{8}$. Remarquons maintenant que $p^2 - 1$ est toujours divisible par 8 et que $\frac{p^2-1}{8}$ est pair si $p \equiv \pm 1 \pmod{8}$ et impair si $p \equiv \pm 3 \pmod{8}$. On a donc

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

2.3 La loi de réciprocité quadratique

On a vu que le symbole de Legendre $(\frac{a}{p})$, en tant que fonction de son numérateur a, ne dépend que de a modulo p et qu'il était multiplicatif, ce qui permet de se concentrer sur les symboles de la forme $(\frac{q}{p})$ avec q un nombre premier impair, en plus des deux symboles $(\frac{-1}{p})$ et $(\frac{2}{p})$. En effet par le théorème fondamental de l'arithmétique, on a

$$a = \pm q_1^{r_1} ... q_k^{r_k}$$

avec les q_i des nombres premiers et donc

$$(\frac{a}{p}) = (\frac{\pm 1}{p})(\frac{q_1}{p})^{r_1} ... (\frac{q_k}{p})^{r_k}$$

On peut aussi voir le symbole de Legendre comme fonction de son dénominateur p. La loi de réciprocité quadratique est une relation entre ce symbole en tant que fonctions de son numérateur et de son dénominateur :

Théorème 2 *: Soient p et q deux nombres premiers impairs. Alors on a :*

$$(\frac{p}{q}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} (\frac{q}{p})$$

De plus

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

et

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

La démonstration de ce théorème sera donnée au numéro prochain, mais faisons déja quelques remarques. La deuxième et la troisième formules ont déja été traitées comme exemples. Il nous reste donc la première qui est une sorte de réciprocité entre savoir si q est résidu quadratique modulo p et si p est résidu quadratique modulo q. Voyons sur quelques exemples comment on peut l'utiliser.
Supposons que l'on veuille savoir quels sont les nombres premiers p pour lesquels 5 est résidu quadratique. Autrement dit nous voulons calculer $(\frac{5}{p})$. D'aprés la loi on a :

$$(\frac{5}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{5-1}{2}} (\frac{p}{5}) = (-1)^{p-1} (\frac{p}{5})$$

Comme $p-1$ est pair (et donc $(-1)^{p-1}=1$), on obtient

$$(\frac{5}{p})=(\frac{p}{5})$$

Le problème revient donc à savoir quels sont les nombres premiers p qui sont résidus quadratiques modulo 5. p modulo 5 peut prendre quatre valeurs $1,2,3$ et 4 dans $\frac{\mathbb{Z}}{5\mathbb{Z}}$ dans lequel on a $1^2=1$, $2^2=4$, $3^2=1$ et $4^2=1$. 1 et 4 sont donc résidus quadratiques modulo 5, mais 2 et 3 ne le sont pas. Donc

$$(\frac{p}{5})=1$$

si $p\equiv 1$ ou $4 \pmod 5$ et

$$(\frac{p}{5})=-1$$

si $p\equiv 2$ ou $3 \pmod 5$. La réponse à notre question est donc : 5 est résidu quadratique modulo p exactement quand $p\equiv 1$ ou 4 modulo 5.
Comme second exemple supposons que l'on veuille savoir si 69 est résidu quadratique modulo $p=389$. Autrement dit nous voulons calculer $(\frac{69}{389})$. Comme $69=3.23$, on a

$$(\frac{69}{389})=(\frac{3.23}{289})=(\frac{3}{389})(\frac{23}{389})$$

et en utilisant la loi, on trouve :

$$(\frac{3}{389})=(-1)^{\frac{3-1}{2}.\frac{389-1}{2}}(\frac{389}{3})=(\frac{2}{3})=-1$$

et

$$\begin{aligned}(\frac{23}{389})&=(-1)^{\frac{23-1}{2}.\frac{389-1}{2}}(\frac{389}{3})=(\frac{21}{23})\\&=(\frac{-2}{23})=(\frac{-1}{23})(\frac{2}{23})\\&=(-1)^{\frac{23-1}{2}}.1=-1\end{aligned}$$

ce qui donne

$$(\frac{69}{389})=(-1)(-1)=1$$

et donc 69 est résidu quadratique modulo 389.

2.4 Démonstration de la loi

Soient p et q deux nombres premiers impairs. On sait que $(\frac{q}{p}) = (-1)^r$ avec r le nombre d'éléments de $R = \{q, 2q, ..., \frac{p-1}{2}q\}$ qui sont dans $\{\frac{p+1}{2}, ..., p-1\}$ et que l'on a noté $x_1^{'}, ..., x_r^{'}$. Les éléments de R qui sont dans $\{1, ..., \frac{p-1}{2}\}$ ont été notés $x_1, ..., x_k$. Chaque élément de R est de la forme qi avec $1 \leq i \leq \frac{p-1}{2}$. Ecrivons :

$$qi = \lfloor \frac{qi}{p} \rfloor p + r_i$$

avec $0 < r_i < p$ et $\lfloor \frac{qi}{p} \rfloor$ etant la partie entière de $\frac{qi}{p}$. Si $1 \leq r_i \leq \frac{p-1}{2}$, alors $r_i = x_j$ pour un certain j et si $\frac{p+1}{2} \leq r_i \leq p-1$, alors $r_i = x_j^{'}$ pour un certain j. Considérons la somme suivante

$$\sum_{i=1}^{\frac{p-1}{2}} qi$$

La parité de cette somme (i.e sa classe modulo 2) peut être calculée de deux manières. On a d'abord

$$\sum_{i=1}^{\frac{p-1}{2}} qi = q \sum_{i=1}^{\frac{p-1}{2}} i = q(\sum_{j=1}^{k} x_j + \sum_{j=1}^{r} (p - x_j^{'}))$$

$$\equiv (\sum_{j=1}^{k} x_j + r + \sum_{j=1}^{r} x_j^{'}) \pmod 2$$

(on a utilisé le fait que $-1 \equiv 1 \pmod 2$ et p et q impairs, ce qui donne en particulier $p - x_j^{'} \equiv 1 + x_j^{'} \pmod 2$). D'autre part on a aussi

$$\sum_{i=1}^{\frac{p-1}{2}} qi = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{qi}{p} \rfloor p + r_i$$

$$= p \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{qi}{p} \rfloor + \sum_{j=1}^{k} x_j + \sum_{j=1}^{r} x_j^{'}$$

$$\equiv \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{qi}{p} \rfloor + \sum_{j=1}^{k} x_j + \sum_{j=1}^{r} x_j^{'} \pmod 2$$

Donc

$$r \equiv S(q,p) \pmod 2$$

avec

$$S(q,p) = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{qi}{p} \rfloor$$

Ainsi on a

$$(\frac{q}{p}) = (-1)^{S(q,p)}$$

En échangeant les rôles de p et q, on trouve

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{S(p,q)+S(q,p)}$$

Mais $S(p,q)+S(q,p)$ est le nombre de points du réseau entier contenus dans la boite rectangulaire de coin inférieur $(1,1)$ et de point supérieur $(\frac{p-1}{2}, \frac{q-1}{2})$ qui est $\frac{p-1}{2}.\frac{q-1}{2}$. On obtient donc finalement

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

et donc

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

Chapitre 3

Relation avec la K-théorie

Dans ce derniere chapitre on fait la relation entre la loi de réciprocité et la K-théorie algébrique. La plupart des résultats seront énoncés sans démonstration, le but étant d'expliquer briévement cette relation interessante.

3.1 Symboles

Soit K un corps commutatif et soit $F^* = F - \{0\}$

Definition 6 *: Un symbole sur K à valeurs dans un groupe abélien A est une application $c : K^* \times K^* \longrightarrow A$ bimultiplicative et qui vérifie*

$$c(x, 1-x) = 1$$

pour tout $x \neq 1$ dans F^*.

Un tel symbole vérifie

$$c(1,x) = c(x,1) = 1; c(x, 1-x^{-1}) = 1; c(x, x^{-1}) = 1$$

$$c(x,x) = c(-1,x) = c(x,-1)$$

et

$$c(x,y) = c(y,x)^{-1}$$

Exemple 1(Le symbole de Hilbert) : Soit $F = \mathbb{Q}_p$ le corps des nombres

p-adiques pour p un nombre premier ou $F = \mathbb{R} = \mathbb{Q}_\infty$ le corps des nombres réels. Le symbole de Hilbert sur F à valeurs dans le groupe $A = \{+1, -1\}$ est le symbole

$$c_p(a, b) = (\frac{a, b}{p})$$

Il est égal à $+1$ si l'équation $ax^2 + by^2 = 1$ a des solutions x et y non toutes deux nulles dans F et il est égal à -1 sinon. En particulier ce symbole est défini pour tous a, b dans $\mathbb{Q}^*$ (puisque $\mathbb{Q} \subset \mathbb{Q}_p$ pour tout p). La relation avec le symbole de Legendre est la suivante : Si $a = p$ et $b = q$ sont des nombres premiers impairs, alors

$$(\frac{p, q}{p}) = (\frac{q}{p})$$

$$(\frac{p, q}{r}) = 1$$

si r est un nombre premier impair avec $r \neq p$ et $r \neq q$ et

$$(\frac{p, q}{2}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

$$(\frac{p, q}{\infty}) = 1$$

Ainsi si P désigne l'ensemble des nombres premiers plus le symbole ∞, on obtient

$$\prod_{r \in P} (\frac{p, q}{r}) = (\frac{p}{q})(\frac{q}{p})(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

et la loi de réciprocité équivaut donc à la formule du produit de Hilbert :

$$\prod_{r \in P} (\frac{a, b}{r}) = 1$$

pour tous nombres rationnels non nuls a, b.

Exemple 2(Le symbole modéré) : Soit F un corps muni d'une valuation discrète v. Soit

$$O = \{x / v(x) \geq 0\}$$

l'anneau de la valuation et soit

$$P = \{x / v(x) > 0\}$$

l'déal maximal de O. L'anneau quotient

$$\frac{O}{P}$$

est un corps appelé le corps résiduel de la valuation. Soient x, y des éléments non nuls de F. L'élément

$$(-1)^{v(x)v(y)}(\frac{x^{v(y)}}{y^{v(x)}})$$

a une valuation nulle. C'est donc un élément de O non nul modulo P. Soit $c_v(x, y)$ sa classe modulo P. Ceci définit donc une application

$$c_v : F^* \times F^* \longrightarrow (\frac{O}{P})^*$$

qui est un symbole sur F à valeurs dans le groupe multiplicatif du corps résiduel. Si $F = \mathbb{Q}_p$ est le corps des p-adiques et v est la valuation p-adique on pose

$$c_v(x, y) = (x, y)_p$$

(avec ici $\frac{O}{P} \cong (\frac{\mathbb{Z}}{p\mathbb{Z}})^*) = A_p$) et on a la relation suivante avec le symbole de Hilbert

$$(\frac{x, y}{p}) = ((x, y)_p)^{\frac{p-1}{2}}$$

Si $p = 2$, la définition précédente conduit à un symbole trivial et on pose

$$(x, y)_2 = (\frac{x, y}{2})$$

à valeurs dans $A_2 = \{-1, +1\}$.

3.2 Le K_2 d'un corps

Le groupe abélien K_2F est défini par les générateurs $\{x, y\}$ avec $x, y \in F^*$ et les relations :

$$\{x, 1 - x\} = 1$$

$$\{x_1x_2, y\} = \{x_1, y\}\{x_2, y\}$$

et

$$\{x, y_1y_2\} = \{x, y_1\}\{x, y_2\}$$

On a automatiquement un morphisme

$$\{.,.\} : F^* \times F^* \longrightarrow K_2F$$

et tout symbole $c : F^* \times F^* \longrightarrow A$ sur F se factorise à travers K_2F : il existe un unique morphisme $\phi : K_2F \longrightarrow A$ tel que

$$c(x, y) = \phi(\{x, y\})$$

Pour $F = \mathbb{Q}$, on a un résultat intéressant démontré par Tate en 1970 qui permet de déterminer la structure de $K_2\mathbb{Q}$:

Proposition 9 *(Tate) : On a un isomorphisme*

$$K_2\mathbb{Q} \longrightarrow \prod_p A_p$$

donné par

$$\{x, y\} \mapsto \prod_p (x, y)_p$$

Remarquer que ce dernier produit a un sens car $(x, y)_p = 1$ pour presque tout p. Ce résultat de Tate et la définition du K_2 permettent de montrer :

Proposition 10 *: Pour tout symbole $c : \mathbb{Q}^* \times \mathbb{Q}^* \longrightarrow A$, il existe une unique famille de morphismes $\phi_p : A_p \longrightarrow A$ telle que*

$$c(x, y) = \prod_p \phi_p((x, y)_p)$$

Preuve : On sait qu'il existe un seul morphisme $\phi : K_2\mathbb{Q} \longrightarrow A$ tel que $c(x, y) = \phi(\{x, y\})$. Comme $K_2\mathbb{Q} \cong \prod_p A_p$ et si on note l'injection canonique $A_p \longrightarrow K_2\mathbb{Q}$ par i_p, on obtient

$$\phi_p = \phi \circ i_p$$

3.3 Lien avec la loi de réciprocité

Appliquons cette dernière proposition au symbole de Hilbert $(\frac{x,y}{\infty})$ qui est à valeurs dans $A_2 = \{-1, +1\}$. Il existe une famille unique de morphismes $\phi_p : A_p \longrightarrow A_2$ tels que

$$(\frac{x, y}{\infty}) = \prod_p \phi_p((x, y)_p)$$

Si p est impair, le groupe A_p est cyclique et il n'y a que deux morphismes $A_p \longrightarrow A_2$ donnés par $z \mapsto 1$ et $z \mapsto z^{\frac{p-1}{2}}$. On obtient donc

$$\phi_p(z) = z^{\epsilon_p \frac{p-1}{2}}$$

avec $\epsilon_p = 0$ ou 1. On a donc

$$\phi_p((x,y)_p) = (((x,y)_p)^{\frac{p-1}{2}})^{\epsilon_p} = (\frac{x,y}{p})^{\epsilon_p}$$

Si $p = 2$, il n'y a aussi que deux morphismes $A_2 \longrightarrow A_2$ donnés par $z \mapsto z^{\epsilon_2}$ avec $\epsilon_2 = 0$ ou 1 et on a

$$\phi_2((x,y)_2) = ((x,y)_2)^{\epsilon_2} = (\frac{x,y}{2})^{\epsilon_2}$$

En combinant tout cela on obtient en définitive

$$(\frac{x,y}{\infty}) = \prod_p (\frac{x,y}{p})^{\epsilon_p}$$

avec $\epsilon_p = 0$ ou 1. Pour montrer la loi de réciprocité, il faut donc montrer que tous les ϵ_p sont égaux à 1. Nous nous contenterons ici de le faire pour ϵ_2. Si on prend $x = y = -1$, on trouve

$$(\frac{-1,-1}{\infty}) = -1$$

et

$$(\frac{-1,-1}{p}) = 1$$

pour p premier impair. En effet l'équation $ax^2 + by^2 = c$ a des racines dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ si $ab \neq 0$. Donc

$$(\frac{-1,-1}{2})^{\epsilon_2} = -1$$

et comme $(\frac{-1,-1}{2}) = -1$ (-1 n'est pas somme de deux carrés dans $\frac{\mathbb{Z}}{8\mathbb{Z}}$), on en déduit que

$$\epsilon_2 = 1$$

Bibliographie

[1] C.F. Gauss, Disquisitiones Arithmeticae, Werke, Band I, Gottingen, 1870.

[2] W. Stein, Explicit Elementary Number Theory, Harvard, 2002.

[3] J. Milnor, Introduction to algebraic K-theory, Princeton University Press, 1971.

[4] J.P. Serre, Cours d'arithmétique, Presses universitaires de France, Paris, 1970.