

Travaux dirigés de DEA

Le théorème de Kummer sur l'équation de Fermat

Alain Kraus

Université de Paris VI

Novembre 2004

Introduction

Ces travaux dirigés comportent six séances de deux heures. Leur objectif est de se familiariser avec les notions de base de la théorie algébrique des nombres, et de les utiliser concrètement sous forme d'exercices, à travers une démonstration du théorème de Kummer sur l'équation de Fermat (1850) (cf. [Ku]) :

Théorème. *Soient p un nombre premier impair et K le sous-corps de \mathbb{C} engendré par les racines p -ièmes de l'unité. On suppose que p ne divise pas le nombre de classes de K . Alors, si x, y, z sont des éléments de K tels que $x^p + y^p = z^p$, on a $xyz = 0$.*

Au cours de la preuve, on admettra le théorème de réciprocité d'Artin concernant le corps de classes de Hilbert d'un corps de nombres. D'un point de vue théorique, la théorie de Galois des extensions finies de corps et les premières propriétés des corps de nombres sont supposées connues : anneaux d'entiers, groupe des unités, groupe des classes d'idéaux, décomposition des idéaux premiers dans les extensions. Toutes ces notions sont exposées en détail par exemple dans le livre de P. Samuel ([Sa]).

Ces notes sont divisées en trois chapitres. Le premier est essentiellement consacré à la notion de corps de classes de Hilbert d'un corps de nombres et à l'énoncé du théorème de réciprocité correspondant. Mis à part l'énoncé de ce théorème, la lecture de ce chapitre n'est pas, à strictement parler, indispensable pour aborder les exercices figurant dans le chapitre II. Cela étant, on pourra y trouver des résultats et des exercices liés à la notion de corps de classes de Hilbert. Il se trouve par ailleurs des exemples concrets illustrant le théorème de réciprocité, ainsi que des applications concernant les nombres premiers représentés par la forme quadratique $x^2 + ny^2$. Par exemple, la description du corps de classes de Hilbert de $\mathbb{Q}(\sqrt{-5})$ permet de prouver qu'un nombre premier, autre que 5, est de la forme $x^2 + 5y^2$ si et seulement si il est congru à 1 ou 9 modulo 20 (c'est un résultat analogue au théorème des deux carrés prouvé par Fermat).

Le deuxième chapitre est constitué des énoncés des exercices sur la démonstration du théorème de Kummer, ainsi que d'un complément dû à Vandiver sur l'équation de Fermat généralisée (1931).

Dans le troisième chapitre, il y a quelques remarques sur l'hypothèse faite dans l'énoncé du théorème. Un nombre premier qui la vérifie est dit régulier. On énoncera quelques résultats sur le groupe des classes de K , ainsi que deux critères très pratiques dus à Kummer permettant de tester si un nombre premier donné est ou non régulier, tout au moins s'il n'est pas trop grand. À titre indicatif, les nombres premiers plus petits que 100, distincts de 37, 59 et 67, sont réguliers. Signalons que l'on ne sait pas étendre le théorème de Kummer aux nombres premiers qui ne sont pas réguliers. Néanmoins, A. Wiles en 1995 est parvenu à démontrer le théorème de Fermat sur \mathbb{Q} comme conséquence de ses travaux

sur la conjecture de Taniyama-Shimura et de ceux de K. Ribet sur les représentations modulaires ([Wi] et [Ri]).

Je remercie D. Bernardi pour les remarques qu'il m'a faites concernant certains points de ce texte.

Table des matières

Chapitre I. Préliminaires	3
1. Ramification	3
2. Extensions non ramifiées	6
3. Nombres de classes des corps quadratiques imaginaires	7
4. Substitution de Frobenius	8
5. Corps de classes de Hilbert - Théorème de réciprocité	11
6. Exemples	13
7. Applications	14
Chapitre II. Le théorème de Kummer (exercices)	17
1. Exercices préliminaires	17
2. Lemmes de Kummer sur les unités	19
3. Démonstration du premier cas	20
4. Démonstration du deuxième cas	22
5. Complément - Théorème de Vandiver	23
Chapitre III. Sur les nombres premiers réguliers	25
1. Sur le groupe des classes de K	25
2. Critères de régularité	28
Bibliographie	30

Chapitre I — Préliminaires

Soit $\overline{\mathbb{Q}}$ la clôture algébrique de \mathbb{Q} dans \mathbb{C} . Tous les corps de nombres considérés dans la suite seront supposés contenus dans $\overline{\mathbb{Q}}$. Un corps de nombres K étant donné, on désignera dans ce chapitre par O_K son anneau d'entiers et D_K son discriminant. Dans ces notes un idéal premier de O_K sera toujours implicitement supposé non nul sans autre précision.

1. Ramification

Considérons un corps de nombres K . Posons $K = \mathbb{Q}(\alpha)$ où $\alpha \in O_K$. Soit $f \in \mathbb{Z}[X]$ le polynôme minimal de α sur \mathbb{Q} . Les \mathbb{Z} -modules O_K et $\mathbb{Z}[\alpha]$ sont libres de rang le degré de K sur \mathbb{Q} . Par suite, $\mathbb{Z}[\alpha]$ est d'indice fini dans O_K . Étant donné un nombre premier p qui ne divise pas cet indice, on utilisera le résultat ci-dessous qui fournit un critère effectif simple pour décrire la décomposition de l'idéal pO_K en produit d'idéaux premiers de O_K ([Coh], p. 196). On note $\overline{f} \in \mathbb{F}_p[X]$ le polynôme déduit de f par réduction.

Théorème 1. *Soit p un nombre premier qui ne divise pas l'indice de $\mathbb{Z}[\alpha]$ dans O_K . Soit*

$$\overline{f} = \prod_{i=1}^g h_i^{e_i},$$

la décomposition de \overline{f} en produit de polynômes irréductibles dans $\mathbb{F}_p[X]$. Pour $i = 1, \dots, g$ soit $f_i \in \mathbb{Z}[X]$ un relèvement unitaire de h_i . Posons

$$\mathfrak{P}_i = pO_K + f_i(\alpha)O_K.$$

Alors, les idéaux \mathfrak{P}_i sont distincts deux à deux et sont les idéaux premiers de O_K au-dessus de p . On a

$$pO_K = \prod_{i=1}^g \mathfrak{P}_i^{e_i},$$

et le degré résiduel de \mathfrak{P}_i sur p est le degré de f_i .

Rappelons que si K est un corps quadratique, pour tout nombre premier p , le type de décomposition de pO_K en produit d'idéaux premiers ne dépend que du symbole de Kronecker- Legendre $\left(\frac{D_K}{p}\right)$. On a (*loc. cit.* ou [Sa], p. 91) :

$$(1) \quad \left(\frac{D_K}{p}\right) = \begin{cases} -1 & \text{si } p \text{ est inerte} \\ 0 & \text{si } p \text{ est ramifié} \\ 1 & \text{si } p \text{ est décomposé.} \end{cases}$$

Exercice 1

Soient $f \in \mathbb{Z}[X]$ un polynôme irréductible unitaire, α une racine de f dans \mathbb{C} et K le corps $\mathbb{Q}(\alpha)$. On note $D(f)$ le discriminant de f . Montrer que l'on a l'égalité

$$D(f) = D_K \left[O_K : \mathbb{Z}[\alpha] \right]^2,$$

où $[O_K : \mathbb{Z}[\alpha]]$ est l'indice de $\mathbb{Z}[\alpha]$ dans O_K .

Exercice 2

On pose $f = X^4 - X - 1 \in \mathbb{Z}[X]$. Soient α une racine de f dans \mathbb{C} et K le corps $\mathbb{Q}(\alpha)$.

- 1) Montrer que f est irréductible sur \mathbb{Q} .
- 2) Calculer le discriminant de f et celui de K .
- 3) Montrer que l'on a $O_K = \mathbb{Z}[\alpha]$.
- 4) Déterminer les décompositions des idéaux $2O_K$ et $7O_K$ en produits d'idéaux premiers.

Exercice 3

Soit K une extension galoisienne finie de \mathbb{Q} qui n'est pas cyclique, i.e. dont le groupe de Galois de K sur \mathbb{Q} n'est pas cyclique. Démontrer que pour tout nombre premier p , l'idéal de O_K engendré par p n'est pas premier, autrement dit, qu'il n'existe pas de nombres premiers inertes dans K .

Considérons maintenant une extension galoisienne finie L/K . Posons $L = K(\alpha)$ où $\alpha \in O_L$. Soient $f \in O_K[X]$ le polynôme minimal de α sur K et \mathfrak{p} un idéal premier de O_K . Rappelons que, L/K étant galoisienne, les degrés résiduels et les indices de ramification des idéaux premiers de O_L au-dessus de \mathfrak{p} sont les mêmes et ne dépendent que de \mathfrak{p} . Posons $k = O_K/\mathfrak{p}$ et notons $\bar{f} \in k[X]$ le polynôme déduit de f par réduction. On utilisera le résultat suivant (cf. [Cox], p. 102) :

Théorème 2. *Supposons que $\bar{f} \in k[X]$ soit séparable. Soit*

$$\bar{f} = \prod_{i=1}^g h_i,$$

la décomposition de \bar{f} en produit de polynômes irréductibles $h_i \in k[X]$. Alors :

- 1) l'idéal \mathfrak{p} est non ramifié dans L et pour tout i le degré de h_i est le degré résiduel de \mathfrak{p} dans L/K .
- 2) Il existe exactement g idéaux premiers de O_L au-dessus de \mathfrak{p} .
- 3) L'idéal \mathfrak{p} est totalement décomposé dans L si et seulement si \bar{f} a une racine dans k .

Notons que si $K = \mathbb{Q}$, en posant $\mathfrak{p} = p\mathbb{Z}$, le fait que \bar{f} soit séparable entraîne que p ne divise pas l'indice de $\mathbb{Z}[\alpha]$ dans O_L (cf. l'exercice 1).

Démonstration du théorème 2 : Notons $e_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$ l'indice de ramification et le degré résiduel de \mathfrak{p} dans L/K . Soit \mathfrak{P} un idéal premier de O_L au-dessus de \mathfrak{p} . Le corps $\ell := O_L/\mathfrak{P}$ est une extension finie de k de degré $f_{\mathfrak{p}}$. Pour tout $x \in O_L$, on note \bar{x} son image dans ℓ .

1) On a

$$f = \prod_{\sigma \in \text{Gal}(L/K)} (X - \sigma(\alpha)),$$

où $\text{Gal}(L/K)$ est le groupe de Galois de L sur K . Il en résulte que

$$(2) \quad \bar{f} = \prod_{\sigma \in \text{Gal}(L/K)} (X - \overline{\sigma(\alpha)}) \in k[X].$$

Soit i un entier entre 1 et g . Il existe $s \in \text{Gal}(L/K)$ tel que l'on ait

$$(3) \quad h_i(\overline{s(\alpha)}) = 0.$$

Soit $f_i \in O_K[X]$ un relèvement de h_i . La condition (3) signifie que $f_i(s(\alpha))$ est dans \mathfrak{P} . Notons $D_{\mathfrak{P}}$ le sous-groupe de décomposition en \mathfrak{P} de $\text{Gal}(L/K)$. Pour tout $\tau \in D_{\mathfrak{P}}$, on a

$$f_i(\tau s(\alpha)) \in \tau(\mathfrak{P}) = \mathfrak{P},$$

et $\overline{\tau s(\alpha)} \in \ell$ est donc une racine de h_i . Puisque \bar{f} est séparable, l'égalité (2) entraîne que pour tous τ_1 et τ_2 dans $D_{\mathfrak{P}}$ distincts, on a

$$\overline{\tau_1 s(\alpha)} \neq \overline{\tau_2 s(\alpha)}.$$

Par suite, h_i a au moins $|D_{\mathfrak{P}}|$ racines distinctes dans ℓ . Si n_i est le degré de h_i , on a donc $n_i \geq |D_{\mathfrak{P}}|$. Puisque $|D_{\mathfrak{P}}| = e_{\mathfrak{p}} f_{\mathfrak{p}}$ ([Sa], p. 106), on obtient ainsi

$$n_i \geq e_{\mathfrak{p}} f_{\mathfrak{p}}.$$

Par ailleurs, h_i étant irréductible sur k , le degré de l'extension $k(\overline{s(\alpha)})/k$ est n_i . Le corps $k(\overline{s(\alpha)})$ étant contenu dans ℓ , on a donc $n_i \leq f_{\mathfrak{p}}$. Les inégalités

$$f_{\mathfrak{p}} \geq n_i \geq e_{\mathfrak{p}} f_{\mathfrak{p}},$$

entraînent alors $e_{\mathfrak{p}} = 1$, $n_i = f_{\mathfrak{p}}$ et l'assertion 1.

2) Le degré de \bar{f} est celui de f i.e. le degré de L sur K . D'après l'assertion 1 on a donc $[L : K] = f_{\mathfrak{p}} g$. Par ailleurs, L/K étant galoisienne, si g' est le nombre d'idéaux premiers de O_L au-dessus de \mathfrak{p} , on a $[L : K] = e_{\mathfrak{p}} f_{\mathfrak{p}} g' = f_{\mathfrak{p}} g'$. D'où $g = g'$.

3) Si \bar{f} a une racine dans k , tel est le cas d'un polynôme h_i , qui étant irréductible, est donc de degré 1. Par suite, on a $f_{\mathfrak{p}} = 1$ puis $g = [L : K]$ i.e. \mathfrak{p} est totalement décomposé dans L . Inversement, l'égalité $g = [L : K]$ entraîne $f_{\mathfrak{p}} = 1$, tous les h_i sont de degré 1 et en particulier \bar{f} a une racine dans k . D'où l'assertion 3 et le théorème.

Dans le cas où L/K est une extension quadratique, on en déduit le résultat suivant ([Cox], p. 114) :

Corollaire 1. Posons $L = K(\sqrt{u})$ où $u \in O_K$. Soit \mathfrak{p} un idéal premier de O_K .

- 1) Si $2u$ n'est pas dans \mathfrak{p} , alors \mathfrak{p} est non ramifié dans L .
- 2) Si u n'est pas dans \mathfrak{p} et s'il existe des éléments $b, c \in O_K$ tels que $u = b^2 - 4c$, alors \mathfrak{p} est non ramifié dans L .

Démonstration : Le discriminant de $f := X^2 - u$ est $4u$ qui n'est pas dans \mathfrak{p} , donc f est séparable modulo \mathfrak{p} , et \mathfrak{p} est non ramifié dans L . En ce qui concerne l'assertion 2 : on a $L = K(\alpha)$ où α est une racine du polynôme $X^2 + bX + c$. Son discriminant est u , qui n'est pas dans \mathfrak{p} , d'où le résultat.

On notera que la deuxième assertion n'a d'intérêt que si $2 \in \mathfrak{p}$.

Exercice 4

Soient K le corps $\mathbb{Q}(i)$ et $L = K(\alpha)$ où α est une racine du polynôme $X^4 - 2 \in K[X]$. Montrer que L/K est une extension galoisienne de degré 4 qui est non ramifiée en tout idéal premier de $\mathbb{Z}[i]$ distinct de celui au-dessus de 2.

2. Extensions non ramifiées

Soient K un corps de nombres et L/K une extension finie de K . Il existe un idéal $\mathfrak{D}_{L/K}$ de O_L , appelé la différentielle de l'extension L/K , qui est tel que ses diviseurs premiers soient exactement les idéaux premiers de O_L qui sont ramifiés dans L/K . C'est le plus grand commun diviseur de tous les idéaux de la forme $f'(\alpha)O_L$, où $\alpha \in O_L$ est un élément primitif de L/K et où $f \in K[X]$ est le polynôme minimal de α sur K (cf. [La], p. 62). Soient \mathfrak{P}_i ($1 \leq i \leq t$) les diviseurs premiers de $\mathfrak{D}_{L/K}$. Posons

$$\mathfrak{D}_{L/K} = \prod_{i=1}^t \mathfrak{P}_i^{m_i} \quad \text{avec} \quad m_i \geq 1.$$

Soit e_i l'indice de ramification de \mathfrak{P}_i sur K . On a alors $m_i \geq e_i - 1$. De plus, $m_i = e_i - 1$ si et seulement si e_i est premier à la caractéristique résiduelle de \mathfrak{P}_i .

Il se trouve dans [Coh] p. 204 un algorithme permettant de déterminer $\mathfrak{D}_{K/\mathbb{Q}}$. La norme de K sur \mathbb{Q} de $\mathfrak{D}_{K/\mathbb{Q}}$ est $|D_K|$. On a la formule de transitivité suivante :

$$\mathfrak{D}_{L/\mathbb{Q}} = \mathfrak{D}_{L/K} \cdot \mathfrak{D}_{K/\mathbb{Q}} O_L.$$

Dans le cas où O_K est de la forme $\mathbb{Z}[\alpha]$ (auquel cas $K = \mathbb{Q}(\alpha)$), si f est le polynôme minimal de α sur \mathbb{Q} , alors $\mathfrak{D}_{K/\mathbb{Q}}$ est l'idéal de O_K engendré par $f'(\alpha)$ (cf. [Se], p. 66).

Exercice 5

Soit $\alpha \in \mathbb{C}$ une racine du polynôme $X^3 - X - 1 \in \mathbb{Z}[X]$ et K le corps $\mathbb{Q}(\alpha)$. Déterminer la différentielle $\mathfrak{D}_{K/\mathbb{Q}}$ de K sur \mathbb{Q} .

Définition 1. On dit que L/K est non ramifiée si les deux conditions suivantes sont satisfaites :

- 1) tout idéal premier de O_L est non ramifié dans L/K .
- 2) Les places à l'infini de K sont non ramifiées dans L .

La condition 2 signifie que si $\sigma : K \rightarrow \overline{\mathbb{Q}}$ est un plongement réel i.e. dont l'image est contenue dans \mathbb{R} , alors tous ses prolongements à L sont aussi réels. En particulier, si K est totalement imaginaire, cette condition est réalisée. Rappelons que la condition 1 n'est jamais satisfaite si $K = \mathbb{Q}$ et $L \neq \mathbb{Q}$. Par ailleurs, il se peut que la condition 1 soit satisfaite sans que la condition 2 le soit. Tel est le cas par exemple si $K = \mathbb{Q}(\sqrt{3})$ et $L = K(i)$.

Exercice 6

Vérifier cette dernière assertion.

Exercice 7

Soient K_1/K et K_2/K deux extensions galoisiennes finies non ramifiées. Montrer que l'extension composée K_1K_2/K est aussi non ramifiée (cet énoncé est encore vrai sans supposer que K_i/K soit galoisienne mais la démonstration est moins simple).

Exercice 8

On pose $K = \mathbb{Q}(\sqrt{-5})$ et $L = K(i)$. Démontrer que l'extension L/K est non ramifiée.

3. Nombres de classes des corps quadratiques imaginaires

La loi de réciprocité d'Artin établit un lien entre le groupe des classes d'idéaux d'un corps de nombres et son corps de classes de Hilbert. On se propose ici de donner une formule permettant de calculer le nombre de classes des corps quadratiques imaginaires, que l'on utilisera dans les exemples du paragraphe 6.

Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique imaginaire, d étant un entier < 0 sans facteurs carrés. Soit χ le caractère quadratique associé à K considéré comme une fonction définie sur \mathbb{Z} . Si $a \in \mathbb{Z}$ n'est pas premier à D_K , on a $\chi(a) = 0$. Si a est premier à D_K on a (cf. par exemple [Ribn], p. 568) :

$$\chi(a) = \begin{cases} \left(\frac{a}{|d|}\right) & \text{si } d \equiv 1 \pmod{4} \\ (-1)^{(a-1)/2} \left(\frac{a}{|d|}\right) & \text{si } d \equiv 3 \pmod{4} \\ (-1)^{(a^2-1)/8} (-1)^{(a-1)(d'-1)/4} \left(\frac{a}{|d'|}\right) & \text{si } d = 2d'. \end{cases}$$

Soit h_K le nombre de classes de K . Supposons que l'on ait $d \neq -1, -3$ (dans ces deux cas, on a $h_K = 1$). On a alors (*loc. cit.*, p. 584) :

$$(4) \quad h_K = \frac{1}{2 - \chi(2)} \sum_{1 \leq j < \frac{|D_K|}{2}} \chi(j).$$

Exercice 9

Soit $K = \mathbb{Q}(\sqrt{-5})$. Calculer le nombre de classes de K de deux façons : en utilisant la formule (4) et en utilisant le corollaire 1 p. 70 de [Sa] (toute classes d'idéaux d'un corps de nombres contient un idéal entier de norme plus petite qu'une constante explicite).

4. Substitution de Frobenius

On considère une extension galoisienne finie L/K de corps de nombres. Soient \mathfrak{P} un idéal premier de O_L et $\mathfrak{p} = \mathfrak{P} \cap O_K$. On suppose dans tout ce paragraphe que

$$(5) \quad L/K \text{ est non ramifiée en } \mathfrak{P},$$

autrement dit, que \mathfrak{p} est non ramifié dans L . Posons $k = O_K/\mathfrak{p}$ et $\ell = O_L/\mathfrak{P}$. Soit q le cardinal de k . La condition (5) entraîne que le sous-groupe de décomposition $D_{\mathfrak{P}}(L/K)$ en \mathfrak{P} de $\text{Gal}(L/K)$ est isomorphe à $\text{Gal}(\ell/k)$ via l'application

$$\varepsilon : D_{\mathfrak{P}}(L/K) \rightarrow \text{Gal}(\ell/k),$$

qui à σ associe l'homomorphisme $\bar{\sigma}$ de ℓ défini, pour $x \in O_L$, par

$$\bar{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}.$$

Le groupe $\text{Gal}(\ell/k)$ est cyclique engendré par l'application $y \mapsto y^q$, qui est l'automorphisme de Frobenius de ℓ/k . Par suite, $D_{\mathfrak{P}}(L/K)$ est aussi cyclique dont un générateur $s_{\mathfrak{P}}$ est défini par l'égalité

$$\varepsilon(s_{\mathfrak{P}}) = \{y \mapsto y^q\}.$$

Il est caractérisé par la propriété suivante (cf. l'exercice 10) :

$$(6) \quad s_{\mathfrak{P}}(x) \equiv x^q \pmod{\mathfrak{P}} \quad \text{pour tout } x \in O_L.$$

Exercice 10

Avec les hypothèses faites au début du paragraphe 4, soient s_1 et s_2 deux éléments de $\text{Gal}(L/K)$ tels que pour tout $x \in O_L$, on ait $s_1(x) \equiv s_2(x) \pmod{\mathfrak{P}}$. Montrer que $s_1 = s_2$.

Définition 2. L'élément $s_{\mathfrak{P}}$ est appelé la substitution de Frobenius en \mathfrak{P} de l'extension L/K . On le note parfois $(\mathfrak{P}, L/K)$.

Considérons une extension E de K contenue dans L (L est une extension galoisienne de E). Posons $\mathfrak{P}_E = \mathfrak{P} \cap O_E$. Soit $f_{\mathfrak{P}_E}$ le degré sur k du corps résiduel de E en l'idéal \mathfrak{P}_E . L'idéal \mathfrak{P} est non ramifié dans L/E . On peut ainsi considérer la substitution de Frobenius $(\mathfrak{P}, L/E)$ qui appartient à $D_{\mathfrak{P}}(L/K)$.

Lemme 1.

- 1) On a $(\mathfrak{P}, L/E) = (\mathfrak{P}, L/K)^{f_{\mathfrak{P}_E}}$.
- 2) Supposons E/K galoisienne. Alors, la restriction de $(\mathfrak{P}, L/K)$ à E est $(\mathfrak{P}_E, E/K)$.
- 3) Soit σ un élément de $\text{Gal}(L/K)$. On a $(\sigma(\mathfrak{P}), L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}$.

Démonstration : 1) D'après (6), pour tout $x \in O_L$ on a

$$(\mathfrak{P}, L/K)^{f_{\mathfrak{P}_E}}(x) \equiv x^{q^{f_{\mathfrak{P}_E}}} \pmod{\mathfrak{P}}.$$

Par ailleurs, on a

$$(\mathfrak{P}, L/E)(x) \equiv x^{q^{f_{\mathfrak{P}_E}}} \pmod{\mathfrak{P}}.$$

On a donc $(\mathfrak{P}, L/K)^{f_{\mathfrak{P}_E}}(x) \equiv (\mathfrak{P}, L/E)(x) \pmod{\mathfrak{P}}$, d'où l'assertion 1.

2) On remarque d'abord que la restriction de $(\mathfrak{P}, L/K)$ à E est un élément du sous-groupe de décomposition $D_{\mathfrak{P}_E}(E/K)$ de $\text{Gal}(E/K)$. Pour tout $x \in O_E$, on a

$$(\mathfrak{P}, L/K)(x) \equiv x^q \pmod{\mathfrak{P}_E} \quad (\mathfrak{P}_E = \mathfrak{P} \cap O_E).$$

La congruence

$$(\mathfrak{P}_E, E/K)(x) \equiv x^q \pmod{\mathfrak{P}_E},$$

entraîne alors résultat.

- 3) Pour tout $x \in O_L$, on a

$$(\mathfrak{P}, L/K)\sigma^{-1}(x) \equiv \sigma^{-1}(x)^q \pmod{\mathfrak{P}},$$

ce qui implique

$$\sigma(\mathfrak{P}, L/K)\sigma^{-1}(x) \equiv x^q \pmod{\sigma(\mathfrak{P})},$$

et l'assertion 3.

Supposons de plus l'extension L/K abélienne. D'après l'assertion 3 du lemme et le fait que $\text{Gal}(L/K)$ opère transitivement sur l'ensemble des idéaux premiers de O_L au-dessus de \mathfrak{p} , la substitution de Frobenius $(\mathfrak{P}, L/K)$ ne dépend dans ce cas que de \mathfrak{p} . On la note alors $(\mathfrak{p}, L/K)$, et on l'appelle le symbole d'Artin de \mathfrak{p} ou la substitution de Frobenius en \mathfrak{p} de L/K . C'est l'élément trivial de $\text{Gal}(L/K)$ si et seulement si \mathfrak{p} est totalement décomposé dans L : c'est une conséquence directe du fait que $(\mathfrak{p}, L/K)$ est un générateur de $D_{\mathfrak{P}}(L/K)$ et que si g est le nombre d'idéaux premiers de O_L au-dessus de \mathfrak{p} , on a $[L : K] = g|D_{\mathfrak{P}}(L/K)|$. Signalons que tout élément de $\text{Gal}(L/K)$ est de la forme $(\mathfrak{p}, L/K)$ pour une infinité d'idéaux premiers \mathfrak{p} de O_K (c'est un cas particulier du théorème de densité de Chebotarev (cf. par exemple [Cox], p. 168)).

Application (Loi de réciprocité quadratique)

Donnons ici une démonstration de la loi de réciprocité quadratique (cf. [Sa], p. 109). Rappelons que si p est un nombre premier impair, pour tout entier a premier à p , le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut 1 si a est un carré modulo p , et -1 sinon. On a

$$(7) \quad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Il s'agit de démontrer l'énoncé suivant :

Théorème 3. *Soient p et q deux nombres premiers impairs distincts. On a l'égalité*

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

Démonstration : Soit ζ une racine primitive q -ième de l'unité. Posons $K = \mathbb{Q}(\zeta)$. Le groupe de Galois de K sur \mathbb{Q} est cyclique isomorphe à \mathbb{F}_q^* , via l'application j définie, pour tout $\sigma \in \text{Gal}(K/\mathbb{Q})$, par l'égalité

$$\sigma(\zeta) = \zeta^{j(\sigma)}.$$

Il existe ainsi un unique corps quadratique F contenu dans K , le groupe $\text{Gal}(K/F)$ étant isomorphe via j au sous-groupe des carrés de \mathbb{F}_q^* . Tous les nombres premiers autres que q sont non ramifiés dans K . Par suite, on a

$$F = \mathbb{Q}(\sqrt{q^*}) \text{ où } q^* = (-1)^{\frac{q-1}{2}} q.$$

Posons $\sigma_p = (p, K/\mathbb{Q}) \in \text{Gal}(K/\mathbb{Q})$. On a

$$(8) \quad \sigma_p(\zeta) = \zeta^p \quad \text{i.e.} \quad j(\sigma_p) = p \pmod{q}.$$

En effet, soit \mathfrak{P} un idéal premier de l'anneau d'entiers de $\mathbb{Q}(\zeta)$ au-dessus de p : d'après (6), on a $\sigma_p(\zeta) \equiv \zeta^p \pmod{\mathfrak{P}}$. Par ailleurs, il existe j tel que $\sigma_p(\zeta) = \zeta^j$. Si $j \not\equiv p \pmod{q}$, on

a $\zeta^j - \zeta^p = (\zeta - 1)u$ où u est une unité de O_K . Il en résulte que $\zeta - 1$ appartient à \mathfrak{P} , et \mathfrak{P} est donc l'unique idéal premier de O_K au-dessus de q , d'où $p = q$ et une contradiction. On déduit alors de (8) que σ_p appartient à $\text{Gal}(K/F)$ si et seulement si $p \bmod q$ est un carré. D'après le lemme 1, la restriction de σ_p à F est $(p, F/\mathbb{Q})$. En identifiant $\text{Gal}(F/\mathbb{Q})$ à $\{\pm 1\}$, on a donc l'égalité

$$(p, F/\mathbb{Q}) = \left(\frac{p}{q}\right).$$

Par ailleurs, on a $(p, F/\mathbb{Q}) = 1$ si et seulement si p est totalement décomposé dans F i.e. si q^* est un carré modulo p . On en déduit que

$$(p, F/\mathbb{Q}) = \left(\frac{q^*}{p}\right).$$

On obtient ainsi

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

D'après (7), on a $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. L'égalité

$$\left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right),$$

entraîne alors le résultat.

Exercice 11

Démontrer que si p est un nombre premier impair, on a

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

5. Corps de classes de Hilbert - Théorème de réciprocité

Soit K un corps de nombres.

Théorème 4. *Il existe une unique extension finie H de K possédant les deux propriétés suivantes :*

- 1) *H est une extension abélienne non ramifiée de K .*
- 2) *Toute extension abélienne non ramifiée de K est contenue dans H .*

Définition 3. *Le corps H est appelé le corps de classes de Hilbert de K .*

Par définition, H est l'extension abélienne non ramifiée maximale de K . Puisque l'extension H/K est finie, il n'existe pas d'extensions abéliennes non ramifiées de K de

degrés sur K arbitrairement grands. La condition "extension abélienne" est essentielle. En effet, il existe des corps de nombres ayant des extensions non ramifiées de degrés arbitrairement grands. Tel est le cas par exemple des corps $\mathbb{Q}(\sqrt{-30030})$ et $\mathbb{Q}(\sqrt{9699690})$ (cf. [Ro]).

Le groupe de Galois $\text{Gal}(H/K)$ est en fait canoniquement isomorphe au groupe des classes d'idéaux $Cl(K)$ de K . Plus précisément, soit I_K le groupe des idéaux fractionnaires non nuls de K . Pour tout $\mathfrak{b} \in I_K$ il existe des idéaux premiers \mathfrak{p} de O_K et des entiers $n_{\mathfrak{p}} \in \mathbb{Z}$ (presque tous nuls) tels que

$$\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}.$$

On définit alors le symbole d'Artin $(\mathfrak{b}, H/K)$ de \mathfrak{b} comme étant

$$(\mathfrak{b}, H/K) = \prod_{\mathfrak{p}} (\mathfrak{p}, H/K)^{n_{\mathfrak{p}}} \in \text{Gal}(H/K).$$

Cela permet de définir un homomorphisme de groupes,

$$\varphi_K : I_K \rightarrow \text{Gal}(H/K),$$

qui à \mathfrak{b} associe $(\mathfrak{b}, H/K)$. Le théorème de réciprocité d'Artin dans le cas des corps de classes de Hilbert est le suivant :

Théorème 5. *L'homomorphisme φ_K est surjectif de noyau le sous-groupe des idéaux fractionnaires principaux. Passé au quotient, φ_K réalise ainsi un isomorphisme de $Cl(K)$ sur $\text{Gal}(H/K)$.*

Le fait que φ_K soit surjectif résulte du théorème de densité de Chebotarev. Notons encore φ_K l'isomorphisme de $Cl(K)$ sur $\text{Gal}(H/K)$ ainsi défini. Il résulte directement du théorème de correspondance de Galois que l'ensemble des extensions abéliennes non ramifiées de K est en bijection avec l'ensemble des sous-groupes de $Cl(K)$, via l'application ψ_K définie par

$$\psi_K(M) = \varphi_K^{-1}(\text{Gal}(H/M)).$$

De plus, si M est un sous-corps de H contenant K , l'homomorphisme $Cl(K) \rightarrow \text{Gal}(M/K)$ obtenu en composant la restriction avec φ_K , est surjectif de noyau $\varphi_K^{-1}(\text{Gal}(H/M))$. Ainsi, φ_K induit un isomorphisme de $Cl(K)/\psi_K(M)$ sur $\text{Gal}(M/K)$.

Proposition. *Soit \mathfrak{p} un idéal premier de O_K . Alors, \mathfrak{p} est totalement décomposé dans H si et seulement si \mathfrak{p} est un idéal principal.*

Démonstration : Dire que \mathfrak{p} est totalement décomposé dans H signifie que la substitution de Frobenius en \mathfrak{p} dans H/K est triviale, autrement dit que \mathfrak{p} est dans le noyau de φ_K i.e. que \mathfrak{p} est principal (d'après le théorème de réciprocité). D'où l'assertion.

6. Exemples

Pour certains corps K , on va donner dans ce paragraphe des exemples de détermination du corps de classes de Hilbert H de K .

1) Tout d'abord, si O_K est principal, alors $H = K$.

2) Supposons $K = \mathbb{Q}(\sqrt{-5})$. On vérifie que le nombre de classes de K est 2 (exercice 9). Par suite, H est une extension quadratique de K . D'après l'exercice 8, on a donc $H = K(i)$.

3) Supposons $K = \mathbb{Q}(\sqrt{-14})$ (cf. [Cox], p. 113). Dans ce cas, on vérifie que $h_K = 4$ (cf. formule (4)). On a donc $[H : K] = 4$. Posons $f = X^4 + 2X^2 - 7 \in \mathbb{Q}[X]$. Soit $\alpha \in \mathbb{C}$ une racine de f . Démontrons que l'on a $H = K(\alpha)$.

3.1) Posons $L = K(\alpha)$. On a $[L : K] = 4$. En effet, soit \mathfrak{p} un idéal premier de O_K au-dessus de 3. Puisque 3 est décomposé dans K (formule (1)), O_K/\mathfrak{p} est isomorphe à \mathbb{F}_3 et l'on vérifie que f est irréductible modulo 3. En particulier, f est irréductible sur K , d'où l'assertion.

3.2) Vérifions que L/K est une extension abélienne de degré 4. Il suffit pour cela de démontrer que L est le corps de décomposition de f sur K . Soit β une racine de f autre que $\pm\alpha$. On a $(\alpha\beta)^2 = -7$, donc le corps de décomposition de f sur K est $K(\alpha, \sqrt{-7})$. Par ailleurs, on a $\alpha^2 = \pm 2\sqrt{2} - 1$. Il en résulte que $\sqrt{2}$ appartient à $K(\alpha)$, ce qui entraîne que $\sqrt{-7}$ est aussi dans $K(\alpha)$, puis l'assertion.

3.3) Démontrons que L/K est non ramifiée. Puisque K est totalement imaginaire, il suffit de prouver que L/K est non ramifiée en tous les idéaux premiers de O_K . Posons $K_1 = K(\sqrt{2})$. On a les inclusions $K \subseteq K_1 \subseteq L$, de sorte qu'il suffit de vérifier que les extensions quadratiques K_1/K et L/K_1 sont non ramifiées.

Vérifions que K_1/K est non ramifiée. Soit \mathfrak{p} un idéal premier de O_K . D'après l'assertion 1 du corollaire 1, \mathfrak{p} est non ramifié dans K_1 si 2 n'est pas dans \mathfrak{p} . Supposons que \mathfrak{p} soit au-dessus de 2. On utilise dans ce cas le fait $K_1 = K(\sqrt{-7})$. Parce que -7 n'est pas dans \mathfrak{p} et que $-7 = 1 - 4 \times 2$, le corollaire 1 entraîne de nouveau que \mathfrak{p} est non ramifié dans K_1 , d'où l'assertion.

Vérifions que L/K_1 est non ramifiée. Posons

$$\mu = 2\sqrt{2} - 1 \quad \text{et} \quad \mu' = -2\sqrt{2} - 1.$$

On a les égalités $L = K_1(\sqrt{\mu}) = K_1(\sqrt{\mu'})$. Soit alors \mathfrak{P} un idéal premier de O_{K_1} . Si 2 n'est pas dans \mathfrak{P} , on déduit de l'égalité $\mu + \mu' = -2$ que μ ou μ' n'est pas dans \mathfrak{P} et donc que \mathfrak{P} est non ramifié dans L . Si 2 est dans \mathfrak{P} , alors μ n'est pas dans \mathfrak{P} car $\mu = 2\sqrt{2} - 1$. Par ailleurs, on a $\mu = (1 + \sqrt{2})^2 - 4$, et \mathfrak{P} est donc non ramifié dans L .

Il résulte de ce qui précède que L est contenu dans H . Les extensions H/K et L/K étant de même degré, on a donc $H = L$.

4) Supposons $K = \mathbb{Q}(\sqrt{-31})$. On pose $f = X^3 + X + 1 \in \mathbb{Q}[X]$. Soit $\alpha \in \mathbb{C}$ une racine de f . On va démontrer que l'on a $H = K(\alpha)$.

On vérifie d'abord par la formule (4) que $h_K = 3$, de sorte que H est une extension de degré 3 de K . Tout revient donc à prouver que $K(\alpha)/K$ est une extension abélienne de degré 3 non ramifiée.

4.1) Posons $L = K(\alpha)$. Si \mathfrak{p} est l'un des deux idéaux premiers de O_K au-dessus de 2, O_K/\mathfrak{p} est isomorphe à \mathbb{F}_2 et f est irréductible modulo 2, donc f est irréductible sur K . Par ailleurs, le discriminant $\Delta(f)$ de f est -31 . Ainsi, L est le corps de décomposition de f sur K et L/K est abélienne de degré 3.

4.2) Vérifions que L/K est non ramifiée. Tel est le cas aux places à l'infini. Notons \mathfrak{p}_{31} l'idéal premier de O_K au-dessus de 31. Pour tout idéal premier \mathfrak{p} de O_K autre que \mathfrak{p}_{31} , f est séparable modulo \mathfrak{p} . D'après le théorème 2, L/K est donc non ramifiée en dehors de \mathfrak{p}_{31} . Il reste à montrer que \mathfrak{p}_{31} est non ramifié dans L . Supposons le contraire. Dans ce cas, L/K étant galoisienne de degré 3, \mathfrak{p}_{31} est totalement ramifié dans L et il existe un unique idéal premier de O_L au-dessus de \mathfrak{p}_{31} . En particulier, il existe un unique idéal premier dans O_L au-dessus de 31. Par ailleurs, $\Delta(f)$ étant sans facteurs carrés, l'anneau d'entiers de $\mathbb{Q}(\alpha)$ est $\mathbb{Z}[\alpha]$ (cf. [Sa], p. 90). La factorisation de f dans $\mathbb{F}_{31}[X]$ étant $(X + 17)^2(X - 3)$, on déduit alors du théorème 1 qu'il existe deux idéaux premiers dans $\mathbb{Z}[\alpha]$ au-dessus de 31. D'où une contradiction et le résultat.

Exercice 12

Soit K le corps $\mathbb{Q}(\sqrt{10})$.

- 1) Calculer le nombre de classes de K .
- 2) Déterminer son corps de classes de Hilbert.

Signalons que si K est un corps quadratique, il est implanté dans le logiciel de calculs Pari ([Pa]), un programme qui fournit un élément primitif de H sur K . Si K est imaginaire, la description générale de H est liée à la théorie de la multiplication complexe et des formes modulaires (cf. par exemple [Coh], [Cox]). Si K est réel, cette description utilise la théorie des unités de Stark (cf. [Coh-Rob]). Dans le cas particulier où le nombre de classes de K est 2, on peut démontrer, si K réel, qu'il existe un diviseur d de D_K , avec $1 < d < D_K$ et $d \equiv 0, 1 \pmod{4}$, tel que $H = K(\sqrt{d})$. La détermination de H se réduit alors à l'examen d'un nombre fini de possibilités (cf. *loc. cit.*).

7. Applications

Soit $n \geq 1$ un entier sans facteurs carrés. Comme conséquence de ce qui précède, on s'intéresse ici à la description des nombres premiers impairs p qui peuvent s'écrire sous la forme $p = x^2 + ny^2$, avec x et y dans \mathbb{Z} . Si $n = 1$, Fermat a démontré que tel est le cas si et seulement si $p \equiv 1 \pmod{4}$. Posons $K = \mathbb{Q}(\sqrt{-n})$ et notons H le corps de classes de Hilbert de K . On va prouver ici le résultat suivant (cf. [Cox], p. 110) :

Théorème 6. *Supposons $n \not\equiv 3 \pmod{4}$. Soit p un nombre premier impair ne divisant pas n . Alors, il existe $x, y \in \mathbb{Z}$ tels que $p = x^2 + ny^2$ si et seulement si p est totalement décomposé dans H .*

Démonstration : Démontrons que les conditions suivantes sont équivalentes, ce qui prouvera le résultat :

- (i) il existe $x, y \in \mathbb{Z}$ tels que $p = x^2 + ny^2$;
- (ii) on a $pO_K = \mathfrak{p}_1\mathfrak{p}_2$ où \mathfrak{p}_i est premier, $\mathfrak{p}_1 \neq \mathfrak{p}_2$ et \mathfrak{p}_1 est principal ;
- (iii) on a $pO_K = \mathfrak{p}_1\mathfrak{p}_2$ où \mathfrak{p}_i est premier, $\mathfrak{p}_1 \neq \mathfrak{p}_2$ et \mathfrak{p}_1 est totalement décomposé dans H ;
- (iv) p est totalement décomposé dans H .

(i) \iff (ii) : supposons (i) réalisée. On a l'égalité

$$p = (x + \sqrt{-ny})(x - \sqrt{-ny}).$$

Posons $\mathfrak{p}_1 = (x + \sqrt{-ny})O_K$ et $\mathfrak{p}_2 = (x - \sqrt{-ny})O_K$. On a alors $pO_K = \mathfrak{p}_1\mathfrak{p}_2$ et \mathfrak{p}_i est distinct de O_K . Le corps K étant de degré 2 sur \mathbb{Q} , les idéaux \mathfrak{p}_i sont donc premiers. Puisque p est impair et ne divise pas n , p est non ramifié dans K , donc $\mathfrak{p}_1 \neq \mathfrak{p}_2$. D'où la condition (ii). Inversement, parce que $n \not\equiv 3 \pmod{4}$, on a $O_K = \mathbb{Z}[\sqrt{-n}]$. Puisque \mathfrak{p}_1 est principal, il existe donc $x, y \in \mathbb{Z}$ tels que $\mathfrak{p}_1 = (x + \sqrt{-ny})O_K$. Les idéaux \mathfrak{p}_1 et \mathfrak{p}_2 étant distincts et conjugués par le groupe de Galois de K sur \mathbb{Q} , on a $\mathfrak{p}_2 = (x - \sqrt{-ny})O_K$. Il en résulte que l'on a $pO_K = (x^2 + ny^2)O_K$, d'où $p = x^2 + ny^2$ et la condition (i).

(ii) \iff (iii) : cette équivalence résulte directement de la proposition p. 12.

(iii) \iff (iv) : on utilise le lemme suivant :

Lemme 2. *Le corps de classes de Hilbert d'un corps de nombres galoisien sur \mathbb{Q} est galoisien sur \mathbb{Q} .*

Démonstration : Soient M une extension galoisienne de \mathbb{Q} et L son corps de classes de Hilbert. Soit σ un plongement de L dans \mathbb{C} . Par transport de structure, le corps $\sigma(L)$ est une extension abélienne non ramifiée de $\sigma(M)$. Puisque M est galoisien sur \mathbb{Q} , on a $\sigma(M) = M$. Il en résulte que $\sigma(L)$ est contenu dans L , puis que $\sigma(L) = L$. D'où le résultat.

Supposons alors la condition (iii) satisfaite. Il existe alors un idéal premier de O_H au-dessus de p , qui est non ramifié et de degré résiduel 1 sur p . L'extension H/\mathbb{Q} étant galoisienne (lemme 2), il en est de même pour tous les idéaux premiers de O_H au-dessus de p . Cela entraîne que p est totalement décomposé dans H . L'implication réciproque est immédiate. D'où le théorème.

Indiquons les deux conséquences suivantes :

Corollaire 2. *Soit p un nombre premier distinct de 5. Les conditions suivantes sont équivalentes :*

- (i) il existe $x, y \in \mathbb{Z}$ tels que $p = x^2 + 5y^2$;
(ii) on a $p \equiv 1, 9 \pmod{20}$.

Démonstration : Le corps de classes de Hilbert de $\mathbb{Q}(\sqrt{-5})$ est $H = \mathbb{Q}(i, \sqrt{-5})$. Ainsi, p est décomposé dans H si et seulement tel est le cas dans $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{-5})$ (justifier cette assertion). On déduit alors du théorème que p est représenté par la forme $x^2 + 5y^2$ si et seulement si $\left(\frac{-5}{p}\right) = 1$ et $\left(\frac{-1}{p}\right) = 1$, ce qui entraîne le résultat.

Corollaire 3. Soit p un nombre premier. Les conditions suivantes sont équivalentes :

- (i) il existe $x, y \in \mathbb{Z}$ tels que $p = x^2 + 14y^2$;
(ii) on a $\left(\frac{-14}{p}\right) = 1$ et le polynôme $(X^2 + 1)^2 - 8 \in \mathbb{Z}[X]$ a une racine modulo p .

Démonstration : On peut supposer que p ne divise pas 14. On a vu que le corps de classes de Hilbert H de $K = \mathbb{Q}(\sqrt{-14})$ est $K(\alpha)$ où $\alpha \in \mathbb{C}$ est une racine de $f := (X^2 + 1)^2 - 8$, qui est le polynôme minimal de α sur K . Il s'agit de vérifier que la condition (ii) caractérise les nombres premiers p totalement décomposés dans H . Supposons p totalement décomposé dans H . On a alors $\left(\frac{-14}{p}\right) = 1$ et si \mathfrak{p} est un idéal premier de O_K au-dessus de p , O_K/\mathfrak{p} est isomorphe à \mathbb{F}_p . Le discriminant de f étant $-2^{14}7$, il en résulte que f est séparable modulo \mathfrak{p} . Puisque \mathfrak{p} est totalement décomposé dans H , on déduit du théorème 2 que f a une racine modulo p , d'où la condition (ii). Inversement, supposons cette condition réalisée. Puisque $\left(\frac{-14}{p}\right) = 1$, p est décomposé dans K . Si \mathfrak{p} est un idéal premier de O_K au-dessus de p , f modulo \mathfrak{p} est séparable et d'après l'hypothèse faite f a une racine modulo \mathfrak{p} . D'après le théorème 2, \mathfrak{p} est donc totalement décomposé dans H et tel est aussi le cas de p . D'où le corollaire.

Exercice 13

Déterminer les nombres premiers p tels que $\left(\frac{-14}{p}\right) = 1$.

Chapitre II — Le théorème de Kummer (exercices)

Dans tout ce chapitre p est un nombre premier impair. Soit ζ une racine primitive p -ième de l'unité. On pose $K = \mathbb{Q}(\zeta)$. Par définition, p est dit régulier s'il ne divise pas le nombre de classes de K . On fournit ci-dessous une démonstration, sous forme d'exercices, du théorème de Kummer sur l'équation de Fermat. Rappelons son énoncé :

Théorème. *Supposons que p soit régulier. Soient x, y et z des éléments de K tels que $x^p + y^p = z^p$. Alors, on a $xyz = 0$.*

Le corps K est une extension galoisienne de \mathbb{Q} de degré $p - 1$ dont le groupe de Galois est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$. On notera dans toute la suite A l'anneau d'entiers de K . On a

$$A = \mathbb{Z}[\zeta].$$

Le discriminant de K est $(-1)^{(p-1)/2}p^{p-2}$, en particulier, p est le seul nombre premier ramifié dans K . Par ailleurs, il existe un unique idéal premier \mathfrak{P} dans A au-dessus de p et l'on a

$$pA = \mathfrak{P}^{p-1} \quad \text{et} \quad \mathfrak{P} = (1 - \zeta)A.$$

On posera désormais $\lambda = 1 - \zeta$ et l'on notera $v_{\mathfrak{P}}$ la valuation \mathfrak{P} -adique de K associée à \mathfrak{P} : on a $v_{\mathfrak{P}}(\lambda) = 1$ et $v_{\mathfrak{P}}(p) = p - 1$.

Énoncés des exercices

Puisque K est le corps des fractions de A , il convient de remarquer au départ que pour démontrer le théorème, on peut se limiter au cas où x, y et z sont des éléments de A .

1. Exercices préliminaires

Exercice 1

Un élément $x \in A$ est dit semi-primaire si les deux conditions suivantes sont réalisées :

- (i) x n'est pas dans \mathfrak{P} ;
 - (ii) il existe $m \in \mathbb{Z}$ tel que $x \equiv m \pmod{\mathfrak{P}^2}$.
- 1) Soit x un élément de A qui n'est pas dans \mathfrak{P} . Montrer qu'il existe un entier naturel r , unique modulo p , tel que $\zeta^r x$ soit semi-primaire.
 - 2) Soient x et y des éléments de A semi-primaires. Montrer que xy est semi-primaire et qu'il existe $m \in \mathbb{Z}$ tel que $x \equiv my \pmod{\mathfrak{P}^2}$.

Exercice 2

Soient x, y et z des éléments de A tels que

$$x^p + y^p = z^p.$$

Posons

$$I = \text{pgcd}\left((x + \zeta^k y)A\right) \quad \text{pour } k = 0, \dots, p-1.$$

1) Montrer que pour tous j et k tels que $0 \leq j < k \leq p-1$, on a

$$(1) \quad I = \text{pgcd}\left((x + \zeta^j y)A, (x + \zeta^k y)A\right).$$

2) En déduire qu'il existe des idéaux J_k de A , premiers entre eux deux à deux, tels que

$$(2) \quad (x + \zeta^k y)A = J_k^p I \quad \text{pour } k = 0, \dots, p-1.$$

Exercice 3

Soient x, y, z et u des éléments de A tels que

$$x^p + y^p = uz^p, \quad uxy \not\equiv 0 \pmod{\mathfrak{P}} \quad \text{et} \quad z \equiv 0 \pmod{\mathfrak{P}}.$$

Montrer que z appartient à \mathfrak{P}^2 .

Exercice 4

Soient u une unité de A et x, y, z des éléments de A vérifiant la condition suivante :

$$x^p + y^p = uz^p, \quad xy \not\equiv 0 \pmod{\mathfrak{P}}, \quad z \neq 0 \quad \text{et} \quad z \equiv 0 \pmod{\mathfrak{P}}.$$

Posons

$$v_{\mathfrak{P}}(z) = m \quad \text{et} \quad I' = \text{pgcd}(xA, yA).$$

1) Montrer que pour tout j tel que $0 \leq j \leq p-1$, $x + \zeta^j y$ appartient à \mathfrak{P} .

2) Montrer qu'il existe un entier j_0 avec $0 \leq j_0 \leq p-1$, tel que

$$v_{\mathfrak{P}}(x + \zeta^{j_0} y) = p(m-1) + 1 \quad \text{et} \quad v_{\mathfrak{P}}(x + \zeta^j y) = 1 \quad \text{si } j \neq j_0.$$

3) En déduire qu'il existe des idéaux I_0, \dots, I_{p-1} de A , premiers entre eux deux à deux et non divisibles par \mathfrak{P} , tels que l'on ait

$$(1) \quad (x + \zeta^{j_0} y)A = \mathfrak{P}^{p(m-1)+1} I' I_{j_0}^p \quad \text{et} \quad (x + \zeta^j y)A = \mathfrak{P} I_j^p \quad \text{si } j \neq j_0.$$

2. Lemmes de Kummer sur les unités

L'objectif de cette partie est de démontrer deux résultats dus à Kummer concernant les unités de A . Dans la démonstration de celui qui suit, on va utiliser le théorème de réciprocité d'Artin pour les corps de classes de Hilbert.

Proposition 1. *Supposons que p soit régulier. Soient u une unité de A et m un entier relatif tels que $u \equiv m \pmod{pA}$. Alors, u est une puissance p -ième dans A .*

Démontrons cet énoncé.

Exercice 5

Soit u une unité de A vérifiant l'hypothèse faite ci-dessus.

On supposera dans la suite que l'on a

$$(1) \quad u \equiv 1 \pmod{pA}.$$

- 1) Montrer que la condition (1) n'est pas restrictive.
- 2) Calculer la norme de K sur \mathbb{Q} de u . En déduire que l'on a $u \equiv 1 \pmod{\lambda^p A}$.

Supposons désormais que u ne soit pas une puissance p -ième dans K . Soit $u^{1/p}$ une racine p -ième de u dans \mathbb{C} . Posons $L = K(u^{1/p})$.

- 3) Montrer que L/K est une extension abélienne de degré p , qui est non ramifiée en dehors de \mathfrak{P} , y compris aux places à l'infini.
- 4) On considère le polynôme

$$f = \frac{(\lambda X - 1)^p + u}{\lambda^p} \in K[X].$$

- 4.1) Vérifier que f est un polynôme unitaire à coefficients dans A .
- 4.2) Soit $\alpha \in \mathbb{C}$ une racine de f . Vérifier que l'on a $L = K(\alpha)$.
- 5) Montrer alors que l'extension L/K est non ramifiée en \mathfrak{P} .
- 6) En déduire une contradiction, puis la proposition 1.

Le résultat que l'on va démontrer maintenant est valable que p soit ou non régulier. On note B l'anneau d'entiers du corps $\mathbb{Q}(\zeta + \zeta^{-1})$, qui est le sous-corps totalement réel maximal de K .

Proposition 2. *Toute unité de A est le produit d'une puissance de ζ par une unité de B .*

Sa démonstration fait l'objet de l'exercice 6.

Exercice 6

- 1) Soit $\alpha \in \mathbb{C}$ un entier algébrique dont tous les conjugués sur \mathbb{Q} sont de module 1. Montrer que α est une racine de l'unité.
- 2) Montrer que les seules racines de l'unité contenues dans K sont les racines $2p$ -ièmes de l'unité.
- 3) Vérifier que la conjugaison complexe, qui à $z \in \mathbb{C}$ associe le conjugué complexe de z , induit un automorphisme τ de K .
- 4) Soit u une unité de A . On pose

$$\alpha = \frac{u}{\tau(u)}.$$

Montrer qu'il existe un entier $a \in \mathbb{Z}$ tel que l'on ait $\alpha = \pm \zeta^a$.

- 5) En considérant les images de u et $\tau(u)$ par la surjection canonique $A \rightarrow A/\mathfrak{P}$, montrer que l'on a en fait $\alpha = \zeta^a$.
- 6) En déduire la proposition 2.

Remarque. Une unité de A est semi-primaire si et seulement si elle appartient à B . Démontrer cette assertion en utilisant la proposition 2 et le fait que l'on a $B = \mathbb{Z}[\zeta + \zeta^{-1}]$ ([Wa], p. 16).

3. Démonstration du premier cas

On suppose dans cette partie qu'il existe trois éléments x, y et z de A tels que

$$(1) \quad x^p + y^p = z^p \quad \text{et} \quad xyz \not\equiv 0 \pmod{\mathfrak{P}}.$$

Démontrer le premier cas du théorème consiste à obtenir une contradiction.

Exercice 7

Démontrer le premier cas du théorème si $p = 3$ et $p = 5$.

On peut donc supposer dans la suite de ce paragraphe que l'on a $p \geq 7$.

Exercice 8

Montrer que pour tout $j = 0, \dots, p-1$, il existe une unité ω_j de A et des éléments μ_j et $\nu_j \in A$, non divisibles par λ , tels que l'on ait

$$\frac{x + \zeta^j y}{x + \zeta^{p-1} y} = \omega_j \left(\frac{\mu_j}{\nu_j} \right)^p.$$

Le fait que z ne soit pas dans \mathfrak{P} (condition (1)) entraîne qu'il en est de même de $x + \zeta^{p-1}y$. D'après l'exercice 1, il existe donc $h \in \mathbb{Z}$ tel que $\zeta^h(x + \zeta^{p-1}y)$ soit semi-primaire. Par ailleurs, d'après la proposition 2, pour tout $j = 0, \dots, p-1$, il existe une unité réelle $\varepsilon_j \in B$ et $c_j \in \mathbb{Z}$ tels que l'on ait

$$(2) \quad \zeta^{-h}\omega_j = \varepsilon_j \zeta^{c_j}.$$

On note $A_{\mathfrak{P}}$ le localisé de A en \mathfrak{P} .

Exercice 9

Soit τ la conjugaison complexe du groupe de Galois de K sur \mathbb{Q} . Posons

$$x' = \frac{x}{\zeta^h(x + \zeta^{p-1}y)} \quad \text{et} \quad y' = \frac{y}{\zeta^h(x + \zeta^{p-1}y)}.$$

Ce sont des éléments de $A_{\mathfrak{P}}$. Montrer que pour tout entier $j = 0, \dots, p-1$, on a

$$x' + \zeta^j y' \equiv \zeta^{2c_j} (\tau(x') + \zeta^{-j} \tau(y')) \pmod{\lambda^p A_{\mathfrak{P}}}.$$

Puisque xy n'est pas dans \mathfrak{P} , quitte à multiplier x et y par des puissances de ζ convenables, on supposera désormais que x et y sont semi-primaires : cette hypothèse n'est pas restrictive pour contredire la condition (1). L'entier $\zeta^h(x + \zeta^{p-1}y)$ étant semi-primaire, il existe donc a et b dans \mathbb{Z} tels que l'on ait (exercice 1)

$$(3) \quad x \equiv a \zeta^h(x + \zeta^{p-1}y) \pmod{\mathfrak{P}^2} \quad \text{et} \quad y \equiv b \zeta^h(x + \zeta^{p-1}y) \pmod{\mathfrak{P}^2}.$$

On a ainsi

$$(4) \quad x' \equiv a \pmod{\mathfrak{P}^2 A_{\mathfrak{P}}} \quad \text{et} \quad y' \equiv b \pmod{\mathfrak{P}^2 A_{\mathfrak{P}}}.$$

Exercice 10

- 1) Montrer que l'on a $a + b \equiv 1 \pmod{p}$.
- 2) Soit j un entier tel que $0 \leq j \leq p-1$. Montrer que l'on a $c_j \equiv jb \pmod{p}$.

Il résulte des exercices 9 et 10 l'existence d'éléments $\rho_j \in A_{\mathfrak{P}}$ tels que l'on ait

$$(5) \quad x' + \zeta^j y' - \zeta^{2jb} \tau(x') - \zeta^{2jb-j} \tau(y') = \rho_j \lambda^p \quad \text{pour} \quad j = 0, \dots, p-1.$$

En explicitant (5) avec $j = 0, \dots, 3$, on obtient un système linéaire en les inconnues $x', y', \tau(x')$ et $\tau(y')$, ayant pour matrice

$$M = \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & \zeta & -\zeta^{2b} & -\zeta^{2b-1} \\ 1 & \zeta^2 & -\zeta^{4b} & -\zeta^{4b-2} \\ 1 & \zeta^3 & -\zeta^{6b} & -\zeta^{6b-3} \end{pmatrix}.$$

Exercice 11

Calculer le déterminant de M et montrer qu'il est divisible dans A par λ^p .

Exercice 12

En examinant la congruence de b modulo p , en déduire le premier cas du théorème i.e. que la condition (1) est impossible.

4. Démonstration du deuxième cas

On suppose dans cette partie qu'il existe trois éléments x, y et z de A tels que

$$(1) \quad x^p + y^p = z^p, \quad xyz \neq 0 \quad \text{et} \quad xyz \equiv 0 \pmod{\mathfrak{P}}.$$

Démontrer le deuxième cas du théorème consiste à contredire cette condition.

Exercice 13

Soit S l'ensemble des entiers $n \geq 1$ vérifiant la condition suivante :

il existe a, b, c dans A et une unité $w \in A$ tels que l'on ait

$$(2) \quad a^p + b^p = w(c\lambda^n)^p \quad \text{et} \quad abc \not\equiv 0 \pmod{\mathfrak{P}}.$$

Montrer que S n'est pas vide.

L'ensemble S n'étant pas vide, il possède un plus petit élément $m \geq 1$. Soient α, β, γ des éléments de A et u une unité de A tels que

$$\alpha^p + \beta^p = u(\gamma\lambda^m)^p \quad \text{et} \quad \alpha\beta\gamma \not\equiv 0 \pmod{\mathfrak{P}}.$$

Exercice 14

Quitte à multiplier β par une racine p -ième de l'unité convenable, montrer que pour tout j tel que $1 \leq j \leq p-1$, il existe une unité $u_j \in A$ et des éléments μ_j, ν_j de A tels que

$$\nu_j^p(\alpha + \zeta^j\beta)\lambda^{p(m-1)} = u_j(\alpha + \beta)\mu_j^p \quad \text{et} \quad \mu_j\nu_j \not\equiv 0 \pmod{\mathfrak{P}}.$$

Rappelons que $1 + \zeta$ est une unité de A . On pose

$$\alpha' = \mu_1\nu_2, \quad \beta' = \mu_2\nu_1, \quad \gamma' = \nu_1\nu_2, \quad \varepsilon = -\frac{u_2}{u_1(1+\zeta)}, \quad \varepsilon' = \frac{\zeta}{u_1(1+\zeta)}.$$

Les éléments ε et ε' sont des unités de A et $\alpha'\beta'\gamma'$ n'est pas dans \mathfrak{P} .

Exercice 15

Montrer que l'on a l'égalité

$$\alpha'^p + \varepsilon\beta'^p = \varepsilon'(\gamma'\lambda^{m-1})^p.$$

Exercice 16

- 1) En utilisant la proposition 1 du paragraphe 2, montrer que ε est une puissance p -ième dans A .
- 2) En déduire une contradiction et le deuxième cas du théorème.

Cela termine la démonstration du théorème de Fermat sur K pour les nombres premiers réguliers.

5. Complément - Théorème de Vandiver

On va démontrer l'énoncé suivant dû à Vandiver ([Va]) qui est une conséquence des résultats de Kummer :

Théorème. Soient p un nombre premier régulier impair et u une unité de A . Soient x, y et z des éléments de K tels que $x^p + y^p = uz^p$. Alors, on a $xyz = 0$.

Démonstration : On peut supposer que x, y et z sont dans A . Par ailleurs, l'idéal premier \mathfrak{P} étant principal, on peut aussi supposer que au plus un de ces éléments appartient à \mathfrak{P} . On est amené à distinguer deux cas.

- 1) Supposons que z ne soit pas dans \mathfrak{P} . Il existe des entiers relatifs a, b et c tels que

$$x \equiv a \pmod{\mathfrak{P}}, \quad y \equiv b \pmod{\mathfrak{P}} \quad \text{et} \quad z \equiv c \pmod{\mathfrak{P}}.$$

On a $x^p \equiv a^p \pmod{\lambda^p}$, $y^p \equiv b^p \pmod{\lambda^p}$ et $z^p \equiv c^p \pmod{\lambda^p}$, d'où

$$a^p + b^p \equiv uc^p \pmod{\lambda^p}.$$

Puisque z n'est pas dans \mathfrak{P} , c n'est pas divisible par p et donc il existe $d \in \mathbb{Z}$ tel que $dc^p \equiv 1 \pmod{p}$. On en déduit la congruence

$$d(a^p + b^p) \equiv u \pmod{pA}.$$

D'après la proposition 1 du paragraphe 2, u est donc une puissance p -ième dans A . Soit $u_1 \in A$ tel que $u = u_1^p$. On a alors l'égalité

$$x^p + y^p = (u_1 z)^p,$$

et le théorème de Kummer entraîne $xyz = 0$, d'où le résultat dans ce cas.

2) Supposons que z soit dans \mathfrak{P} . D'après l'hypothèse faite, xy n'appartient pas à \mathfrak{P} . Si z n'est pas nul, il existe alors un plus petit entier $m \geq 1$ vérifiant la condition suivante : il existe α, β, γ dans A et une unité w de A tels que l'on ait

$$\alpha^p + \beta^p = w(\gamma\lambda^m)^p \quad \text{et} \quad \alpha\beta\gamma \not\equiv 0 \pmod{\mathfrak{P}}.$$

Il suffit alors d'utiliser, sans modification, les énoncés des exercices 14, 15 et 16 pour obtenir une contradiction.

D'où le théorème.

Chapitre III — Sur les nombres premiers réguliers

On se propose dans ce chapitre de faire quelques remarques sur l'hypothèse faite dans l'énoncé du théorème de Kummer. Il se pose naturellement le problème de savoir décider si un nombre premier p donné est régulier ou non. À travers une étude profonde du groupe des classes du corps des racines p -ièmes de l'unité, Kummer a établi plusieurs résultats très pratiques permettant de tester si tel est le cas. On va énoncer certains de ses résultats sans démonstration afin de mettre en évidence l'efficacité de son théorème. On pourra par exemple consulter à ce sujet [Bo-Sh] ou [Ribn].

1. Sur le groupe des classes de K

Soient p un nombre premier impair, ζ une racine primitive p -ième de l'unité et K le corps $\mathbb{Q}(\zeta)$. On note h le nombre de classes de K et h^+ celui de son sous-corps réel maximal K^+ .

Proposition 1. *L'entier h^+ divise h .*

Démonstration : L'extension K/K^+ étant ramifiée en l'idéal premier au-dessus de p , la proposition 1 est une conséquence directe du résultat suivant :

Proposition 2. *Soient E un corps de nombres et L/E une extension finie. On suppose que L/E ne contient pas de sous-extensions F/E abéliennes et non ramifiées avec $F \neq E$. Alors, le nombre de classes de E divise celui de L .*

Démonstration : Soit H le corps de classes de Hilbert de E . D'après l'hypothèse faite, on a l'égalité $H \cap L = E$. Il en résulte que l'extension HL/L est galoisienne de groupe de Galois isomorphe à $\text{Gal}(H/E)$ via le morphisme de restriction. Par ailleurs, l'extension HL/L est non ramifiée (justifier cette assertion aux places finies) ; en ce qui concerne les places à l'infini : soient $\sigma : L \rightarrow \mathbb{R}$ un plongement réel de L et $\tau : HL \rightarrow \mathbb{C}$ un des ses prolongements à HL . Il s'obtient en considérant la restriction de σ à E et un prolongement convenable de cette restriction à H . On en déduit que $\tau(HL)$ est contenu dans \mathbb{R} , ce qui prouve que HL/L est non ramifiée aux places à l'infini. L'extension HL/L étant abélienne et non ramifiée, HL est donc contenu dans le corps de classes de Hilbert de L . Le théorème de réciprocité d'Artin entraîne alors le résultat.

Il existe donc un entier que l'on note souvent h^- tel que l'on ait $h = h^+ h^-$. Énonçons quelques propriétés de ces deux entiers. Soient A (resp. B) l'anneau d'entiers de K (resp. de K^+) et A^* (resp. B^*) son groupe des unités.

1.1. Le facteur h^+

Il est en fait beaucoup plus difficile à calculer que h^- . Il est lié à l'étude du groupe B^* . D'après le théorème des unités de Dirichlet, B^* est isomorphe à $\{\pm 1\} \times \mathbb{Z}^r$ où $r = (p-3)/2$.

Autrement dit, il existe r unités u_1, \dots, u_r de B telles que tout $u \in B^*$ s'écrive de manière unique sous la forme

$$u = \pm \prod_{i=1}^r u_i^{n_i} \quad \text{avec} \quad n_i \in \mathbb{Z}.$$

On dit que les u_i forment un système d'unités fondamentales de K^+ . On définit le régulateur R^+ de K^+ comme suit. Soient $\sigma_1, \dots, \sigma_{r+1}$ les $(p-1)/2$ plongements de K^+ dans \mathbb{R} . Par définition, R^+ est la valeur absolue du déterminant de n'importe quelle matrice extraite d'ordre r de la matrice de taille $(r, r+1)$ dont l'élément de la i -ème ligne et de la j -ième colonne est

$$\log |\sigma_j(u_i)| \quad \text{avec} \quad 1 \leq i \leq r \quad \text{et} \quad 1 \leq j \leq r+1.$$

Ce déterminant ne dépend pas de la matrice extraite choisie car la norme sur \mathbb{Q} d'une unité est ± 1 . On vérifie par ailleurs que R^+ est indépendant du choix du système d'unités fondamentales, ainsi que de la numérotation des plongements réels de K^+ .

Exercice 1

Calculer le régulateur de $\mathbb{Q}(\mu_5)^+$.

La détermination d'un système d'unités fondamentales de K^+ est en général très difficile. On ne sait d'ailleurs pas déterminer un tel système si p est de l'ordre de 100. On connaît néanmoins un sous-groupe d'indice fini de B^* , appelé parfois le groupe des unités cyclotomiques. Plus précisément, soient r et s des entiers premiers à p . Alors

$$(1) \quad \frac{1 - \zeta^r}{1 - \zeta^s} \in A^*.$$

En effet, il existe $t \geq 1$ tel que $r \equiv st \pmod{p}$, on a

$$\frac{1 - \zeta^r}{1 - \zeta^s} = \frac{1 - \zeta^{st}}{1 - \zeta^s} = 1 + \zeta^s + \dots + \zeta^{s(t-1)} \in A,$$

et le même argument vaut pour $(1 - \zeta^s)/(1 - \zeta^r)$. D'après l'exercice 6 du chapitre II (questions 4 et 5), il existe donc $j \in \mathbb{Z}$ tel que l'on ait

$$\frac{1 - \zeta^s}{1 - \zeta} = \zeta^{2j} \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}}.$$

Par suite,

$$\left| \frac{1 - \zeta^s}{1 - \zeta} \right|^2 = \frac{1 - \zeta^s}{1 - \zeta} \times \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}} \in K^2.$$

Il en résulte que, en prenant la racine carrée positive,

$$(2) \quad v_s := \sqrt{\frac{1 - \zeta^s}{1 - \zeta} \times \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}}} \in B^* \quad \text{pour} \quad s = 2, \dots, \frac{p-1}{2}.$$

On vérifie directement que l'on obtient ainsi $(p-3)/2$ unités distinctes positives de B^* autres que ± 1 . Par ailleurs, on démontre que les v_s sont \mathbb{Z} -linéairement indépendantes. Le sous-groupe V de B^* engendré par les v_s est donc d'indice fini dans B^* . Soit U^+ le sous-groupe des unités positives de B^* . Alors, $[U^+ : V]$ étant l'indice de V dans U^+ , on a

$$(3) \quad h^+ = [U^+ : V].$$

En particulier, on a $h^+ = 1$ si et seulement si les v_s forment un système d'unités fondamentales de B .

Donnons maintenant une formule qui relie le régulateur R^+ et h^+ . Soit g le plus petit entier ≥ 1 tel que $g \bmod p$ soit générateur du groupe multiplicatif \mathbb{F}_p^* . Soit η une racine primitive $p-1$ -ième de l'unité. On a alors

$$(4) \quad h^+ = \frac{1}{R^+} \prod_{k=1}^{(p-3)/2} \left| \sum_{j=0}^{(p-3)/2} \eta^{2kj} \log \left| 1 - \zeta^{g^j} \right| \right|.$$

Exercice 2

Calculer h^+ si $p = 5$.

Signalons qu'il existe des heuristiques selon lesquelles pour environ trois quarts des nombres premiers l'entier h^+ correspondant vaut 1.

1.2. Le facteur h^-

Pour tout $j = 0, \dots, p-2$, on définit des entiers g_j par la condition

$$(5) \quad g_j \equiv g^j \bmod p \quad \text{et} \quad 1 \leq g_j < p.$$

On pose

$$F(X) = \sum_{j=0}^{p-2} g_j X^j \in \mathbb{Z}[X].$$

On a alors, η étant une racine primitive $p-1$ -ième de l'unité,

$$(6) \quad h^- = \frac{1}{(2p)^{(p-3)/2}} \left| F(\eta) F(\eta^3) \cdots F(\eta^{p-2}) \right|.$$

À titre indicatif, vérifions que $b := F(\eta) F(\eta^3) \cdots F(\eta^{p-2})$ est un entier relatif. Considérons pour cela le corps $L = \mathbb{Q}(\eta)$. L'extension L/\mathbb{Q} est galoisienne de degré l'indicateur d'Euler de $p-1$. Soit σ un élément de $\text{Gal}(L/\mathbb{Q})$. Il existe un entier k , premier à $p-1$ et compris entre 1 et $p-1$, tel que $\sigma(\eta) = \eta^k$. Posons $m = (p-1)/2$. On a

$$\sigma(b) = \prod_{j=1}^m F(\eta^{k(2j-1)}).$$

L'ensemble des éléments $k(2j - 1) \bmod. p - 1$ pour $1 \leq j \leq m$ est de cardinal m : si $k(2j - 1) \equiv k(2j' - 1) \bmod. p - 1$, on a $j \equiv j' \bmod. m$ car k est premier à $p - 1$, d'où $j = j'$. Puisque k est impair, il coïncide donc avec l'ensemble des $2j' - 1 \bmod. p - 1$ pour $1 \leq j' \leq m$. Par suite, $\sigma(b) = b$ et b est dans \mathbb{Q} . Puisque b est un entier de L , b est donc dans \mathbb{Z} .

On notera qu'il n'est nullement évident que les deuxièmes membres des égalités (4) et (6) définissent des entiers.

Exercice 3

Calculer h^- si $p = 5$.

2. Critères de régularité

La formule (6) permet de calculer explicitement h^- , tout au moins si p n'est pas trop grand. Cette formule s'avère particulièrement utile en vue de décider si un nombre premier p est régulier ; s'il ne l'est pas, on dit qu'il est irrégulier. Kummer a en effet démontré en 1850 le résultat suivant :

$$(7) \quad h^+ \equiv 0 \bmod. p \implies h^- \equiv 0 \bmod. p.$$

En particulier, on en déduit que

$$(8) \quad p \text{ est irrégulier si et seulement si } p \text{ divise } h^-.$$

Signalons à ce propos la conjecture suivante attribuée à Vandiver, qui a été vérifiée pour tous les nombres premiers $p < 4.10^6$ ([B-C-E-M]) :

Conjecture. *L'entier h^+ n'est jamais divisible par p .*

Une étude faite par Kummer du facteur h^- a alors pour conséquence le résultat suivant :

Théorème 1. *Le nombre premier p est irrégulier si et seulement si il existe un entier n tel que l'on ait*

$$\sum_{j=1}^{p-1} j^{2n} \equiv 0 \bmod. p^2 \quad \text{et} \quad n \in \left\{ 1, \dots, \frac{p-3}{2} \right\}.$$

Exercice 3

Pour tout entier naturel m tel que $p - 1$ ne divise pas m , montrer que l'on a

$$\sum_{j=1}^{p-1} j^m \equiv 0 \bmod. p.$$

Tel est en donc le cas si $m = 2n$ et $n = 1, \dots, \frac{p-3}{2}$.

Il existe par ailleurs un critère de régularité de Kummer qui s'exprime en termes des nombres de Bernoulli. Ce sont des nombres rationnels qui sont définis à partir des coefficients du développement en série de Laurent de la fonction méromorphe sur \mathbb{C} qui à z associe $z/(e^z - 1)$, dont les pôles sont les $2n\pi i$ ou $n \in \mathbb{Z}$. Le n -ième nombre de Bernoulli B_n est défini à partir de l'égalité (valable pour $0 < |z| < 2\pi$) :

$$(9) \quad \frac{z}{e^z - 1} = \sum_{n \geq 0} \frac{B_n}{n!} z^n.$$

On a par exemple

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \dots, B_{12} = -\frac{691}{2730}, \dots, B_{32} = -\frac{37 \times 683 \times 305065927}{510}.$$

Par ailleurs, on a $B_{2n+1} = 0$ pour tout $n \geq 1$ (vérifier cette assertion). Les B_{2n} permettent de calculer les valeurs de la fonction zêta de Riemann aux entiers pairs. En effet, en utilisant le développement en série de la fonction $\cot z$, on obtient la formule d'Euler :

$$B_{2n} = (-1)^{n-1} \frac{\zeta(2n)(2n)!}{\pi^{2n} 2^{2n-1}} \quad \text{pour tout } n \geq 1.$$

Posons

$$B_{2n} = \frac{N_{2n}}{D_{2n}} \quad \text{avec } D_{2n} > 0, \text{ pgcd}(N_{2n}, D_{2n}) = 1.$$

Les dénominateurs D_{2n} sont connus : ils sont sans facteurs carrés et un nombre premier ℓ divise D_{2n} si et seulement si $\ell - 1$ divise $2n$. On peut démontrer la congruence

$$(10) \quad pN_{2n} \equiv D_{2n} \sum_{j=1}^{p-1} j^{2n} \pmod{p^2} \quad \text{pour tout } n \geq 1.$$

Le théorème 1 entraîne alors le résultat suivant :

Théorème 2. *Le nombre premier p est irrégulier si et seulement si p divise le numérateur de l'un des nombres de Bernoulli B_2, B_4, \dots, B_{p-3} .*

À l'aide de ces résultats, on peut ainsi constater que les nombres premiers irréguliers plus petits que 100 sont 37, 59 et 67 (le numérateur de B_{32} est divisible par 37). Signalons qu'il existe d'autres congruences que (10) permettant de tester la régularité d'un nombre premier p , en donnant directement la valeur de B_{2n} modulo p (cf. par exemple [Wa], p. 181). On ne sait pas démontrer l'existence d'une infinité de nombres premiers réguliers. Là encore il existe des heuristiques qui rendent plausible le fait qu'en moyenne trois nombres premiers sur cinq devraient être réguliers. Cette proportion est en accord avec les résultats de [B-C-E-M]. Cela étant, Jensen a démontré en 1915 l'existence d'une infinité de nombres premiers irréguliers. Il y en a par exemple une infinité congrus à 3 modulo 4.

Bibliographie

- [Bo-Sh] Z. I. Borevitch et I. R. Shafarevitch, *Théorie des nombres*, Gauthier-Villars Paris, 1967.
- [B-C-E-M] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, Irregular primes and cyclotomic invariants to four million, *Math. Comp.* **61** (1993), 151-153.
- [Coh] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag, 1993.
- [Coh-Rob] H. Cohen et X.-F. Roblot, Computing the Hilbert class field of real quadratic fields, *Math. Comp.* **69** (2000), 1229-1244.
- [Cox] D. Cox, *Primes of the form $x^2 + ny^2$, Fermat, Class Field Theory, and Complex Multiplication*, Wiley-Interscience, 1989.
- [Ku] E. E. Kummer, *Collected Papers*, vol. I, édité par A. Weil, Springer-Verlag 1975.
- [La] S. Lang, *Algebraic Number Theory*, Second Edition, Springer GTM 110, 1994.
- [Pa] C. Batut, D. Bernardi, H. Cohen et M. Olivier, User's guide to PARI-GP (version 2.1.4).
- [Riben] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer-Universitext, 2001.
- [Ribet] K. Ribet, On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431-476.
- [Ro] P. Roquette, On class field towers, dans *Algebraic Number Theory*, ed. par J. W. S. Cassels et A. Fröhlich, Academic Press, New York 1967, 231-249.
- [Sa] P. Samuel, *Théorie algébrique des nombres*, deuxième édition, Hermann, Paris 1971.
- [Se] J.-P. Serre, *Corps locaux*, Hermann, troisième édition 1968.
- [Va] H. S. Vandiver, Summary of results and proofs on Fermat's Last Theorem (sixth paper), *Proc. Nat. Acad. Sci.*, **17** (1931), 661-673.
- [Wa] L. Washington, *Introduction to Cyclotomic Fields*, Springer GTM 83, 1982.
- [Wi] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.* **141** (1995), 443-551.
-