Kummer

et le théorème

de Fermat

Table des matières

1 Les équations de degré 2, 3, 4, 5 **5**

1.1 L'équation de degré 2 5

1.2 L'équation de degré 4 6

1.3 L'équation de degré 3 7

1.4 L'équation de degré 5 12

2 Corps cyclotomique et notion de régularité **20**

2.1 Introduction 20

2.2 Définitions et notations 21

2.3 Corps cyclotomique 23

2.4 Entiers cyclotomiques 25

2.5 Nombres premiers réguliers 27

3 Premier résultat de Kummer sur le grand théorème de Fermat **28**

3.1 Introduction 28

3.2 Premier cas 30

3.3 Second cas 33

3.4 Le théorème de Fermat pour les nombres premiers réguliers 40

4 Arithmétique cyclotomique **41**

4.1 Unités 41

4.2 Décomposition des idéaux premiers, discriminant et ramification 45

4.3 Unités cyclotomiques 48

5 Nombre de classes de $\mathbb{Q}(\xi)$ **51**

5.1 La fonction ζ_K 53

5.2 Domaine fondamental 54

5.3 Nombre de classes de K 58

5.4 Fonction ζ_K et fonctions L 61

5.5 Fonction ζ_K et nombre de classes de K 71

5.6 Appendice : un théorème de Dirichlet 72

5.7 Appendice : caractères modulo l 75

5.8 Appendice : sommes de Gauss 76

5.9 Appendice : extensions cyclotomiques de degré quelconque 78

6 Second résultat de Kummer sur le grand théorème de Fermat **81**

6.1 Introduction 81

6.2 h_0 est entier 83

6.3 h_1 est entier 90

6.4 Condition de divisibilité de h_1 par l 97
6.5 Si l divise h_0, alors l divise h_1 102
6.6 Lemme de Kummer 111
6.7 Le second théorème de Kummer 113
6.8 Appendice : lemme algébrique 114
6.9 Appendice : nombres et polynômes de Bernoulli . 115

A Nombres algébriques **126**
A.1 Corps de nombres algébriques 126
A.2 Corps finis 135
A.3 Anneaux d'entiers algébriques 138
A.4 Classes d'idéaux 149
A.5 Unités 155
A.6 Réseaux de $\mathbb{R}^n$ 159

Chapitre 1

Les équations de degré 2, 3, 4, 5

1.1 L'équation de degré 2

Lemme 1.1.1. *Si $a^2 = bc$ avec $(b, c) = 1$, alors b et c sont des carrés.*

Démonstration. Immédiate compte tenu de l'unicité de la décomposition de tout nombre entier en facteurs premiers. □

Lemme 1.1.2. *Si $a^2 + b^2 = c^2$ avec $(a, b, c) = 1$, alors c est impair, et entre a et b, un seul est impair.*

Démonstration. Les résidus des carrés modulo 4 valent 0 ou 1. □

Théoreme 1.1.3. *Si $a^2 + b^2 = c^2$ avec $(a, b, c) = 1$ avec par exemple b pair, alors il existe d et e tels que $(e, d) = 1$ et $c = d^2 + e^2$, $a = d^2 - e^2$, $b = 2de$.*

Démonstration. 1. On écrit $b = 2f$. On a : $4f^2 = c^2 - a^2 = (c + a)(c - a)$ et $f^2 = (c + a)/2 \times (c - a)/2$.

2. c et a étant impairs et premiers entre eux, $(c+a)/2$ et $(c-a)/2$ sont entiers et premiers entre eux.
3. D'après 1.1.1, ce sont des carrés : $(c+a)/2 = d^2$, $(c-a)/2 = e^2$.
4. Donc : $c = d^2 + e^2$, $a = d^2 - e^2$, $b = 2de$.

□

1.2 L'équation de degré 4

Théoreme 1.2.1. *$x^4 + y^4 = z^2$ n'a pas de solution.*

Démonstration. S'il existe une solution, il en existe une avec des entiers premiers entre eux. Supposons que l'on ait $x^4 + y^4 = z^2$ avec $(x, y, z) = 1$.

1. D'après 1.1.3, il existe a et b, b pair, tels que $(a, b) = 1$ et $z = a^2 + b^2$, $x^2 = a^2 - b^2$, $y^2 = 2ab$.
2. b est pair : $b = 2f$. On a donc $a^2 = x^2 + 4f^2$ et $y^2 = 4af$.
3. D'après 1.1.1, a et f sont des carrés premiers entre eux ; il existe d et e tels que : $(d, e) = 1$, $a = d^2$, $f = e^2$. On a alors : $d^4 = x^2 + 4e^4$.
4. D'après 1.1.3, il existe f et g premiers entre eux tels que $d^2 = f^2 + g^2$, $x = f^2 - g^2$, $2e^2 = 2fg$. On a donc $e^2 = fg$.
5. D'après 1.1.1, f et g sont des carrés : $f = h^2$, $g = k^2$.
6. Et finalement : $d^2 = h^4 + k^4$.

On obtient le résultat par descente infinie : la nouvelle solution est strictement plus "petite" que la première. □

1.3 L'équation de degré 3

1.3.1 Les entiers d'Eisenstein

Definition 1.3.1. *Soit* $\alpha = (1+i\sqrt{3})/2 \in \mathbb{C}$. *On note* $\mathbb{Z}[\alpha]$ *l'ensemble de nombres complexes de la forme* $a + b\alpha$ *avec* $a, b \in \mathbb{Z}$.

Lemme 1.3.2. $\mathbb{Z}[\alpha]$ *est un anneau*

Démonstration. $\alpha^2 = (-1 + i\sqrt{3})/2 = \alpha - 1$. □

Lemme 1.3.3. $\alpha^2 \neq 1$, $\alpha^3 \neq 1$, $\alpha^6 = 1$.

Démonstration. $\alpha^2 = \alpha - 1$, $\alpha^3 = \alpha\alpha^2 = \alpha(\alpha - 1) = \alpha^2 - \alpha = \alpha - 1 - \alpha = -1$, $\alpha^6 = 1$. □

Definition 1.3.4. $N(a + i\sqrt{3}b) = a^2 + 3b^2$.

Lemme 1.3.5. $N(a + \alpha b) = a^2 + ab + b^2$.

Démonstration. On développe. □

Lemme 1.3.6. *Les unités de A sont les racines 6-èmes de l'unité.*

Démonstration. Elles vérifient $N(a + \alpha b) = 1$. On résout $a^2 + ab + b^2 = 1$ en nombre entiers. Si a et b sont de même signe, alors les solutions sont : $(1, 0)$, $(-1, 0)$, $(0, 1)$, $(0, -1)$. Sinon, les solutions sont : $(1, -1)$, $(-1, 1)$. L'ensemble des solutions correspond à : $\alpha, \alpha^2, \ldots, \alpha^5$. □

Lemme 1.3.7. *A est factoriel.*

Démonstration. En fait A est euclidien :

1. Soient z' et z'' dans $A = \mathbb{Z}[\alpha]$.
2. Montrons qu'il existe q et r dans A tels que $z' = qz'' + r$ et $N(r) < N(z'')$.
3. Soit $z = z'/z''$ dans $Q[\alpha]$. On a $z = x + \alpha y$ avec $x, y \in Q$.
4. On choisit a et b dans $\mathbb{Z}$ tels que $| x - a | \leq 1/2, | y - b | \leq 1/2$.
5. On pose $q = a + \alpha b$. On a : $N(z - q) = (x - a)^2 + (x - a)(y - b) + (y - b)^2 \leq 3/4 < 1$; soit $N(z'/z'' - q) < 1$, soit $N(z' - qz'') < N(z'')$.
6. On pose $r = z' - qz''$.

Et on a le résultat. □

1.3.2 La solution

Lemme 1.3.8. *Soit x, y, z sans facteur commun et tels que $x^3 + y^3 + z^3 = 0$. Deux sont impairs (par exemple x et y), l'un est pair (donc z). Soit : $u = (x + y)/2$, $v = (x - y)/2$. Alors $x^3 + y^3 = 2u(u^2 + 3v^2)$, et*

— *u et v sont de parités différentes*

— *u et v sont premiers entre eux*

— *$2u$ et $u^2 + 3v^2$ sont premiers entre eux*

— *$2u$ et $u^2 + 3v^2$ sont des cubes*

Démonstration. 1. Soient u et v tels que définis plus haut.

$$\begin{aligned} 2u(u^2+3v^2) &= 2\frac{x+y}{2}\left((\frac{x+y}{2})^2+3(\frac{x-y}{2})^2\right) \\ &= \frac{x+y}{4}\left((x^2+2xy+y^2)+3(x^2-2xy+y^2)\right) \\ &= \frac{x+y}{4}\left(4x^2-4xy+4y^2\right) \\ &= (x+y)\left(x^2-xy+y^2\right) \\ &= x^3+y^3 \end{aligned}$$

2. u et v sont premiers entre eux : sinon $x = u + v$ et $y = u - v$ ne seraient pas premiers entre eux.
3. u et v sont de parité différente : il suffit de monter que u et v ne sont pas tous les deux impairs ; mais dans ce cas, $x = u + v$ et $y = u - v$ seraient tous les deux pairs.
4. $2u$ et $u^2 + 3v^2$ sont premiers entre eux : les deux seuls cas non triviaux pour un diviseur commun sont $d = 2$ et $d = 3$. $d = 2$ est impossible car alors u et v seraient de même parité. Si 3 divise u, alors comme $z^3 = 2u(u^2 + 3v^2)$, 3 divise z ; on a $(3z')^3 = 2(3u')((3u')^2 + 3v^2)$, soit $3^2z'^3 = 2u'((3u')^3 + v^2)$; et 3 divise v : u et v ne sont pas premiers entre eux.
5. $2u$ et $u^2 + 3v^2$ sont des cubes : cela découle du théorème fondamental de l'arithmétique associé au résultat précédent.

□

Lemme 1.3.9. *Si* $u^2 + 3v^2 = w^3$ *avec* u *et* v *de parité différente,*

u et v premiers entre eux, alors il existe a, b, c tels que $2u = (2a + b)(a - b)(a + 2b)$, $2v = 3ab(a + b)$.

Démonstration. 1. On a : $(u + i\sqrt{3}v)(u - i\sqrt{3}v) = w^3$.

2. Montrons que : $(u + i\sqrt{3}v)$ et $(u - i\sqrt{3}v)$ sont premiers entre eux dans A. Sinon, soit $d \in A$ un diviseur commun. Alors d divise leur somme $2u$ et leur différence $2i\sqrt{3}v$. $N(d)$ divise $N(2u) = 4u^2$ et $N(2i\sqrt{3}) = 12v^2$ dans $\mathbb{Z}$. Si 3 divise u, 3 divise w, 3 divise v ; or u et v sont premiers entre eux. Donc le p. g. c. d. de $4u^2$ et $12v^2$ est 4. $N(d)$ divise 4. Comme d n'est pas une unité, ceci est impossible car $N(d)$ divise $N(u + i\sqrt{3}v) = u^2 + 3v^2$ qui est impair parce que u et v sont de parité différente.

3. Donc, à une unité près, $(u + i\sqrt{3}v)$ et $(u - i\sqrt{3}v)$ sont des cubes dans A : $u + i\sqrt{3}v = \alpha^k(a + b\alpha)^3$ avec $k = 0, 1, 2, \ldots, 5$.

4. Si on développe $u + i\sqrt{3}v = \alpha^k(a + b\alpha)^3$, pour les différentes valeurs de k, on obtient :

k	$2u$	$2v$
0	$2a^3 + 3ba^2 - 3b^2a - 2b^3$	$3ba^2 + 3b^2a$
1	$a^3 - 3ba^2 - 6b^2a - b^3$	$a^3 + 3ba^2 - b^3$
2	$-a^3 - 6ba^2 - 3b^2a + b^3$	$a^3 - 3b^2a - b^3$
3	$-2a^3 - 3ba^2 + 3b^2a + 2b^3$	$-3ba^2 - 3b^2a$
4	$-a^3 + 3ba^2 + 6b^2a + b^3$	$-a^3 - 3ba^2 + b^3$
5	$a^3 + 6ba^2 + 3b^2a - b^3$	$-a^3 + 3b^2a + b^3$

(1.1)

5. Si $k = 0$ ou 3, on vérifie les formules $2u = \pm(2a + b)(a - b)(a + 2b)$, $2v = \pm 3ab(a + b)$.
6. Si $k = 1$, on a $v - u = 3ab(a + b)$. Mais $v - u$ est impair alors que $3ab(a + b)$ est toujours pair.
7. Les autres valeurs de k se traitent de la même façon.

□

Théoreme 1.3.10. $x^3 + y^3 + z^3 = 0$ *n' a pas de solution*

Démonstration. Soit x, y, z une solution. Soient u, v les entiers associés par le lemme 1.3.8. Soient a, b, c les entiers associés par le lemme 1.3.9.

1. On a $2u = (2a + b)(a - b)(a + 2b)$, et d'autre part $2u$ est un cube.
2. On montre que $(2a + b), (a - b), (a + 2b)$ sont premiers entre eux.
   a) Si d divise $2a + b$ et $a - b$, alors d divise $3a = (2a + b) + (a - b)$.
   b) Si d divise $a + 2b$ et $a - b$, alors d divise $3a = (a + 2b) + 2(a - b)$.
   c) Si d divise $a + 2b$ et $2a + b$, alors d divise $3a = 2(2a + b) - (a + 2b)$.

   Donc d divise $u = (2a+b)(a-b)(a+2b)/2$ et $v = 3ab(a+b)/2$. Or u et v sont premiers.

3. Donc $(2a+b), (a-b), (a+2b)$ sont donc des cubes : $(2a+b) = f^3$, $(a-b) = g^3$, $(a+2b) = h^3$. On a donc : $f^3 + g^3 = h^3$.

On obtient le résultat par descente infinie : la nouvelle solution est strictement plus "petite" que la première. □

1.4 L'équation de degré 5

1.4.1 L'anneau $\mathbb{Z}[\rho]$

Definition 1.4.1. *Soit* $\rho = (1+\sqrt{5})/2$ *et* $\mathbb{Z}[\rho] = \{a + b\rho \mid a, b \in \mathbb{Z}\}$.

Lemme 1.4.2. $\mathbb{Z}[\rho] = \{(a + b\sqrt{5})/2 \mid a, b \in \mathbb{Z}$ *de même parité*$\}$.

Démonstration. Il suffit de développer. □

Lemme 1.4.3. $\mathbb{Z}[\rho]$ *est un anneau.*

Démonstration. $\rho^2 = 1 + \rho$. □

Definition 1.4.4. $N(a + b\sqrt{5}) = a^2 - 5b^2$

Lemme 1.4.5. $N(a + b\rho) = a^2 + ab - b^2$

Démonstration.

$$\begin{aligned} N(a+b\rho) &= N(a + b(1+\sqrt{5})/2) \\ &= N((a + b/2) + (b/2)\sqrt{5}) \\ &= (a + b/2)^2 - 5(b/2)^2 \\ &= a^2 + ab - b^2 \end{aligned}$$

□

Lemme 1.4.6. $\rho^{-1} = \rho - 1$.

Démonstration. Immédiate. □

Lemme 1.4.7. *Les unités de* $\mathbb{Z}[\rho]$ *sont de la forme* $\pm\rho^n$, $n \in \mathbb{Z}$.

Démonstration.

1. On a $N(\rho) = -1$ et donc $|N(\pm\rho^n)| = 1$
2. Si $|N(a + b\rho) = 1|$, on a également $|N((a + b\rho)\rho)| = 1$ et $|N((a + b\rho)\rho^{-1})| = 1$
3. $(a + b\rho)\rho = (a + b)\rho + a\rho = (2a + b)\rho$
4. $(a + b\rho)\rho^{-1} = (b - a)\rho + a\rho = b\rho$.
5. On a toujours $|2a + b| < |a + b|$, ou $|b| < |a + b|$. On peut toujours diminuer le module de la somme des coefficients.
6. A la fin, on trouve une unité de la forme ± 1, $\pm\rho$

□

Lemme 1.4.8. $\mathbb{Z}[\rho]$ *est un anneau factoriel.*

Démonstration. En fait A est euclidien :

1. Soient z' et z'' dans $A = \mathbb{Z}[\rho]$.
2. Montrons qu'il existe q et r dans A tels que $z' = qz'' + r$ et $|N(r)| < |N(z'')|$.
3. Soit $z = z'/z''$ dans $Q[\rho]$. On a $z = x + \rho y$ avec $x, y \in Q$.
4. On choisit a et b dans $\mathbb{Z}$ tels que $| x - a | \leq 1/2, | y - b | \leq 1/2$.

5. On pose $q = a + \rho b$. On a : $N(z-q) = (x-a)^2 + (x-a)(y-b) - (y-b)^2$; donc : $|N(z-q)| \leq (x-a)^2 + |(x-a)(y-b)| + (y-b)^2 \leq 3/4 < 1$; donc $|N(z'/z'' - q)| < 1$, donc $|N(z' - qz'')| < |N(z'')|$.
6. On pose $r = z' - qz''$.

Et on a le résultat. □

Lemme 1.4.9. *Si x et y sont premiers entre eux, si y est un multiple de 5 et si $x^2 - 5y^2 = z^5$, alors il existe m et n premiers entre eux, de parité contraires tels que $x + y\sqrt{5} = (m + n\sqrt{5})^5$.*

Démonstration. On décompose $x^2 - 5y^2 = (x + \sqrt{5}y)(x - \sqrt{5}y)$ et on montre que les deux facteurs sont premiers entre eux dans $\mathbb{Z}[\rho]$.

1. Si $d = a + b\rho$ divise $(x + \sqrt{5}y)$ et $(x - \sqrt{5}y)$, il divise leur somme $2x$ et leur différence $2\sqrt{5}y$.
2. Alors $N(d)$ divise $N(2x) = 4x^2$ et $N(2\sqrt{5}y) = 20y^2$
3. Comme x et y sont premiers entre eux, $N(d) = 1$ ou $N(d) = 4$.
4. Si $N(d) = 1$, c'est fini.
5. Si $N(d) = 4$, $d = 2\rho^n$.
6. On peut supposer que $d = 2$.
7. Donc x et y sont pairs.

□

Lemme 1.4.10. *Si x et y sont premiers entre eux, si y est un multiple de 5 et si $(x^2 - 5y^2)/2 = z^5$, alors il existe m et n premiers entre eux, tels que $(x + y\sqrt{5})/2 = ((n + m\sqrt{5})/2)^5$.*

Démonstration. Similaire. □

Lemme 1.4.11. *Si* $x + y\sqrt{5} = (m + n\sqrt{5})^5$, *alors* $x = n^5 + 50n^3m^2 + 125nm^4$, $y = 5n^4m + 50n^2m^3 + 25m^5$, $z = n^2 - 5m^2$. *Si* $(x + y\sqrt{5})/2 = ((n + m\sqrt{5})/2)^5$, *alors* $16x = n^5 + 50n^3m^2 + 125nm^4$, $16y = 5n^4m + 50n^2m^3 + 25m^5$, $4z = n^2 - 5m^2$.

Démonstration. On développe. □

1.4.2 Un théorème de Sophie Germain

Soit $\overline{x}$ le résidu de x modulo 11.

Lemme 1.4.12. *Pour tout* x, $\overline{x^5} = \overline{0}$ *ou* $\overline{\pm 1}$.

Démonstration. D'après le petit théorème de Fermat, pour tout x, $\overline{x^{10}} = \overline{0}$ *ou* $\overline{1}$; si $\overline{x^{10}} = \overline{0}$ alors $\overline{x^5} = \overline{0}$; si $\overline{x^{10}} = \overline{1}$, alors $\overline{x^5} = \overline{\pm 1}$. □

Lemme 1.4.13. *Si* $\overline{x^5 + y^5 + z^5} = \overline{0}$, *alors* $\overline{x}$ *ou* $\overline{y}$ *ou* $\overline{z}$ *est nul.*

Démonstration. Si $\overline{x}$ ou $\overline{y}$ ou $\overline{z}$ valent ± 1, alors il est impossible que $\overline{x^5 + y^5 + z^5} = \overline{\overline{x^5} + \overline{y^5} + \overline{z^5}} = \overline{0}$. □

1.4.3 La solution

Proposition 1.4.14. *Si* $x^5 + y^5 + y^5 = 0$, *alors* x, y *ou* z *est multiple de* 5.

Démonstration. 1. On considère une solution dont aucun des éléments n'est multiple de 5.

2. On a : $-x^5 = y^5 + z^5 = (y+z)(y^4 - y^3z + y^2z^2 - yz^3 + z^4)$.
3. Montrons que : $(y+z)$ et $(y^4 - y^3z + y^2z^2 - yz^3 + z^4)$ sont premiers entre eux : soit r un diviseur premier commun ; alors $y^4 - y^3z + y^2z^2 - yz^3 + z^4 = 0(r)$, $y = -z + (r)$, et $y^4 - y^3z + y^2z^2 - yz^3 + z^4 = 5z^4(r)$; donc r divise z et $y+z$; ce qui est contradictoire.
4. Donc $(y+z)$ et $(y^4 - y^3z + y^2z^2 - yz^3 + z^4)$ sont de puissances 5-ièmes.
5. Le même raisonnement peut être fait avec les autres variables.

$$\begin{array}{l|l|l} y+z=a^5 & y^4 - y^3z + y^2z^2 - yz^3 + z^4 = \alpha^5 & x = -a\alpha \\ z+x=b^5 & z^4 - z^3x + z^2x^2 - zx^3 + x^4 = \beta^5 & y = -b\beta \\ x+y=c^5 & x^4 - x^3y + x^2y^2 - xy^3 + y^4 = \gamma^5 & z = -c\gamma \end{array} \tag{1.2}$$

6. Modulo 11, d'après le lemme 1.4.13, $\overline{x}$ ou $\overline{y}$ ou $\overline{z}$ est nul.
7. Supposons $\overline{x}$ nul. On a : $0 = \overline{2x} = \overline{b^5 + c^5 - a^5}$. D'après le lemme 1.4.13, $\overline{a}$ ou $\overline{b}$ ou $\overline{c}$ est nul.
   a) Si $\overline{b} = 0$, alors $\overline{y} = \overline{-b\beta} = 0$; mais x et y sont premiers entre eux.
   b) Si $\overline{c} = 0$, alors $\overline{z} = \overline{-c\gamma} = 0$; mais z et x sont premiers entre eux.
   c) Si $\overline{a} = 0$, $\overline{y} = -\overline{z}$ et $\overline{\alpha^5} = \overline{y^4 - y^3z + y^2z^2 - yz^3 + z^4} = \overline{5y^5}$, et $\overline{(\alpha y^{-1})^5} = \overline{5}$; ce qui contredit le lemme 1.4.12.

□

Théoreme 1.4.15. *$x^5 + y^5 + z^5$ n'a pas de solution.*

Démonstration. 1. Soit (x, y, z) une solution. D'après le résultat précédent, l'une des variables x, y ou z est divisible par 5. Par exemple z.

2. Si z est pair.
   a) $u = (x + y)/2$ et $v = (x - y)/2$ sont premiers entre eux et de parités différentes.
   b) L'equation devient $z^5 = 2u(u^4 + 10u^2v^2 + 5v^4)$.
   c) Comme 5 divise z, il divise u : $u = 5w$.
   d) $z^5 = 10w(625w^4 + 250u^2v^2 + 5v^4) = 50w(125w^4 + 50u^2v^2 + v^4)$.
   e) Les deux facteurs de z^5, $50w$ et $125w^4 + 50u^2v^2 + v^4$ sont premiers entre eux.
   f) Donc : $50w = a^5$, $125w^4 + 50u^2v^2 + v^4 = b^5$.
   g) Donc : $125w^4 + 50u^2v^2 + v^4 = (v^2 + 25w^2)^2 - 500w^2 = u^2 - 5t^2$ avec $u = v^2 + 25w^2$, $t = 10w^2$.
   h) Donc $u^2 - 5t^2 = b^5$. D'après le lemme 1.4.10, il existe m et n premiers entre eux, de parités différentes tels que $u = n^5 + 50n^3m^2 + 125nm^4$, $t = 5n^4m + 50n^2m^3 + 25m^5$.
   i) Donc : $5^4 2m(n^2 + 10n^2m^2 + 5m^4) = 5^3 2t = 5^4 2^2 w^2 = (5^2 2w)^2 = (a^5)^2 = a^{10} = (a^2)^5$.
   j) Donc, les deux termes de ce produit étant premiers entre eux, on a : $5^4 2m = c^5$, $n^4 + 10n^2m^2 + 5m^4 = d^5$. Et ceci est impossible. En effet, sinon :

i. m est multiple de 5

ii. On écrit : $a = n^2 + 5m^2$, $b = 2m^2$, $a^2 - 5b^2 = c^5$

iii. D'après le lemme 1.4.13 : $a = p^2 + 5p^3q^2 + 125pq^4$, $b = 5p^4q + 50p^2q^3 + 25q^5$.

iv. $5^5 5^3 2q(p^4 + 10p^2q^2 + 5q^4) = 5^8 2b = 5^8 2^2 m^2 = (5^4 2m)^2 = (c^5)^2 = c^{10}$

v. $5^4 2q$ et $p^4 + 10p^2q^2 + 5q^4$ sont premiers entre eux

vi. Donc : $5^4 2q = u^5$, $p^4 + 10p^2q^2 + 5q^4 = v^5$.

vii. On conclut par un argument de descente infinie

3. Si z est impair.

a) $u = x + y$ et $v = x - y$ sont impairs, premiers entre eux.

b) L'équation devient $u(u^4 + 10u^2v^2 + 5v^4) = 16z^5$.

c) Comme 5 divise z, il divise u : $u = 5w$.

d) $25w(v^4 + 50v^2w^2 + 125w^4) = 16z^5$.

e) $25w$ et $v^4 + 50v^2w^2 + 125w^4$ sont premiers entre eux.

f) Donc $25w = a^5$, $(v^2 + 25w^2)^2 - 5(10w^2)^2 = 16b^5$.

g) Avec $r = (v^2 + 25w^2)/2$ $s = 5w^2$; on obtient : $(r/2)^2 - 5(s/2)^2 = b^5$.

h) On applique le lemme 1.4.10 : il existe m et n premiers entre eux, tels que $(r + s\sqrt{5})/2 = ((n + m\sqrt{5})/2)^5$, donc tels que $16r = n^5 + 50n^3m^2 + 125nm^4$, $16s = 5n^4m + 50n^2m^3 + 25m^5$, $4z = n^2 - 5m^2$.

i) Le reste de la démonstration est similaire à celle du cas où z est impair.

□

Chapitre 2

Corps cyclotomique et notion de régularité

2.1 Introduction

Si on note $\xi_3 = e^{2i\pi/3} = (1 - i\sqrt{3})/2$, on trouve immédiatement en développant les facteurs que : $x^3 + y^3 = (x + y)(x + \xi_3 y)(x + \xi_3^2 y)$. Cela se généralise et le point de départ de l'approche suivie par Kummer est l'égalité suivante que nous démontrons plus tard : pour un nombre premier impair l, $\xi_l = e^{2i\pi/l}$ étant une racine l-ième de 1, on a :

$$x^l + y^l = (x + y)(x + \xi_l y)(x + \xi_l^2 y) \dots (x + \xi_l^{l-1} y)$$

Nous présentons ici les propriétés des extensions cyclotomiques de degré premier : $\mathbb{Q}(\xi_l)$. Ce chapitre repose sur les définitions données dans les appendices A.1, A.3, A.4 et A.5 qui donnent une présentation élémentaire de la théorie des nombres algébriques.

2.2 Définitions et notations

Definition 2.2.1. *Soit l un nombre premier supérieur à deux. Le* ***l-ème corps cyclotomique*** *est l'extension $K = \mathbb{Q}(\xi)$, où $\xi = e^{2i\pi/l}$ une racine l-ième de l'unité. Le* ***l-ème polynome cyclotomique*** *est* $\Phi_l(X) = X^{l-1} + X^{l-2} + \cdots + X + 1$

Lemme 2.2.2. $X^l - 1 = (X-1)\Phi_l(X)$

Démonstration. On développe. □

Lemme 2.2.3. *ξ est solution de* $\Phi_l(X) = 0$

Démonstration. Cela découle de 2.2.2 et de ce que $\xi \neq 1$ □

Lemme 2.2.4. *ξ^i est solution de* $\Phi_l(X) = 0$ *pour* $i = 1, \ldots, l-1$

Démonstration. Puisque i est premier avec l, considérés modulo l, les ensembles, $\{0, 1, 2, \ldots, l-1\}$ et $\{0, i, 2i, \ldots, (l-1)i\}$ sont identiques. On a donc :

$$\begin{aligned} 0 &= \Phi_l(\xi) = \xi^{l-1} + X^{l-2} + \cdots + \xi + 1 \\ &= \xi^{i(l-1)} + \xi^{i(l-2)} + \cdots + \xi^{i(0)} = \Phi_l(\xi^i) \end{aligned}$$

□

Lemme 2.2.5.

$$\Phi_l(X) = (X-\xi)(X-\xi^2)\ldots(X-\xi^{l-1}) = \prod_{k=1}^{l-1}(X-\xi^k)$$

Démonstration. On connaît le degré : $l-1$ et autant de racines de Φ_l. □

Proposition 2.2.6.

$$x^l + y^l = (x+y)(x+\xi y)(x+\xi^2 y)\dots(x+\xi^{l-1}y)$$

Démonstration. On a :

$$X^l - 1 = (X-1)\Phi_l(X) = (X-1)\prod_{k=1}^{l-1}(X-\xi^k)$$

On pose dans cette équation : $X = -x/y$. Et on réduit au même dénominateur. □

Lemme 2.2.7. *Critère d'Eisenstein. Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire donné par $f(X) = X^n + f_{n-1}X^{n-1} + \cdots + f_1X + f_0$, si l est un nombre premier qui divise les coefficients a_i, si l^2 ne divise pas a_0, alors $f(X)$ est irréductible*

Démonstration.

1. Supposons que f est un polynôme réductible ; alors $f(X) = g(X)h(X)$ avec $g, h \in \mathbb{Q}[X]$, g, h étant de coefficient dominant 1,
2. $g, h \in \mathbb{Z}[X]$: les racines de g et h sont parmi celles de f, donc sont entières sur $\mathbb{Z}$. Les coefficients de g et h sont des combinaisons de ces racines. Ils sont dans $\mathbb{Q}$ et entiers sur $\mathbb{Z}$: ils sont dans $\mathbb{Z}$.

3. Dans $(\mathbb{Z}/l\mathbb{Z})[X]$: $\overline{f}(X) = X^n$. On peut donc écrire : $\overline{g}(X) = X^i$, $\overline{h}(X) = X^j$ avec $i + j = n$. g_0 et h_0 sont nuls ou divisibles par l ; si l'un des deux est nul ; il en est de même de leur produit f_0 ; ce qui est exclus ; donc l divise g_0 et h_0 mais l^2 ne divise pas $f_0 = g_0 h_0$.

□

Lemme 2.2.8. *$\Phi_l(X)$ est irréductible.*

Démonstration. Soit $Y = X - 1$. On écrit :

$$\Phi_l(X) \quad = \quad (X^l - 1)/(X - 1) = ((Y + 1)^l - 1)/Y = Y^l + \sum_{j=1}^{l-1} C_p^j Y^{j-1}$$

Les coefficients C_p^j sont multiples de l, le terme constant $C_p^1 = l$ n'est pas divsible par l^2. On applique le critère d'Eisenstein. □

2.3 Corps cyclotomique

Lemme 2.3.1. *$[K : \mathbb{Q}]$ est une extension Galoisienne cyclique. Son groupe de Galois est : $Gal(K : \mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{l-1})$ où $\sigma_i(\xi) = \xi^i$.*

Démonstration. Le degré de K sur $\mathbb{Q}$ est $l - 1$. Les σ_i constituent $(l - 1)$ isomorphismes différents. De plus, pour tout p premier avec l, on a l'égalité entre ensembles :$\{\sigma_1, \sigma_2, \ldots, \sigma_{l-1})\} = \{\sigma_p, \sigma_p^2, \ldots, \sigma_p^{l-1})\}$. Donc $Gal(K : \mathbb{Q}))$ est cyclique. □

Definition 2.3.2. *A tout $\alpha \in K$, on associe e*

1. *sa **norme** : $N(\alpha) = \prod_{i=1}^{l-1} \sigma_i(\alpha)$*
2. *sa **trace** : $T(\alpha) = \sum_{i=1}^{l-1} \sigma_i(\alpha)$.*

Notation 2.3.3. *Dans ce qui suit :*

1. *O_K l'anneau des entiers de K (cf. chapites A.3).*
2. *$\lambda = 1 - \xi$.*
3. *$m = (l-1)/2$.*

Lemme 2.3.4. *On a :*

1. *$N(\xi) = 1$,*
2. *$N(\lambda) = l$,*
3. *$T(\xi^j) = -1$ pour $1 \leq j \leq l-1$,*
4. *$T(1) = l - 1$,*
5. *$T(\lambda) = l$,*
6. *$T(a_0 + a_1\xi + \cdots + a_{l-2}\xi^{l-2}) = la_0 - (a_0 + a_1 + \cdots + a_{l-2})$*

Démonstration.

1. $N(\xi) = \xi\xi^2 \ldots \xi^{l-1} = \xi^{1+2+\cdots+(l-1)} = \xi^{l(l-1)/2} = 1^{(l-1)/2} = 1$
2. On a : $N(\lambda) = \prod_{i=1}^{l-1}(1 - \xi^i) = \Phi_l(1) = l$.
3. La trace de ξ est la somme des racines du polynôme $\Phi_l(x)$; c'est l'opposé du coefficient de x dans ce polynôme. Donc : $T(\xi^j) = -1$ pour $1 \leq j \leq l-1$.
4. $T(1) = \sum_{i=1}^{l-1} \sigma_i(1) = l - 1$.

5. $T(\lambda) = T(1) - T(\xi) = l - 1 - (-1) = l$.
6. On développe :

$$\begin{aligned} T(a_0 + a_1\xi + \cdots + a_{l-2}\xi^{l-2}) &= a_0T(1) + a_1T(\xi) + \cdots + a_{l-2}T(\xi^{l-2})) \\ &= la_0 - (a_0 + a_1 + \cdots + a_{l-2}) \end{aligned}$$

□

Lemme 2.3.5. *λ est premier.*

Démonstration. $N(\lambda) = l$ □

2.4 Entiers cyclotomiques

Definition 2.4.1. *$\mathbb{Z}(\xi)$ est l'ensemble* $\{a_0 + a_1\xi + \cdots + a_{l-2}\xi^{l-2} \mid a_i \in \mathbb{Z}\}$.

Lemme 2.4.2. *Si $\alpha \in O_K$, alors $T(\alpha) \in \mathbb{Z}$.*

Démonstration. On a une équation : $0 = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} + \alpha^n$. Et $T(\alpha) = -b_{n-1}$. □

Lemme 2.4.3. $\lambda O_K \bigcap \mathbb{Z} = l\mathbb{Z}$

Démonstration.
1. Il est clair que $\mathbb{Z}(\xi) \subset O_K$.
2. D'après 4.1.2, $l \in \lambda O_K$, donc $l\mathbb{Z} \subset \lambda O_K \bigcap \mathbb{Z}$.
3. Soit $a \in \lambda O_K \bigcap \mathbb{Z}$.

4. Comme $a \in \lambda O_K, a = \lambda b, b \in \mathbb{Z}(\xi)$. Alors $N(a) = N(\lambda)N(b) = lN(b)$ et $N(b) \in \mathbb{Z}$.
5. Comme $a \in \mathbb{Z}$, $N(a) = a^{l-1}$.
6. Donc $a^{l-1} = lN(b)$ et $a \in l\mathbb{Z}$

□

Lemme 2.4.4. *Pour tout $\alpha \in O_K$, $T(\alpha\lambda) \in l\mathbb{Z}$*

Démonstration.
1. $T(\alpha\lambda) \in \lambda O_K$ par définition de la trace.
2. $T(\alpha\lambda) \in \mathbb{Z}$.
3. On applique le lemme 2.4.3

□

Théoreme 2.4.5. $\mathbb{Z}(\xi) = O_K$

Démonstration.
1. Soit $\alpha = a_0 + a_1\xi + \cdots + a_{l-2}\xi^{l-2} \in O_K$
2. Les coefficients $a_i \in \mathbb{Q}$; il faut montrer qu'ils sont entiers.
3. On a $\alpha\lambda = a_0(1-\xi) + a - 1(\xi - \xi^2) + \cdots + a_{l-2}(\xi^{l-2} + \xi^{l-1})$
4. La fonction trace est additive. Avec 2.3.4, on obtient : $T(\alpha\lambda) = a_0 l$.
5. De 2.4.4, on déduit que $la_0 \in l\mathbb{Z}$. Donc $a_0 \in \mathbb{Z}$.
6. On a : $\xi^{-1} = \xi^{l-1}$. Donc $(\alpha - a_0)\xi^{-1} = a_1 + a_2\xi + \cdots + a_{l-2}\xi^{l-3} \in O_K$.
7. On lui applique le même raisonnement et on conclut que $a_1 \in \mathbb{Z}$.
8. On itère le procédé.

□

2.5 Nombres premiers réguliers

Definition 2.5.1. *Un nombre premier l est **régulier** si il y est vérifié la condition suivante : soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de $O_K = \mathbb{Q}(\xi_l)$; si leur produit est une puissance l-ième : $\mathfrak{ab} = \mathfrak{c}^l$, et s'ils sont premiers entre eux : $(\mathfrak{a}, \mathfrak{b}) = 1$, alors chacun d'eux est une puissance l-ième : $\mathfrak{a} = \kappa^l$ et $\mathfrak{b} = \mathfrak{g}^l$.*

Lemme 2.5.2. *Un nombre premier l est régulier si il seulement si il ne divise pas $h(K)$.*

Démonstration. Immédiate. □

Lemme 2.5.3. *Un nombre premier l est régulier si il seulement lorsque pour tout ideal I de O_K, si I^l est principal, alors I est principal.*

Démonstration. Immédiate. □

Chapitre 3

Premier résultat de Kummer sur le grand théorème de Fermat

3.1 Introduction

Soit l un nombre premier supérieur à 2.

Definition 3.1.1. *On appelle **premier cas** du théorème de Fermat, la proposition suivante : il n'existe pas d'entiers x, y, z tels que $x^l + y^l + z^l = 0$, l ne divise pas xyz.*

*On appelle **second cas** du théorème de Fermat, la proposition suivante : il n'existe pas d'entiers x, y, z tels que $x^l + y^l + z^l = 0$, l divise xyz.*

Notation 3.1.2. *Dans ce qui suit, nous utilisons, issues du chapitre précédent 2 sur les corps cyclotomiques, les notations suivantes :*

1. *$\xi = e^{2i\pi/l}$ est une racine l-ième de l'unité.*

2. *Le corps cyclotomique K est l'extension* $\mathbb{Q}[\xi]$. *Elle est degré* $l - 1$.
3. O_K *est l'anneau des entiers de K ; c'est* $\mathbb{Z}[\xi_k]$.
4. *N est la norme dans K*
5. *Pour* $\gamma \in K$, (γ) *est l'idéal fractionnaire engendré par* γ.

Nous utilisons, issues de ce même chapitre les définitions et résultats suivants :

1. Le *nombre de classes* $h(K)$ est l'indice du sous-groupe des idéaux premiers dans le groupe de tous les idéaux de K.
2. Un nombre premier est *régulier* si, lorsque le produit de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de O_K, premiers entre eux, est une puissance l-ième : $\mathfrak{ab} = \mathfrak{c}^l$, alors chacun d'eux est une puissance l-ième : $\mathfrak{a} = \mathfrak{k}^l$ et $\mathfrak{b} = \mathfrak{g}^l$. Un nombre premier l est régulier si il seulement si il ne divise pas $h(K)$.
3. $\lambda = 1 - \xi$ est un nombre premier de O_K de norme l.
4. $1 + \xi$ est une unité.

Nous considérons les deux conditions :

1. $\mathbf{A}(l)$: l est un nombre premier régulier
2. $\mathbf{B}(l)$: toute unité de O_K qui est congrue à un nombre entier modulo l est une puissance l-ième.

Nous allons montrer dans ce chapitre que :

Théoreme 3.1.3. ***A(l)*** *et* ***B(l)*** *impliquent le théorème de Fermat pour* l.

Dans toute la suite de ce chapitre, nous supposons que **A(l)** et **B(l)** sont vérifiées.

3.2 Premier cas

Théoreme 3.2.1. *Si on a **A(l)** et **B(l)**, l'équation $x^l + y^l + z^l = 0$ n'a pas de solution dans laquelle x, y et z sont premiers entre eux et l ne divise pas xyz.*

La démonstration est basée sur les points suivants.

1. $(x + \xi^i y)$ et $(x + \xi^j y)$ sont premiers entre eux dans O_K

   Démonstration. a) Soit $\mathfrak{a}$ un idéal de O_K qui est diviseur commun de $(x + \xi^i y)$ et $(x + \xi^j y)$

   b) $\mathfrak{a}$ divise $(\xi^j - \xi^i)y = (x + \xi^i y) - (x + \xi^j y)$. Donc $N(\mathfrak{a})$ divise $N(\xi^j - \xi^i)N(y) = l y^{l-1}$

   c) $\mathfrak{a}$ divise $(1 - \xi^{i-j})x = (x + \xi^i y) - \xi^{i-j}(x + \xi^j y)$. Donc $N(\mathfrak{a})$ divise $N(1 - \xi^{i-j})N(x) = l x^{l-1}$

   d) $N(\mathfrak{a}) = l$: sinon $N(\mathfrak{a})$ diviserait x et y.

   e) Comme $\mathfrak{a}$ divise $x + \xi^i y$, $N(\mathfrak{a})$ divise $N(x + \xi^i y)(x + y) = x^l + y^l$.

   f) Donc l divise z^l

   g) Donc l divise z. Contradiction.

   □

2. Il existe $\alpha \in O_K$ et une unité ν tels que $x + \xi y = \nu \alpha^l$. Cela vient du lemme précédent et de la condition $\mathbf{A}(l)$.

3. Il existe k tel que : $x\xi^{-k} + y\xi^{1-k} - x\xi^{k} - y\xi^{k-1} \equiv 0 \pmod{l}$

   Démonstration. a) On vient de voir qu'il existe $\alpha \in O_K$ et une unité ν tels que $x + \xi y = \nu\alpha^l$.

   b) Il existe $a \in \mathbb{Z}$ and $\beta \in O_K$ tel que $\alpha^l - a = l\beta$ d'après 4.1.3.

   c) Il existe $r \in \mathbb{R} \bigcap O_K$ et $k \in \mathbb{Z}$ tels que $\nu = r\xi^k$ d'après 4.1.5.

   d) Donc $x + \xi y = (r\xi^k)(a + l\beta)$ et $(x + \xi y)\xi^{-k} = r(a + l\beta)$

   e) En prenant le conjugué $(x + \xi^{-1}y)\xi^k = r(a + l\overline{\beta})$ et en faisant la différence, on obtient : $x\xi^{-k} + y\xi^{1-k} - x\xi^{k} - y\xi^{k-1} = rl(\beta - \overline{\beta})$

   □

4. Le nombre k est différent de 0 et de 1 modulo l

   Démonstration. a) Si $k \equiv 0 \pmod{l}$, alors en développant la congruence précédente : $x\xi^{-k} + y\xi^{1-k} - x\xi^{k} - y\xi^{k-1} \equiv 0 \pmod{l}$, on trouve : $y(\xi - \xi^{-1}) \equiv 0 \pmod{l}$, soit $y(\xi - \xi^{-1}) = l\theta$.

   b) On peut écrire, $y(\xi - \xi^{-1}) = y\xi(1 - \xi^2) = y\xi(1 - \xi)(1 + \xi)$

   c) La norme est multiplicative, donc $N(y)N(\xi)N(1-\xi)N(1+\xi) = N(l)N(\theta)$

   d) On sait que $\lambda = 1 + \xi$ est une unité, donc $N(1 + \xi) = 1$.

   e) On en déduit que : $y^{l-1} \times 1 \times l = l^{l-1}N(\theta)$ et que l divise y ; ce qui n'est pas.

f) On utilise exactement le même argument si $k \equiv 1 \pmod{l}$

□

5. Le nombre k est tel que deux parmi $\{k, -k, 1-k, -1+k\}$ sont congrus modulo l.

   Démonstration. a) On a :

$$\begin{aligned} x\xi^{-k} + y\xi^{1-k} - x\xi^{k} - y\xi^{k-1} &= l\gamma \text{ avec } \gamma \in O_K \\ \frac{x}{l}\xi^{-k} + \frac{y}{l}\xi^{1-k} - \frac{x}{l}\xi^{k} - \frac{y}{l}\xi^{k-1} &= \gamma \in O_K \end{aligned}$$

   b) Rappelons que : $\{1, \xi, \xi^2, \ldots, \xi^{l-2}\}$ est une base de O_K sur $\mathbb{Z}$

   c) Si tous les exposants $\{k, -k, 1-k, -1+k\}$ sont différents modulo l, alors $x/l \in \mathbb{Z}$. Ce qui n'est pas.

□

6. Le nombre k est tel que $2k - 1 \equiv \pmod{l}$: on examine tous les cas, il y en a 6, 4 sont impossibles, les deux autres se réduisent à $2k - 1 \equiv \pmod{l}$.

7. l divise $x - y$

   Démonstration. Avec k défini précédemment, on a :

   a) On peut écrire :
   $l\gamma\xi^k = x + y\xi - x\xi^{2k} - y\xi^{2k-1} = x + y\xi - x\xi^1 - y = (x - y)(1 - \xi)$

   b) Mais $N(l\gamma\xi^k) = l^{l-1}N(\gamma)$.

c) Et $N((x-y)(1-\xi)) = N(x-y)N(1-\xi) = (x-y)^{l-1}l$

d) Donc $l^{l-1}N(\gamma) = (x-y)^{l-1}l$ et l divise $x-y$.

□

8. l divise $x-z$. Par symétrie de l'équation $x^l + y^l + z^l = 0$.
9. $l = 3$: on développe, en tenant compte des résultats précédents : $0 = x^l + y^l + z^l = x^l + (x+al)^l + (x+bl)^l = 3x^l + cl$; comme l est premier avec x, ceci n'est possible que si $l = 3$.
10. $x^3 + y^3 + z^3 = 0$ n'a pas de solutions telles l ne divise pas xyz. En effet, les cubes de nombres premiers avec 3 valent ± 1 modulo 3.

3.3 Second cas

Nous supposons que l divise xyz.

Lemme 3.3.1. *Tout entier algébrique $\alpha \in O_K$ est congru modulo λ à un entier $a \in \mathbb{Z}$.*

Démonstration.

$$\alpha \quad = \quad \sum_{i=0}^{l-1} a_i \xi^i = \sum_{i=0}^{l-1} a_i (1-\lambda)^i \equiv \sum_{i=0}^{l-1} a_i \pmod{\lambda}$$

□

Lemme 3.3.2. *$(\alpha + \xi^i \beta)/(\alpha + \xi^j \beta)$ est une unité.*

Démonstration. On prend la norme. □

Nous allons monter que l'assertion suivante est fausse, puis qu'elle est impliquée par une éventuelle solution du second cas du théorème de Fermat :

Hypothèse 3.3.3. *L'équation :*

$$\alpha^l + \beta^l = \lambda^{lm}\nu\gamma^l$$

a une solution telle que (a) $m \geq 0$, (b) γ est premier avec λ, (c) ν une unité de O_K.

Nous supposons dans les lemmes qui suivent que 3.3.3 est vérifiée.

Lemme 3.3.4. *On peut se ramener au cas où :*

1. *Pour $i > 0$, $\alpha + \xi^i\beta$ est divisible par λ, pas par λ^2.*
2. *$\alpha + \beta$ est divisible par $\lambda^{l(m-1)+1}$*

Démonstration. 1. L'équation de l'hypothèse 3.3.3 s'écrit :

$$\prod_{i=0}^{l-1}(\alpha + \xi^i\beta) = \lambda^{lm}\nu\gamma^l$$

Comme λ est premier, un des $(\alpha + \xi^i\beta)$ est divisible par λ. Donc, d'après 3.3.2, tous les $(\alpha + \xi^i\beta)$ sont divisibles par λ .

2. Deux des $(\alpha + \xi^i\beta)$ ne sont pas égaux modulo λ^2. Sinon l'égalité $(\alpha + \xi^i\beta) - (\alpha + \xi^j\beta) = \lambda^2\gamma$ implique $\xi^i\beta(1 - \xi^{j-i}) =$

$\lambda^2\gamma$, implique $\xi^i\beta = (1-\xi)^2(1-\xi^{j-i})^{-1}\gamma$, implique $\xi^i\beta = \lambda\nu\gamma$ ce qui est impossible parce que $\xi^i\beta$ est premier avec λ.

3. Donc deux des $(\alpha + \xi^i\beta)/\lambda$ ne sont pas égaux modulo λ.
4. Comme $N(\lambda) = l$, les $(\alpha + \xi^i\beta)/\lambda$ forment un ensemble complet de résidus modulo λ.
5. Un seul d'entre eux $(\alpha + \xi^i\beta)/\lambda$ est congru à 0 modulo λ ; alors $(\alpha + \xi^i\beta)$ est congru à 0 modulo λ^2. On peut supposer pour la suite que c'est $\alpha + \beta$. Alors, pour $i > 0$, $(\alpha + \xi^i\beta)$ est multiple de λ mais pas de λ^2.
6. On écrit, θ_i et λ étant premiers entre eux,

$$\begin{aligned}(\alpha+\beta)\prod_{i=1}^{l-1}(\alpha+\xi^i\beta) &= \lambda^{lm}\nu\gamma^l \\ \theta_0\lambda^{p_0}\prod_{i=1}^{l-1}\theta_i\lambda &= \lambda^{lm}\nu\gamma^l\end{aligned}$$

On égalise les coefficients de λ. On trouve que $p_0 + l - 1 = lm$. Soit que : $p_0 = l(m-1) + 1$

□

Lemme 3.3.5. $m \geq 1$

Démonstration. Évidente dans la démonstration du lemme précédent : $m = 0$ implique que le facteur p_0 est négatif ; or il est plus grand que 2. □

Lemme 3.3.6. *On note $\mathfrak{m}$ l'idéal de O_K engendré par par α et β. Pour $0 \leq i \leq l-1$, il existe des idéaux $\mathfrak{g}_i$ tels que :*

1. *$\mathfrak{g}_i$ est premier avec (λ)*
2. *Pour $i > 0$, $(\alpha + \xi^i\beta) = (\lambda)\mathfrak{m}\mathfrak{g}_i$.*
3. *$(\alpha + \beta) = (\lambda)^{l(m-1)+1}\mathfrak{m}\mathfrak{g}_0$*

Démonstration. C'est 3.3.4, avec $\mathfrak{m}\mathfrak{g}_i = (\theta_i)$ □

Lemme 3.3.7. *Les idéaux $\mathfrak{g}_i$ de 3.3.6 sont premiers entre eux.*

Démonstration.

1. Si $\mathfrak{g}_i = \mathfrak{q}\mathfrak{r}_i$ et $\mathfrak{g}_j = \mathfrak{q}\mathfrak{r}_j$, alors (a) $\alpha + \xi^i\beta = \lambda\tau_i\rho_i$, avec $\tau_i \in \mathfrak{q}\mathfrak{m}$, $\rho_i \in \mathfrak{r}_i$, et (b) $\alpha + \xi^j\beta = \lambda\tau_j\rho_j$, avec $\tau_j \in \mathfrak{q}\mathfrak{m}$, $\rho_j \in \mathfrak{r}_j$.
2. On résout :

$$\begin{aligned} \beta &= \frac{\lambda}{\xi^i - \xi^j}(\tau_i\rho_i - \tau_j\rho_j) \\ \alpha &= \frac{\lambda}{\xi^i - \xi^j}(\tau_i\rho_i\xi^{-i} - \tau_j\rho_j\xi^{-j}) \end{aligned}$$

3. Comme $\lambda/(\xi^i - \xi^j)$ est une unité, $\mathfrak{q}\mathfrak{m}$ divise α et β, alors que $\mathfrak{m}$ est leur pgcd. $\mathfrak{q}$ est est une unité.

□

Lemme 3.3.8. *Il existe un idéal entier $\mathfrak{a}_j$ tel que : $\mathfrak{g}_j = \mathfrak{a}_j^l$*

Démonstration.

1. On a, en termes d'ideaux : $\mathfrak{m}^l(\lambda)^{lm}\mathfrak{g}_0 \ldots \mathfrak{g}_{l-1} = (\lambda)^{lm}(\gamma)^l$; donc, en simplifiant : $\mathfrak{m}^l\mathfrak{g}_0 \ldots \mathfrak{g}_{l-1} = \gamma^l$.

2. Les $\mathfrak{g}_j$ sont premiers entre eux. D'après **A(l)** : l est régulier et pour tout j, il existe un idéal $\mathfrak{a}_j$ tel que $\mathfrak{g}_j = \mathfrak{a}_j^l$.

□

Lemme 3.3.9. *Il existe $\alpha', \beta', \gamma' \in O_K$, premiers avec λ et des unités μ et κ tels que :*

$$\alpha'^l - \mu\beta'^l = \kappa\lambda^{l(m-1)}\gamma'^l$$

Démonstration. 1. En développant 3.3.6 avec 3.3.8, on obtient les égalités : $(\alpha+\beta) = (\lambda)^{l(m-1)+1}\mathfrak{a}_0^l$ et $(\alpha+\xi^j\beta) = (\lambda)\mathfrak{a}_j^l$. On peut donc écrire en termes d'idéaux fractionnaires : $(\alpha+\xi^j\beta) = (\alpha+\beta)(\lambda)^{-l(m-1)}(\mathfrak{a}_j\mathfrak{a}_0^{-1})^l$.

2. Les idéaux $\mathfrak{g}_j\mathfrak{g}_0^{-1}$ sont principaux : en effet leur puissance l-ème est principale (équation ci-dessus) et d'après la condition **A(l)**, l est premier avec le nombres des classes de O_K.

3. Puisque les idéaux $\mathfrak{g}_j$ sont principaux et premiers avec λ, on a : $\mathfrak{g}_j\mathfrak{g}_0^{-1} = (\alpha_j/\beta_j)$, où α_j et β_j ne sont pas divisibles par λ . D'où : $(\alpha+\xi^j\beta) = (\alpha+\beta)\lambda^{-l(m-1)}(\alpha_j/\beta_j)^l\nu_j$ pour $1 \leq j \leq l-1$, où ν_j est une unité.

4. L'égalité $\xi(\alpha+\beta) = (\alpha+\xi\beta)(1+\xi) - (\alpha+\xi^2\beta)$ devient

$$\xi(\alpha+\beta) \quad = \quad (\alpha+\beta)\lambda^{-l(m-1)}\left((\frac{\alpha_1}{\beta_1})^l\nu_1(1+\xi) - (\frac{\alpha_2}{\beta_2})^l\nu_2\right)$$

En divisant par $\alpha+\beta$, en multipliant par $(\beta_1\beta_2)^l\lambda^{l(m-1)}$, et en

divisant par ν_2, on obtient :

$$\left((\alpha_1\beta_2)^l \frac{\nu_1(1+\xi)}{\nu_2} - (\alpha_2\beta_1)^l\right) = \lambda^{l(m-1)}(\beta_1\beta_2)^l \frac{\xi}{\nu_2}$$

5. On pose $\alpha' = \alpha_1\beta_2$, $\beta' = \alpha_2\beta_1$, $\gamma' = \beta_1\beta_2$, $\mu = \nu_1(1+\xi)/\nu_2$, $\kappa = \xi/\nu_2$. On a alors $\alpha'^l - \mu\beta'^l = \kappa\lambda^{l(m-1)}\gamma'^l$
6. μ et κ sont des unités puisque ν_1, ν_2 et $1+\nu$ sont des unités.
7. α' β', γ' sont premiers avec λ par construction.

□

Lemme 3.3.10. *Il existe une unité ν telle que $\mu = \nu^l$.*

Démonstration.
1. D'après le lemme précédent : $\alpha'^l - \mu\beta'^l \equiv 0 \mod \lambda'^l$.
2. Comme β' et λ'^l sont premiers dans O_K, il existe β'' tel que $\beta'\beta'' \equiv 1 \pmod{\lambda^l}$. En multipliant par β''^l, on obtient : $(\alpha'\beta'')^l - \mu \equiv 0 \pmod{\lambda^l}$.
3. D'après 3.3.1, il existe $a \in \mathbb{Z}$ tel que $-\alpha'\beta'' \equiv a \pmod{\lambda}$.
4. Alors $(-\alpha'\beta'')^l \equiv a^l \pmod{\lambda^l}$. Soit $\mu \equiv a^l \pmod{\lambda^l}$. Comme l divise λ^l, $\mu \equiv a^l \pmod{l}$.
5. La condition **B(l)** implique qu'il existe ν tel que $\mu = \nu^l$.

□

Lemme 3.3.11.

$$\alpha^l + (-\nu\beta)^l = \kappa\lambda^{l(m-1)}\gamma^l$$

Démonstration. Evidente. □

Théoreme 3.3.12. *Si **A(l)** et **B(l)**, l'équation $\alpha^l + \beta^l = \lambda^{lm}\nu\gamma^l$ n'a pas de solution (α, β, γ) dans O_K avec une unité ν et γ premier avec λ.*

Démonstration. Avec la succession des lemmes précédents, une équation du type : $\alpha^l + \beta^l = \lambda^{lm}\nu\gamma^l$ implique une équation du type : $\alpha^l + \beta^l = \lambda^{l(m-1)}\nu\gamma^l$. On arrive ainsi à une solution de l'équation de l'hypothèse 3.3.3 dans laquelle $m = 0$; ce qui est impossible d'après 3.3.5. □

Théoreme 3.3.13. *Si **A(l)** et **B(l)**, l'équation $x^l + y^l = z^l$ n'a pas de solution où l divise z.*

Démonstration.

1. Soit (x, y, z) tels que $x^l + y^l = z^l$ et l divise z.
2. On écrit : $z = l^k z_0$ avec $(l, z_0) = 1$
3. On a : $l = \lambda^{l-1}u$ avec $N(u) = 1$
4. Soit : $x^l + y^l = \left((\lambda^{l-1}u)^k z_0\right)^l$.
5. Soit : $x^l + y^l = \lambda^{lm}\nu z_0^l$ avec $m = k(l-1)$ et $N(\nu) = 1$.
6. Et on a une solution de l'équation $\alpha^l + \beta^l = \lambda^{lm}\nu\gamma^l$.

□

Théoreme 3.3.14. *Si **A(l)** et **B(l)** l'équation $x^l + y^l + z^l = 0$ n'a pas de solution dans laquelle x, y et z sont premiers entre eux et l ne divise pas xyz.*

3.4 Le théorème de Fermat pour les nombres premiers réguliers

Théoreme 3.4.1. *Si **A(l)** et **B(l)**, alors l'équation* $x^l + y^l + z^l = 0$ *n'a pas de solution.*

Démonstration. Conséquence de 3.2.1 et 3.3.14 □

Chapitre 4

Arithmétique cyclotomique

Soit K le l-ème corps cyclotomique.

4.1 Unités

Lemme 4.1.1. $(1-\xi^k)/(1-\xi)$ *est une unité de* O_K

Démonstration. 1. $(1-\xi^k)/(1-\xi)$ s'écrit $1+\xi+\xi^2+\cdots+\xi^{k-1}$, donc est dans O_K.

2. Il existe a et b tels que $ak + bp = 1$.

$$\begin{aligned}(1-\xi)/(1-\xi^k) &= (1-\xi^{ak+bp})/(1-\xi^k)\\ &= (1-\xi^{ak})/(1-\xi^k)\\ &= 1+\xi^k+\xi^{2k}+\cdots+\xi^{(a-1)k} \in O_K\end{aligned}$$

Donc $(1-\xi)/(1-\xi^k) \in O_K$

3. $(1-\xi^k)/(1-\xi)$ et son inverse appartiennent à O_K. Ce sont des unités.

□

Lemme 4.1.2. *l/λ^{l-1} est une unité.*

Démonstration. D'après 2.3.4 : $N(\lambda) = l$, et la définition de λ : $\lambda = 1 - \xi$, on a :

$$\frac{l}{\lambda^{l-1}} = \frac{\prod_{i=1}^{l-1} 1-\xi^i}{\prod_{i=1}^{l-1} 1-\xi} = \prod_{i=1}^{l-1} \frac{1-\xi^i}{1-\xi}$$

□

Lemme 4.1.3. *Pour $\alpha \in O_K$ il existe un entier $a \in \mathbb{Z}$ tel que l divise $\alpha^l - a$.*

Démonstration.

1. Comme $N(\lambda) = l$, λ est premier dans O_K. De plus, $O_K/\lambda O_K$ est isomorphe à $\mathbb{Z}/l\mathbb{Z}$. Il existe donc $b \in \{0, 1, \ldots, l-1\}$ tel que λ divise $\alpha - b$.
2. On écrit $\alpha^l - b^l = \prod_{k=0}^{l-1}(\alpha - \xi^k b)$. On écrit : $\alpha - \xi^k b = \alpha - b + (1-\xi^k)b$. Mais : $1 - \xi^k = (1-\xi)\left((1-\xi^k)/(1-\xi)\right)$ et $\left((1-\xi^k)/(1-\xi)\right)$ est une unité.
3. Donc λ divise chaque $\alpha - \xi^k b$. Donc l qui divise λ^{l-1} divise $\alpha^l - b^l$. Et le résultat avec $a = b^l$.

□

Lemme 4.1.4. *Soit $g \in \mathbb{Z}[X]$ un polynôme unitaire dont les racines dans $\mathbb{C}$ sont de norme 1. Alors ces racines sont des racines de l'unité.*

Démonstration.

1. Soit α_i les racines de g Soit $g_k(X) = \prod_i (X - \alpha_i^k)$
2. Alors $g_k(X) \in \mathbb{Z}[X]$ parce que ses racines sont permutées par les σ_i. On a : $g_k(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0$.
3. Les coefficients a_j sont bornés : ce sont les polynomes symétriques en les racines α_j^k et $|\alpha_j^k| = 1$. Il y a un nombre fini de polynômes de même degré et à coefficients bornés. Donc $g_k = g_h$ pour des entiers $k < h$.
4. Donc il existe une permutation des racines σ telle que $\alpha_j^k = \alpha_{\sigma(j)}^h$. On a alors : $\alpha_j^{(k^2)} = (\alpha_j^k)^k = (\alpha_{\sigma(j)}^h)^k = (\alpha_{\sigma(j)}^k)^h = (\alpha_{\sigma^2(j)}^h)^h = \alpha_{\sigma^2(j)}^{(h^2)}$
5. Mais σ est d'ordre fini o. On a : $\alpha_j^{(k^o)} = \alpha_j^{(h^o)}$, soit : $\alpha_j^{(h^o)-(k^o)} = 1$

□

Lemme 4.1.5. *Si u est une unité de O_K, alors $u = r\xi^k$ où $r \in \mathbb{R}$ et $k \in \mathbb{Z}$*

Démonstration.

1. On a : $\sigma_j(\xi) = \xi^j$, $\overline{\sigma_j(\xi)} = \sigma_{l-j}(\xi)$, $\overline{\sigma_j(\alpha)} = \sigma_{l-j}(\alpha)$ pour $\alpha \in O_K$.
2. On pose : $u_j = \sigma_j(u)$; c'est aussi une unité. On a : $N(u) = u_1u_2 \ldots u_{l-1} = (u_1u_{l-1})(u_2u_{l-2}) \ldots$. Mais $u_iu_{l-i} = u_i\overline{u_i} = |u_i|^2 > 0$. . . .. Donc $N(u) > 0$ et $N(u) = 1$.
3. En tant que division de deux unités, u_j/u_{l-j} est une unité. On en prend la norme : $|u_j/u_{l-j}|^2 = (u_ju_{l-j})/(u_ju_{l-j}) = 1$.

4. Le polynôme $\prod_{j=1}^{l-1}(X - u_j/u_{l-j})$ est dans $\mathbb{Z}(x)$ et toutes ses racines sont de module 1. D'après 4.1.4, ce sont des racines de l'unité : $u/u_{l-1} = \xi^h$
5. l étant impair, h ou $h + l$ est pair. Si h est pair, on pose $h = 2k$. Si $h + l$ est pair, on pose $h + l = 2k$. On peut écrire : $u_1/u_{l-1} = \xi^{2k}$
6. On a dans tous les cas : $u_1\xi^{-k} = u_{l-1}\xi^k$. Les deux sont conjugués. Donc réels.

□

Notation 4.1.6. *Dans toute la suite, on note* $(\epsilon_1, \ldots, \epsilon_r)$ *un système d'unités fondamentales de* K*. D'après 4.1.5, on peut les supposer toutes positives. D'après le théorème des unités (A.5.2), on a :* $r = m - 1$.

Definition 4.1.7. *Le* ***régulateur*** $\mathcal{R}$ *est le volume du parallélotope (de dimension* $(m-1)$ *engendré dans* $\mathbb{R}^m$ *par les images des unités* ϵ_i *par le plongement logarithmique* L*. Il est donné par :*

$$\mathcal{R} = 2^{m-1}\begin{vmatrix} \log|\sigma_1(\epsilon_1)| & \log|\sigma_1(\epsilon_2)| & \ldots & \log|\sigma_1(\epsilon_{m-1})| \\ \log|\sigma_2(\epsilon_1)| & \log|\sigma_2(\epsilon_2)| & \ldots & \log|\sigma_2(\epsilon_{m-1})| \\ \ldots & \ldots & \ldots & \ldots \\ \log|\sigma_{m-1}(\epsilon_1)| & \log|\sigma_{m-1}(\epsilon_2)| & \ldots & \log|\sigma_{m-1}(\epsilon_{m-1})| \end{vmatrix}$$

4.2 Décomposition des idéaux premiers, discriminant et ramification

Lemme 4.2.1. *Avec $m = (l-1)/2$, le discriminant de K est donné par $\mathcal{D} = (-1)^m l^{l-1}$*

Démonstration. On considère la base $1, \xi, \ldots, \xi^{l-2}$. On considère le groupe de Galois sous la forme $\sigma_1, \ldots, \sigma_{l-1}$. Où σ_i est défini par $\sigma(\xi) = \xi^{2i}$. On a :

$$\begin{aligned}
\mathcal{D} &= \begin{vmatrix} \sigma_1(1) & \sigma_2(1) & \ldots & \sigma_{l-1}(1) \\ \sigma_1(\xi) & \sigma_2(\xi) & \ldots & \sigma_{l-1}(\xi) \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_1(\xi^{l-2}) & \sigma_2(\xi^{l-2}) & \ldots & \sigma_{l-1}(\xi^{l-2}) \end{vmatrix} \\
&= \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \xi^2 & \xi^4 & \ldots & \xi^{2(l-2)} \\ \ldots & \ldots & \ldots & \ldots \\ \xi^{2(l-1)} & \xi^{4(l-1)} & \ldots & \xi^{2(l-2)(l-1)} \end{vmatrix} \\
&= \prod_{1 \le i < j \le l-1} (\xi^{2i} - \xi^{2j}) = \prod_{1 \le i < j \le l-1} \xi^{2i}(1 - \xi^{2(j-i)}) \\
&= \prod_{1 \le i < j \le l-1} \xi^{2i} \prod_{1 \le i < j \le l-1} (1 - \xi^{2(j-i)}) = (-1)^{\frac{l-1}{2}} l^{l-1}
\end{aligned}$$

□

Lemme 4.2.2. *p se ramifie dans O_K si et seulement si il divise l*

Démonstration. D'après A.3.33, p se ramifie dans O_K si et seulement si il divise $\mathfrak{D} = (-1)^m l^{l-1}$. □

Lemme 4.2.3. *En termes d'idéaux, on a :* $lO_K = (\lambda)^{l-1}$.

Démonstration. D'après 4.1.2 □

Lemme 4.2.4. *Soit p premier avec l. Le résidu modulo p de $\Phi_l(X)$ n'a pas de racines doubles dans $\mathbb{F}_p$.*

Démonstration. Soit $H(X) = X^l - 1$. On a $H'(X) = lX^{l-1}$ et $pH(X) - XH'(X) = l$. Comme l est inversible dans $\mathbb{F}_p$, $H(X)$ et $H'(X)$ y sont premiers entre eux, n'y ont pas de racines communes, et $H(X)$ n'y a pas de racines doubles. Or Φ_l divise H. □

Lemme 4.2.5. *Si $\mathfrak{P}$ ne divise pas l, alors* $N(\mathfrak{P}) \equiv 1 \pmod{l}$.

Démonstration. Soit p qui est au dessus $\mathfrak{P}$. On a vu que $\overline{X^l - 1}$ n'a pas de racines doubles dans $\mathbb{F}_p$: les l racines $\overline{1}, \overline{\xi}, \ldots, \overline{\xi^{l-1}}$ sont deux à deux distinctes. Elles forment un sous groupe multiplicatif de $\mathbb{F}_p^*$. Celui-ci est d'ordre $N(\mathfrak{P}) - 1$. Donc l divise $N(\mathfrak{P}) - 1$. □

Definition 4.2.6. *Soit p premier avec l. L'**exposant** de p modulo l est le plus petit nombre naturel $f_p > 0$ tel que $p^{f_p} \equiv 1 \mod l$. Il est clair que f_p divise $(l-1)$. Soit $g_p = (l-1)/f_p$.*

Lemme 4.2.7. *Soit p premier avec l. Alors, p a g_p diviseurs premiers. On a $pO_K = \mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_{g_p}$ et $N(\mathfrak{P}_k) = p^{f_p}$.*

Démonstration. 1. Dans O_K, on a une factorisation $p = \mathfrak{P}_1 \dots \mathfrak{P}_g$. Soit $\mathfrak{P}$ un de ces diviseurs et s son degré : $N(\mathfrak{P}) = p^s$. D'après 4.2.5, $p^s \equiv 1 \pmod{l}$. Donc $s \geq f_p$.

2. Chacun des p^s éléments de $O_K/\mathfrak{P}$ est le résidu d'un entier de O_k de la forme

$$\kappa = \sum_{j=0}^{l-2} a_j \xi^j$$

On élève κ à la puissance p^{f_p} ; comme $p^{f_p} \equiv 1 \pmod{l}$, $\xi^{p^{f_p}} = \xi$; comme, pour $\alpha, \beta \in O_K$ $(\alpha + \beta)^{p^{f_p}} \equiv \alpha^{p^{f_p}} + \beta^{p^{f_p}} \pmod{\mathfrak{P}}$, pour $a \in \mathbb{Z}$, on a : $a^{p^{f_p}} \equiv a \pmod{\mathfrak{P}}$. On en déduit que

$$\kappa^{p^{f_p}} \equiv \kappa \pmod{\mathfrak{P}}$$

Donc chacun des $\overline{\kappa}$ est une racine de $X^{p^{f_p}}$ dans $O_K/\mathfrak{P}$. Mais dans tout corps, le nombre de racines n'excède pas le degré, d'ou $p^s \leq p^{f_p}$.

3. Donc $s = f_p$.

4. On prend la norme de la décomposition de p :

$$\begin{aligned} N(p) &= N(\mathfrak{P}_1) \dots N(\mathfrak{P}_g) \\ p^{l-1} &= p^{f_p} \dots p^{f_p} = p^{g \times f_p} \end{aligned}$$

Et le résultat puisque $g_p = (l-1)/f_p$.

□

4.3 Unités cyclotomiques

Notation 4.3.1. *Soit* $\rho = e^{\frac{i\pi}{l}} = \xi^m$.

Definition 4.3.2. *Soit* $1 \leq k < m$. *Une* ***unité cyclotomique*** *est une unité de la forme :*

$$\eta_k = \frac{\xi^k - 1}{\xi - 1}\rho^{1-k} = \frac{\xi^k - 1}{\xi - 1}(-\xi^m)^{1-k} = \frac{\xi^k - 1}{\xi - 1}\xi^{m(1-k)}(-1)^{1-k}$$

Lemme 4.3.3. ρ *est une racine de* 1 *contenue dans* K.

Démonstration. $(l-1)$ est pair. □

Lemme 4.3.4. *Une unité cyclotomique est réelle et positive.*

Démonstration.

$$\eta_k = \frac{e^{\frac{2ik\pi}{l}} - 1}{e^{\frac{2\pi}{l}} - 1} \times \frac{e^{\frac{i\pi}{l}}}{e^{i\frac{k\pi}{l}}} = \frac{e^{i\frac{k\pi}{l}} - e^{-i\frac{k\pi}{l}}}{e^{i\frac{\pi}{l}} - e^{-i\frac{\pi}{l}}} = \frac{\sin\frac{k\pi}{l}}{\sin\frac{\pi}{l}}$$

□

Lemme 4.3.5. *Une unité est cyclotomique si et seulement si elle peut se mettre sous la forme*

$$\pm\xi^j \prod_{k=1}^{m} (1 - \xi^{q^k})^{n_k}$$

avec $\sum_{k=1}^{m} n_k = 0$.

Démonstration. 1. La démonstration consiste à associer un nombre $h \in [1, m-1]$ à un nombre $k \in [1, m-1]$ tel que $\pm q^k \equiv h \pmod{l}$. Chacune de ces associations se résume à changer une expression de signe et à la multiplier par une racine de l'unité : si $-q^k \equiv h \pmod{l}$, on écrit $1 - \xi^h = 1 - \xi^{-q^k} = -\xi^{-q^k}(1 - \xi^{q^k})$; si $q^k \equiv h \pmod{l}$, on écrit $1 - \xi^h = 1 - \xi^{q^k}$.

2. Par ailleurs $q^m \equiv -1 \pmod{l}$; donc $1 - \xi = \xi(\xi^{-1} - 1) = -\xi(1 - \xi^{q^m})$. La encore, il s'agit de changer une expression de signe et de la multiplier par une racine de l'unité

3. Soit η_h une unité cyclotomique. Elle peut s'écrire :

$$\eta_h \quad = \quad \pm(1 - \xi^{q^k})^1 (1 - \xi^{q^m})^{-1} \xi^j$$

4. Soit θ un nombre cyclotomique tel que défini dans le lemme : On a :

$$\prod_{k=1}^{m} (1 - \xi)^{n_k} \quad = \quad (1 - \xi)^{\sum_{k=1}^{m} n_k} = (1 - \xi)^0 = 1$$

Donc

$$\begin{aligned} \theta \quad &= \quad \pm\xi^j \prod_{k=1}^{m} \left(\frac{1 - \xi^{q^k}}{1 - \xi} \right)^{n_k} = \pm\xi^j \prod_{k=1}^{m-1} \left(\frac{1 - \xi^{q^k}}{1 - \xi} \right)^{n_k} \left(\frac{1 - \xi^{q^m}}{1 - \xi} \right)^{n_m} \\ &= \quad \pm\xi^j \prod_{k=1}^{m} \left(\frac{1 - \xi^{q^k}}{1 - \xi} \right)^{n_k} = \pm\xi^j \prod_{h=1}^{m-1} \eta_h^{n_k} \left(\frac{1 - \xi^{q^m}}{1 - \xi} \right)^{n_m} = \pm\xi^j \prod_{h=1}^{m-1} \eta_h^{n_k} \end{aligned}$$

□

Chapitre 5

Nombre de classes de $\mathbb{Q}(\xi)$

Le but de ce chapitre est de donner une formule pour le nombre de classes $h(K)$ d'un corps $K = \mathbb{Q}[\xi]$.

Nous donnons la démonstration pour $\mathbb{Q}[\xi]$. En fait, un résultat similaire est valide pour tout corps de nombres algébriques, et la démonstration est à peine plus compliquée.

Soient $m = (l-1)/2$ et $\Re$ le régulateur de l'extension $[K : \mathbb{Q}]$. Nous allons définir la fonction ζ_K associée au corps K et montrerons que

$$\lim_{s\to 1}(s-1)\zeta_K(s) \quad = \quad h(K)\frac{2^{m-1}\pi^m\Re}{l^{m+1}}$$

donc que :

$$h(K) \quad = \quad \frac{l^{m+1}}{2^{m-1}\pi^m\Re}\lim_{s\to 1}(s-1)\zeta_K(s)$$

Nous calculerons

$$\lim_{s\to 1}(s-1)\zeta_K(s)$$

Nous en déduirons que $h(K)$ peut s'écrire :

$$h(K) \quad = \quad \frac{2^{m-1}}{\Re}\prod_{k=1}^{m-1}\left|\sum_{p=0}^{m-1}\theta^{2kr}\log|1-\xi^{q^p}|\right| \times \frac{1}{(2l)^{m-1}}\prod_{k=1,m-1}\left|F(\theta^{2k-1})\right|$$

Les termes de cette formule sont les suivants :

1. $q \in \mathbb{Z}$ est une racine primitive $l-1$-ième. On a $q^{l-1} \equiv 1 \pmod{l}$ et $q^j \not\equiv 1 \pmod{l}$ pour $1 \leq j \leq l$. Modulo l, les deux ensembles $0, 1, 2, \ldots, l-1$ et $1, q, q^2, q^3, \ldots, q^{l-2}$ sont les mêmes.
2. q_s est le plus petit résidu de q^s modulo m et F est le polynôme $F(x) = \sum_{k=0}^{l-2} q_s x^s$.
3. $\theta \in \mathbb{C}$ est une racine de 1 d'ordre $l-1$.

Nous utilisons dans la démonstration les définitions et résultats vus dans le chapitre 2 :

1. $\mathfrak{D}$ est le discriminant de l'extension $[K : \mathbb{Q}]$;
2. G est le groupe de Galois de K sur $\mathbb{Q}$. Soit σ un générateur de ce groupe. On a $G = \{1, \sigma, \sigma^2, \ldots, \sigma^{l-2}\} = \{1, \sigma^q, \sigma^{q^2}, \ldots, \sigma^{q^{l-2}}\}$

Lemme 5.0.1. *Le nombres de racines de l'unité contenues dans K est 2l.*

Démonstration. Ce sont les nombres de la forme $\pm\xi^k, 0 \leq k < l$. En posant $\rho = e^{i\pi/l}$, ce sont les nombres de la forme $\rho^k, 0 \leq k < 2l-1$

□

5.1 La fonction ζ_K

Definition 5.1.1. *La fonction ζ_K est, la somme étant étendue à tous les idéaux entiers de O_K, définie par :*

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$$

Notation 5.1.2. *Soit $\mathfrak{C}$ une classe d'idéaux de K, on note :*

$$\zeta_{K,\mathfrak{C}}(s) \quad = \quad \sum_{\mathfrak{a}\in\mathfrak{C}} N(\mathfrak{a})^{-s}$$

On a évidemment :

$$\zeta_K(s) = \sum_{\mathfrak{C}} \zeta_{K,\mathfrak{C}}(s)$$

Nous allons montrer que pour toute classe d'idéaux $\mathfrak{C}$, on a :

$$\lim_{s\to 1^+} (s-1)\zeta_{K,\mathfrak{C}}(s) = \frac{2^{m-1}\pi^m \mathfrak{R}}{l^{m+1}}$$

Donc que :

$$\lim_{s\to 1}(s-1)\zeta_K(s) \quad = \quad h(K)\frac{2^{m-1}\pi^m\Re}{l^{m+1}}$$

5.2 Domaine fondamental

Pour démontrer que

$$\lim_{s\to 1^+}(s-1)\zeta_{K,\mathfrak{C}}(s) = \frac{2^{m-1}\pi^m\Re}{l^{m+1}}$$

nous allons caractériser les classes d'idéaux à l'aide du plongement logarithmique vu dans l'appendice sur les entiers algébriques.

Lemme 5.2.1. *Soit L le plongement logarithmique de K dans $\mathbb{R}^m$. Soit $\epsilon_1, \ldots, \epsilon_{m-1}$ un système d'unités fondamentales. Soit $U = (1, \ldots, 1) \in \mathbb{R}^m$. Alors $\{U, L(\epsilon_1), \ldots, L(\epsilon_{m-1})\}$ constitue une base de $\mathbb{R}^m$.*

Démonstration. Les images des unités fondamentales par le plongement logarithmique, $L(\epsilon_i)$ forment une base de $\{x = (x_i) \in \mathbb{R}^m \mid \sum_i x_i = 0\}$. Le vecteur U n'appartient pas à ce sous espace, donc l'ensemble $\{U, L(\epsilon_1), \ldots, L(\epsilon_{m-1})\}$ constitue une base de $\mathbb{R}^m$. Tout $x \in \mathbb{R}^m$ s'écrit de façon unique $x = a_0U + a_1L(\epsilon_1) + \cdots + a_{m-1}L(\epsilon_{m-1})$. □

Definition 5.2.2. *Le **domaine fondamental** de K est l'ensemble $X \subset \mathbb{C}^m$ constitué des éléments : $z = (z_1, \ldots, z_m) \subset \mathbb{C}^m$ tels que*

1. $N(z) = \prod_{i=1}^m z_i \neq 0$.

2. *Si* $L(z) = y_0 U + \sum_{i=1}^{m-1} y_i L(\epsilon_i)$ *alors* $0 \leq y_i < 1$ *pour* $0 < i < m$.
3. $0 \leq Arg(z_1) \leq \pi/l$. *On a :*

Lemme 5.2.3. *X est un cône de* $\mathbb{C}^m$.

Démonstration. Il faut montrer que si $z \in X$, si $a \in \mathbb{R}^+$, alors $az \in X$.

1. $N(az) = a^m N(z) \neq 0$.
2. $L(az) = (\log a)U + L(z)$.
3. L'argument de la première composante de az et celui de z sont les mêmes.

□

Lemme 5.2.4. *Tout* $z = (z_1, \ldots, z_m) \in \mathbb{C}^m$ *s'écrit de façon unique* $z = x + L(\nu)$ *où* $x \in X$ *et* ν *est une unité de K.*

Démonstration. Existence et unicité.

1. Existence. Soit k tel que l'argument de z_1 vérifie $0 \leq Arg(z_1) - k\pi/l < \pi/l$. On écrit :

$$L(z) \quad = \quad y_0 U + y_1 L(\epsilon_1) + \cdots + y_{m-1} L(\epsilon_{m-1})$$

Pour $0 < j \leq m-1$, on pose $y_j = k_j + t_j$ avec $k_j \in \mathbb{Z}$ et $t_j \in [0, 1]$. On écrit que :

$$\nu \quad = \quad \xi^k \epsilon_1^{k_1} \ldots \epsilon_{m-1}^{k_{m-1}}$$

Soit $x = z\xi^{-k}$. Alors $x \in X$. En effet $L(x) = L(z) + L(\xi^{-k}) = y_0U + t_1L(\epsilon_1) + \cdots + t_{m-1}L(\epsilon_{m-1})$ et $Arg(x_1) = Arg(z_1) - k\pi/l$.

2. Unicité. On a $L(\xi^k) = \left(\log|\sigma_1(\xi^k)|, \ldots, \log|\sigma_m(\xi^k)|\right) = (0, \ldots, 0)$. Si $x + L(\nu) = x' + L(\nu')$, alors :

$$\begin{aligned} L(x) &= t_0U + t_1L(\epsilon_1) + \cdots + t_{m-1}L(\epsilon_{m-1}) \\ L(x') &= t'_0U + t'_1L(\epsilon_1) + \cdots + a'_{m-1}L(\epsilon_{m-1}) \\ L(\nu) &= k_1L(\epsilon_1) + \cdots + k_{m-1}L(\epsilon_{m-1}) \\ L(\nu') &= k'_1L(\epsilon_1) + \cdots + k'_{m-1}L(\epsilon_{m-1}) \end{aligned}$$

Les k_i sont entiers. Les t_i sont réels, positifs, inférieurs à 1. On a donc $L(\nu) = L(\nu')$. Donc ν/ν' est une racine des $2l$ racines de 1. En comparant les coefficients de la composante de $L(\epsilon_1)$, $t_1 = t'_1 + k\pi/l$. Et ceci n'est possible que si $k = 0$.

□

Lemme 5.2.5. *Pour tout $\alpha \in O_K$, il existe un unique $\beta \in O_K$ et une unité ν, tels que $\alpha = \beta\nu$ et $L(\beta) \in X$.*

Démonstration.

1. On écrit $L(\alpha) = z + L(\nu)$ avec une unité ν et $z \in X$
2. On pose $\beta = \alpha/\nu$.
3. On a $L(\beta) = L(\alpha) - L(\nu) = z \in X$

□

Lemme 5.2.6. *Soit ν une unité et $S \subset \mathbb{C}^m$. Alors $\mu(S) = \mu(L(\nu)S)$.*

Démonstration. Le déterminant de l'application $y \to L(x)y$ est égal à la norme de x pour tout $x \in O_K$. □

Notation 5.2.7. *On note*

1. $T \subset X \subset \mathbb{C}^m$ *l'ensemble des* x *tels que* $N(x) \leq 1$.
2. $T_k = L(\rho^k)T$, *pour* $0 \leq k \leq l-1$.
3. V, *la réunion des* T_k.

Lemme 5.2.8. *Les ensembles T_k sont disjoints.*

Démonstration. La multiplication par $L(\rho^k)$ conserve la norme. Elle ne change que le terme a_0 dans l'expression d'un élément de $\mathbb{C}^m$ sur la base $(U, L(\epsilon_i))$. Elle ajoute $k\pi/l$ à l'argument de la première composante. □

Lemme 5.2.9. $\mu(V) = (2l) \times \mu(T)$

Démonstration. Pour chaque k, on a : $\mu(T) = \mu(T_k)$ et il y a deux $2l$ valeurs possibles de k. □

Lemme 5.2.10. V *est l'ensemble des* $x \in \mathbb{C}^m$ *tels que* $L(x) = a_0U + a_1L(\epsilon_1) + \ldots a_mL(\epsilon_m)$ *avec avec* $0 \leq a_i < 1$ *pour* $i > 0$, *et* $0 < \log(N(x) < 1$.

Démonstration. Lemmes précédents. □

Lemme 5.2.11. *Soit* $\Re$ *le régulateur de* K. *Alors :* $\mu(V) = \pi^m\Re$.

Démonstration. Par définition, $\Re$ est le volume du parallelotope engendré dans $\mathbb{R}^m$par les $L(\epsilon_i)$, $1 \leq i \leq m-1$. On considère le changement de variable $(x_i, y_i) \to (\rho_i, \theta_i)$. Les conditions sur V deviennent $0 < \rho_i \leq 1$ et $0 \leq \theta_i \leq 2\pi$. Le Jacobien de ce changement de variable est $\Re/(\rho_1..\rho_m)$

$$\begin{aligned}\mu(V) &= \int_0^{2\pi} \partial\theta_1 \ldots \int_0^{2\pi} \partial\theta_m \int_0^1 \rho_1 \partial\rho_1 \ldots \int_0^1 \rho_m \partial\rho_m \\ &= \pi^m \Re \int_0^1 \partial\xi_1 \ldots \int_0^1 \partial\xi_m = \pi^m \Re\end{aligned}$$

□

Lemme 5.2.12.

$$\mu(T) = \frac{\pi^m \Re}{2l}$$

Démonstration. Lemmes précédents. □

5.3 Nombre de classes de K

Lemme 5.3.1. *Soit $\mathfrak{C}$ une classes d'idéaux. Soit $\mathfrak{b}$ dans $\mathfrak{C}^{-1}$.*

$$\zeta_{K,\mathfrak{C}}(s) = N(\mathfrak{b})^s \sum_{\substack{(\alpha) \\ \alpha \equiv 0 \pmod{\mathfrak{b}}}} |N(\alpha)|^{-s}$$

Démonstration. Pour tout $\mathfrak{a} \in \mathfrak{C}$, $\mathfrak{ab}$ est principal : $\mathfrak{ab} = (\alpha)$. Il y a bijection entre les éléments de $\mathfrak{C}$ et les entiers non associés (i.e. à

une unité près) de O_K tels que $\alpha \in \mathfrak{b}$. On a de plus $|N(\alpha)| = N(\mathfrak{a}\mathfrak{b})$. La sommation est prise sur les entiers non associés de O_K. D'où le résultat.

$$\zeta_{K,\mathfrak{C}}(s) = \sum_{\mathfrak{a}\in\mathfrak{C}} N(\mathfrak{a})^{-s} = N(\mathfrak{b})^s \sum_{\substack{(\alpha) \\ \alpha\equiv 0 \pmod{\mathfrak{b}}}} |N(\alpha)|^{-s}$$

□

Lemme 5.3.2. *Soit $M_\mathfrak{b} \subset \mathbb{R}^{l-1}$ l'image par le plongement canonique C de l'ensemble des entiers $\alpha \in O_K$ divisibles par $\mathfrak{b}$. Le volume du parallélépipède fondamental de $M_\mathfrak{b}$ est donné par*

$$W_b = \frac{l^m}{2^m} N(\mathfrak{b})$$

Démonstration. Découle de la valeur de $\mathfrak{D} : \mathfrak{D} = l^{l-1}$ et de A.4.8. □

Lemme 5.3.3. *On a :*

$$\zeta_{K,\mathfrak{C}}(s) = N(\mathfrak{b})^s \sum_{x\in M_\mathfrak{b} \bigcap X} |N(x)|^{-s}$$

Démonstration. Pour $(\alpha) \in O_K$, $\alpha \equiv 0 \pmod{\mathfrak{b}}$, il existe $x \in M_\mathfrak{b} \bigcap X$ tel que $x = C(\alpha)$, où X est le domaine fondamental vu plus haut. Deux entiers sont associés si et seulement s'il leur correspond le même élément x. Alors, comme $N(\alpha) = N(C(\alpha))$, on a le résultat. □

Lemme 5.3.4. *On a*

$$\lim_{s\to 1^+}(s-1)\zeta(s)=1$$

Démonstration. Un des premiers résultats de la théorie de la fonction ζ □

Lemme 5.3.5. *Pour toute classe d'idéaux $\mathfrak{C}$, on a :*

$$\lim_{s\to 1^+}(s-1)\zeta_{K,\mathfrak{C}}(s)=\frac{2^{m-1}\pi^m\mathfrak{R}}{l^{m+1}}$$

Démonstration. On utilise le théorème 5.6.1, donné en appendice, dans lequel

1. le cône X est le domaine fondamental.
2. la fonction f est donnée par $f(x)=|N(x)|^{-s}$. D'après 5.2.12, l'ensemble T des éléments de norme ≤ 1 est de volume est $V=\pi^m\mathfrak{R}/(2l)$.
3. le réseau est $M_{\mathfrak{b}}$. D'après 5.3.2, le volume de son parallélépipède est donné par $W_{\mathfrak{b}}=N(\mathfrak{b})l^m/2^m$.

On a :

$$\begin{aligned}
\lim_{s\to 1^+}(s-1)\zeta_{K,\mathfrak{C}}(s) &= \lim_{s\to 1^+}(s-1)N(\mathfrak{b})^s \sum_{x\in M_\mathfrak{b}\bigcap X}|N(x)|^{-s} \\
&= N(\mathfrak{b})\lim_{s\to 1^+}(s-1)\sum_{x\in M_\mathfrak{b}\bigcap X}|N(x)|^{-s} \\
&= N(\mathfrak{b})\frac{V}{W_b} \\
&= N(\mathfrak{b})\frac{\pi^m\Re}{2l}/\frac{N(\mathfrak{b})l^m}{2^m} \\
&= \frac{2^{m-1}\pi^m\Re}{l^{m+1}}
\end{aligned}$$

□

Théoreme 5.3.6.

$$h(K) = \frac{l^{m+1}}{2^{m-1}\pi^m\Re}\lim_{s\to 1}(s-1)\zeta_K(s)$$

Démonstration. Découle de 5.3.5. □

5.4 Fonction ζ_K et fonctions L

Le but de cette section est d'expliciter

$$\lim_{s\to 1}(s-1)\zeta_K(s)$$

5.4.1 Décomposition

Lemme 5.4.1.

$$\zeta_K(s) = \prod_{\mathfrak{L}} \frac{1}{1 - N(\mathfrak{L})^{-s}}$$

Démonstration. La même que pour la fonction ζ, la norme étant multiplicative, les idéaux premiers engendrant les idéaux entiers de O_K. □

Lemme 5.4.2.

$$\prod_{\mathfrak{L}|l} (1 - N(\mathfrak{L})^{-s}) = 1 - l^{-s}$$

Démonstration. D'après 4.1.2, $\lambda = 1 - \xi$ est le seul diviseur premier de l et $N(\lambda) = l$. □

Lemme 5.4.3. *Si p ne divise pas l,*

$$\prod_{\mathfrak{P}|p} (1 - N(\mathfrak{P})^{-s}) \quad = \quad \left(1 - p^{-f_p s}\right)^{g_p}$$

Démonstration. Soit $\mathfrak{P}$ est un des diviseurs de p. D'après 4.2.7, $N(\mathfrak{P}) = p^{f_p}$ où f_p est l'exposant de p modulo l et il existe $g_p = (l-1)/f_p$ tels diviseurs. □

5.4.2 Fonctions L

Definition 5.4.4. *A un caractère modulo l, χ , on associe la fonction L_χ :*

$$L_\chi(s) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}$$

Lemme 5.4.5. *Si $\chi \neq \chi_0$, L_χ converge pour $\Re(s) > 0$. En particulier pour $s = 1$.*

Démonstration. Découle de la formule sommatoire d'Abel. □

Lemme 5.4.6.

$$L_\chi(s) = \prod_{j=0}^{l-2} \frac{1}{1-\chi(l)l^{-s}}$$

Démonstration. Même démonstration que pour ζ. □

Lemme 5.4.7. *On a :*

$$L_{\chi_0}(s) = (1-l^{-s})\zeta(s)$$

Démonstration. Définition de χ_0. □

Lemme 5.4.8. *Soit p premier avec l ; on a :*

$$\left(\frac{1}{1-p^{-f_p s}}\right)^{g_p} = \prod_{j=0}^{l-2}(1-\chi_j(p)l^{-s})$$

Démonstration. Pour tout caractère χ, $\chi(p)$ est une racine d'ordre f_p de 1 : $\chi(p) = \epsilon^k$. Réciproquement, pour toute racine ϵ^k, il existe et un seul caractère χ tel que $\chi(p) = 1$. Donc lorsque χ parcourt les caractères, $\chi(p)$ parcourt les racines ϵ^k, $k = 0, 1, \ldots, f_p - 1$. Chacune des racines est obtenue $g_p = (p-1)/f_f$ fois.

$$\begin{aligned} 1 - (p^{-s})^{f_p} &= \prod_{k=0}^{f_p-1} (1 - \xi^k p^{-s}) \\ \prod_{k=0}^{f_p-1} (1 - \xi^k p^{-s})^{g_p} &= \prod_{j=0}^{l-2} (1 - \chi_j(p) l^{-s}) \end{aligned}$$

□

Théoreme 5.4.9.

$$\zeta_K(s) = \zeta(s) \prod_{\chi \neq \chi_0} L_\chi(s)$$

Démonstration. 1. Par définition :

$$\zeta_K(s) = \prod_{\mathfrak{Q}} \frac{1}{1 - N(\mathfrak{Q})^{-s}} = \prod_{\mathfrak{Q}|l} \frac{1}{1 - N(\mathfrak{Q})^{-s}} \prod_{p \neq l} \prod_{\mathfrak{P}|p} \frac{1}{1 - N(\mathfrak{Q})^{-s}}$$

2. D'après 5.4.2,

$$\prod_{\mathfrak{Q}|l} \frac{1}{1 - N(\mathfrak{Q})^{-s}} = \frac{1}{1 - l^{-s}}$$

3. D'après 5.4.3, si p ne divise pas l,

$$\prod_{\mathfrak{P}|p} \frac{1}{1 - N(\mathfrak{P})^{-s}} = \left(\frac{1}{1 - p^{-f_p s}}\right)^{g_p}$$

4. D'après 5.4.8

$$\left(\frac{1}{1 - p^{-f_p s}}\right)^{g_p} = \prod_{j=0}^{l-2} (1 - \chi_j(p) l^{-s})$$

5. On écrit :

$$\begin{aligned} \zeta_K(s) &= \frac{1}{1 - l^{-s}} \prod_{j=0}^{l-2} \prod_{p} \frac{1}{1 - \chi_j(p) l^{-s}} \\ &= \frac{1}{1 - p^{-s}} \prod_{j=0}^{l-2} L_{\chi_j}(s) \\ &= \zeta(s) \prod_{j=1}^{l-2} L_{\chi_j}(s) \end{aligned}$$

□

Théoreme 5.4.10.

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \prod_{j=1}^{l-1} L_{\chi_j}(1)$$

Démonstration. On sait que $\lim_{s \to 1}(s-1)\zeta(s) = 1$. On utilise 5.4.5.

□

5.4.3 Valeurs des fonctions L en $s = 1$

Lemme 5.4.11.

$$L_{\chi_j}(1) = -\frac{1}{l}\sum_{k=1}^{l-1}\tau_k(\chi_j)\log(1-\xi^{-k})$$

Démonstration. On pose $c_{nx} = 1$ si $n \equiv x \pmod{l}$ et $c_{nx} = 0$ sinon. On a :

$$L_{\chi_j}(s) = \sum_{(x,l)=1}\chi_j(x)\sum_{n\equiv x \pmod{l}} n^{-s} = \sum_{(x,l)=1}\chi_j(x)\sum_n c_{nx}n^{-s}$$

Mais :

$$c_{nx} = \frac{1}{l}\sum_{k=0}^{l-1}\xi^{(x-n)k}$$

D'où :

$$\begin{aligned} L_{\chi_j}(s) &= \sum_{(x,l)=1}\chi_j(x)\sum_n c_{nx}n^{-s} = \sum_{(x,l)=1}\chi_j(x)\sum_n\frac{1}{l}\sum_{k=0}^{l-1}\xi^{(x-n)k}n^{-s} \\ &= \frac{1}{l}\sum_{k=0}^{m-1}\left(\sum_{(x,l)=1}\chi_j(x)\xi^{xk}\right)\sum_n\xi^{-nk}n^{-s} = \frac{1}{l}\sum_{k=0}^{l-1}\tau_k(\chi_j)\sum_n\xi^{-nk}n^{-s} \end{aligned}$$

Pour $s = 1$:

$$\sum_n \xi^{-nk} \frac{1}{n} = -\log(1 - \xi^{-k})$$

Et le résultat. □

Lemme 5.4.12.

$$L_{\chi_j}(1) = -\frac{\tau(\chi_j)}{l} \sum_{k=1}^{l-1} \overline{\chi_j}(k) \log(1 - \xi^{-k})$$

Démonstration.

$$\tau_k(\chi_j) = \overline{\chi}(k)\tau(\chi_j)$$

□

Lemme 5.4.13. *Soit k, tel que $|k| \leq l$, $(k, l) = 1$. Alors :*

$$\begin{aligned}
\log(1 - \xi^{-k}) &= \log|1 - \xi^{-k}| + i\pi\left(\frac{1}{2} - \frac{k}{l}\right) \\
\log(1 - \xi^{k}) &= \log|1 - \xi^{k}| - i\pi\left(\frac{1}{2} - \frac{k}{l}\right) \\
\log|1 - \xi^{-k}| &= \log|1 - \xi^{k}|
\end{aligned}$$

Démonstration. Dans le cercle trigonométrique, comme dans tout cercle, l'angle au centre est le double de l'angle inscrit. L'argument de $(1 - \xi^k)$ vaut $-\pi\left(\frac{1}{2} - \frac{k}{p}\right)$. Enfin $\log|1 - \xi^{-k}|$ et $\log|1 - \xi^k$ sont

conjugués l'un de l'autre. □

Notation 5.4.14. *On pose :*

$$S_j = \sum_{k=1}^{l-1} \overline{\chi_j}(k) \log(1-\xi^{-k})$$

Lemme 5.4.15. *Soit χ_{2j} un caractère pair.*

$$L_{\chi_{2j}}(1) = -\frac{\tau(\chi_{2i})}{l} \sum_{k=1}^{l-1} \overline{\chi_{2i}}(k) \log(1-\xi^{-k})$$

Démonstration. On remplace k par $-k$:

$$S_{2j} = \sum_{k=1}^{l-2} \overline{\chi}^{2j}(k) \log(1-\xi^{-k})$$

On somme les deux expressions de S_{2j} :

$$\begin{aligned} 2S_{2j} &= \sum_{k=1}^{l-1} \overline{\chi}_{2j}(k) \left(\log(1-\xi^{-k}) + \log(1-\xi^{k}) \right) \\ &= 2 \sum_{k=1}^{l-1} \overline{\chi_{2j}}(k) \log|1-\xi^{-k}| \end{aligned}$$

Et :

$$L_{\chi_{2i}}(1) = -\frac{\tau(\chi_{2i})}{l} S_{2j} = -\frac{\tau(\chi_{2i})}{l} \sum_{k=1}^{l-1} \overline{\chi_{2i}}(k) \log|1-\xi^{-k}|$$

$$\left|L_{\chi_{2i}}(1)\right| = \frac{|\tau(\chi_{2i})|}{l}\left|\sum_{k=1}^{l-1}\overline{\chi_{2i}}(k)\log(1-\xi^{-k})\right|$$

□

Lemme 5.4.16. *Soit χ_{2j} un caractère pair.*

$$\left|L_{\chi_{2j}}(1)\right| = \frac{2}{\sqrt{l}}\left|\sum_{p=0}^{l-2}\theta^{2jp}\log|1-\xi^{q^p}|\right|$$

Démonstration. On utilise le lemme précédent, la formule donnant la norme d'une somme de Gauss. □

Lemme 5.4.17. *Les deux ensembles $\{1,2,\ldots,l-1\}$ et $\{q,q^2,\ldots,q^{l-1}\}$ sont identiques modulo l.*

Démonstration. Par définition d'une unité principale modulo l. □

Notation 5.4.18. *On note q_j tel que $1 \leq q_j \leq l$ et $q^j \equiv q_j \pmod{l}$.*

Lemme 5.4.19. *$j \to q_j$ est une permutation de $\{1,2,\ldots,l-1\}$.*

Démonstration. Evidente. □

Notation 5.4.20. *Dans toute la suite on note F le polynôme défini par $F(X) = \sum_{k=0}^{l-2} q_k X^k$ où q_k est le plus petit entier positif congru à q^k modulo l.*

Lemme 5.4.21. *Soit χ_{2j-1} un caractère impair.*

$$\left|L_{\chi_{2j-1}}(1)\right| = \frac{\pi\sqrt{l}}{l^2}\left|F(\theta^{2j-1})\right|$$

Démonstration. De la même façon :

$$S_{2j-1} = \sum_{k=1}^{l-1}\overline{\chi_{2j-1}(k)}\log(1-\xi^{-k}) = -\sum_{k=1}^{l-1}\overline{\chi_{2j-1}(k)}\log(1-\xi^{k})$$

$$2S_{2j-1} = \sum_{\substack{k=1\\(k,l)=1}}^{l-1}\overline{\chi_{2j-1}(k)}\left(2i\pi\left(\frac{1}{2}-\frac{k}{l}\right)\right) \; car \log|1-\xi^{-k}| = \log|1-\xi^{-k}|$$

Mais :

$$\sum_{\substack{k=1\\(k,l)=1}}^{l-1}\overline{\chi_{2j-1}(k)} = 0$$

Donc

$$\begin{aligned} S_{2j-1} &= -\frac{i\pi}{l}\sum_{\substack{k=1\\(k,l)=1}}^{l-1} k\overline{\chi_{2j-1}(k)} \\ &= -\frac{i\pi}{l}\sum_{n=0}^{l-2} q_s\overline{\chi_{2j-1}(q_s)} \\ &= -\frac{i\pi}{l}F(\theta^{2s-1}) \end{aligned}$$

Et finalement

$$\begin{aligned} \left|L_{\chi_{2j-1}}(1)\right| &= \left|\frac{\tau(\chi_{2j-1})}{l} S_{2j-1}\right| \\ &= \frac{\pi\sqrt{l}}{l^2}\left|F(\theta^{2j-1})\right| \end{aligned}$$

□

5.5 Fonction ζ_K et nombre de classes de K

Théoreme 5.5.1.

$$h(K) = \frac{l^{m+1}}{2^{m-1}\pi^m \Re} \times \prod_{j=1}^{l-1} L_{\chi_1^j}(1)$$

Démonstration. Immédiat avec les lemmes précédents. □

Théoreme 5.5.2. *$h(K) = h_0 \times h_1$ avec :*

$$\begin{aligned} h_0 &= \frac{2^{m-1}}{\Re} \prod_{k=1}^{m-1} \left|\sum_{p=0}^{m-1} \theta^{2kr} \log|1-\xi^{q^p}|\right| \\ h_1 &= \frac{1}{(2l)^{m-1}} \prod_{k=1,m} \left|F(\theta^{2k-1})\right| \end{aligned}$$

Démonstration. On développe :

$$\begin{aligned}
h(K) &= \frac{l^{m+1}}{2^{m-1}\pi^m\mathfrak{R}} \times \prod_{j=1}^{l-1} L_{\chi_1^j}(1) \\
&= \frac{l^{m+1}}{2^{m-1}\pi^m\mathfrak{R}} \times \prod_{j=1}^{m} L_{\chi_1^{2j}}(1) \times \prod_{j=1}^{m} L_{\chi_1^{2j-1}}(1) \\
&= \frac{l^{m+1}}{2^{m-1}\pi^m\mathfrak{R}} \times \prod_{j=1}^{m} \left(\frac{2}{\sqrt{l}} \left| \sum_{p=0}^{l-2} \theta^{2jp} \log|1-\xi^{q^p}| \right| \right) \times \prod_{j=1}^{m} \left(\frac{\pi\sqrt{l}}{l^2} \left| F(\theta^{2j-1}) \right| \right) \\
&= \frac{2}{l^{m-1}\mathfrak{R}} \times \prod_{j=1}^{m} \left| \sum_{p=0}^{l-2} \theta^{2jp} \log|1-\xi^{q^p}| \right| \times \prod_{j=1}^{m} \left| F(\theta^{2j-1}) \right| \\
&= \frac{2^{m-1}}{\mathfrak{R}} \times \prod_{j=1}^{m} \left| \sum_{p=0}^{l-2} \theta^{2jp} \log|1-\xi^{q^p}| \right| \times \frac{1}{(2l)^{m-1}} \times \prod_{j=1}^{m} \left| F(\theta^{2j-1}) \right|
\end{aligned}$$

□

5.6 Appendice : un théorème de Dirichlet

Théoreme 5.6.1. *Soient*

1. *X un cone dans $\mathbb{R}^n$,*
2. *Une fonction f de $\mathbb{R}^n$, dans $\mathbb{R}$, telle que (a) $f(\alpha x) = \alpha^n f(x)$, et (b) l'ensemble $T = \{x \in \mathbb{R}^n \mid f(x) \leq 1\}$ est borné et de volume V non nul.*
3. *M un réseau de dimension n dont le parallélépipède fonda-*

mental est de volume W.

On pose

$$Z(s) = \sum_{x \in X \bigcap M} \frac{1}{f(x)^s}$$

Alors

$$\lim_{s \to 1+} (s-1)Z(s) = \frac{V}{W}$$

Démonstration. Soit $r > 0$. Soit M_r la contraction de M par un facteur r. Le parallélépipède fondamental de M_r est W/r^n. Soit $N_r = \#(M_r \bigcap T)$. On a :

$$\begin{aligned} V = \lim_{r \to \infty} N_r \frac{W}{r^n} &= W \lim_{r \to \infty} \frac{N_r}{r^n} \\ \lim_{r \to \infty} \frac{N_r}{r^n} &= \frac{V}{W} \end{aligned}$$

Soit T_r obtenu en dilatant l'ensemble T par facteur r. On a : $N(r) = \#(M \bigcap T_r)$. Et $M \bigcap T_r = \{x \in M \mid f(x) \leq r\}$. On ordonne les points $(M \bigcap T_r)$ selon la valeur de f :

$$0 < f(x_1) \leq f(x_2) \leq \cdots \leq f(x_{N(r)})$$

On pose $r_k = \sqrt[n]{f(x_k)}$. On a : $N(r_k) \geq k$. En effet les k premiers élements de la liste appartiennent à T_{r_k}. On a, pour tout ϵ, $N(r_k - \epsilon) < k$: il suffit de considérer le k-ième terme de la liste. Donc

$N(r_k - \epsilon) \leq k \leq N(r_k)$. On en déduit que

$$\frac{N(r_k - \epsilon)}{(r_k - \epsilon)^n} \left(\frac{r_k - \epsilon}{r_k} \right)^n \quad \leq \quad \frac{k}{r_k^n} \leq \frac{N(r_k)}{r_k^n}$$

Lorsque $k \to \infty$, $r_k \to \infty$

$$\lim_{k \to \infty} \frac{k}{f(x_k)} \quad = \quad \frac{V}{W}$$

Soit pour $\epsilon > 0$, il existe k_0 tel que pour $k > k_0$, on ait :

$$(\frac{V}{W} - \epsilon)\frac{1}{k} \quad \leq \quad \frac{1}{f(x_k)} \leq (\frac{V}{W} + \epsilon)\frac{1}{k}$$

En sommant et en élevant à la puissance s, on a :

$$(\frac{V}{W} - \epsilon)^s \sum_{k \geq k_0} \frac{1}{k^s} \quad \leq \quad \sum_{k \geq k_0} \frac{1}{(f(x_k))^s} \leq (\frac{V}{W} + \epsilon) \sum_{k \geq k_0} \frac{1}{k^s}$$

On multiplie par $s - 1$ et on fait tendre s vers 1. On utilise le fait que

$$1 = \lim_{s \to 1+} (s-1)\zeta(s) = \lim_{s \to 1+} (s-1) \sum_{k \geq k_0} \frac{1}{k^s}$$

On obtient :

$$\frac{V}{W} - \epsilon \quad \leq \quad \lim_{s \to 1+} (s-1) \sum_k \frac{1}{(f(x_k))^s} \leq \frac{V}{W} + \epsilon$$

□

5.7 Appendice : caractères modulo l

Definition 5.7.1. *Un **caractère modulo** l est un homomorphisme de groupe $\chi : (\mathbb{Z}/l\mathbb{Z})^* \to \mathbb{C}^*$. On a : $\chi(ab) = \chi(a)\chi(b)$. On le prolonge à $\mathbb{Z}$ tout entier en posant $\chi(n) = 0$ si $(n, l) = 1$ et $\chi(n) = \chi(n \pmod l)$ sinon.*

Notation 5.7.2. *Soit q une racine primitive modulo l. Soit θ une racine primitive $(l-1)$-ième de 1. On peut définir les caractères modulo l suivants :*

1. *χ_0 le caractère défini par $\chi_0(\xi^q) = 1$.*
2. *χ_1 est le caractère défini par $\chi_1(q^n) = \theta^n$.*
3. *Pour $0 \leq k \leq l-1$, χ_k le caractère défini par $\chi_k(q^n) = \theta^{kn}$; on a : $\chi_k = \chi_1^k$.*

Lemme 5.7.3. *Soit χ un caractère modulo l :*

$$\sum_{a \pmod l} \chi(a) = \begin{cases} l-1 \text{ si } \chi = \chi_0 \\ 0 \text{ sinon} \end{cases}$$

Démonstration. Il est évident que $\sum_a \chi_0(a) = l - 1$. Si $\chi \neq \chi$, il existe b tel que $\chi(b) \neq 1$. On écrit :

$$\sum_{a \bmod l} \chi(a) = \sum_{a \bmod l} \chi(ab) = \chi(b) \sum_{a \bmod l} \chi(a)$$

□

Lemme 5.7.4. *Les caractères modulo l sont de la forme χ_1^h, $h = 1, l-1$. Il y a $l-1$ caractères modulo l.*

Démonstration. Un caractère χ est défini par $\chi(q)$ qui doit être une racine $(l-1)$ de 1. Et les puissances θ^h constituent toutes les racines de l'unité. □

Definition 5.7.5. *Les caractères modulo l de la forme χ_1^{2j} sont dits **pairs**. Ceux de la forme χ_1^{2j-1} sont dits **impairs***

Lemme 5.7.6. *Il y a m caractères pairs et m caractères impairs.*

5.8 Appendice : sommes de Gauss

Definition 5.8.1. *Soit l un nombre premier, ξ un racine p-ième de 1, χ un caractère modulo l. Soit $F_l = \mathbb{Z}/l\mathbb{Z}$. La somme de Gauss associée à χ est donnée par :*

$$\tau(\chi) = \sum_{n=1}^{l-1} \chi(n)\xi^n$$

Lemme 5.8.2.

$$|\tau(\chi)| = \sqrt{l}$$

Démonstration. 1. On a : $\overline{\xi} = \xi^{l-1}$.

2. On a : $\chi(a^{-1}) = \overline{\chi(a)}$. En effet $\chi(a^{-1})\chi(a) = \chi(1) = 1$.

3. On développe :

$$\begin{aligned}
|\tau(\chi)|^2 &= \sum_{n=1}^{l-1} \chi(n)\xi^n \sum_{m=1}^{l-1} \overline{\chi(m)\xi^m} \\
&= \sum_{n=1}^{l-1} \chi(n)\xi^n \sum_{m=1}^{l-1} \chi(m^{-1})\xi^{(l-1)m} \\
&= \sum_{n=1}^{l-1}\sum_{m=1}^{l-1} \chi(nm^{-1})\xi^{n-m} \\
&= \sum_{n=1}^{l-1} \chi(1) + \sum_{n=1}^{l-1}\sum_{m\neq n, m=0}^{l-1} \chi(nm^{-1})\xi^{n-m}
\end{aligned}$$

4. On a :

$$\sum_{r=1}^{l-1} \xi^r = \xi \sum_{r=0}^{l-2} \xi^r = \xi \frac{1-\xi^{l-1}}{1-\xi} = \frac{\xi - \xi^l}{1-\xi} = \frac{\xi - 1}{1-\xi} = -1$$

5. On a, pour $\chi \neq \chi_0$:

$$\sum_{s=2}^{l-1} \chi(s) = \sum_{s=1}^{l-1} \chi(s) - \chi(1) = -\chi(1) = -1$$

6. On fait le changement de variables $(n, m) \to (r = n - m, s = nm^{-1})$. Les valeurs possibles, modulo l, pour r et s, sont $r \neq 0$

et $s \neq 1$. On a alors : $m = (s-1)^{-1}r$ et $n = s(s-1)^{-1}r$.

$$|\tau(\chi)|^2 = \sum_{n=1}^{l-1} \chi(1) + \sum_{r=1}^{l-1} \xi^r \sum_{s=2}^{l-1} \chi(s) = l - 1 + (-1)(-1) = l$$

□

5.9 Appendice : extensions cyclotomiques de degré quelconque

Faisons quelques rappels sur la fonction ϕ d'Euler.

Definition 5.9.1. *Fonction ϕ d'Euler : $\phi(m) = \#\{n \mid 1 \leq n < m, (n,m) = 1\}$*

Lemme 5.9.2. *On a :*

1. $\phi(p) = p - 1$
2. $\phi(p^r) = (p-1)p^{r-1}$
3. *Si* $(m,n) = 1$, $\phi(mn) = \phi(m)\phi(n)$
4. $\phi(p_1^{r_1} \dots p_i^{r_i}) = (p_1 - 1)p_1^{r_1 - 1} \dots (p_i - 1)p_i^{r_i - 1}$
5. *p divise m si et seulement si il divise $\phi(m)$*

Soit $m \in \mathbb{N}$, non nécessairement premier.

Definition 5.9.3. *Une racine primitive m-ième est un nombre algébrique ξ_m tel que $\xi_m^m = 1$ et $\xi_m^n \neq 1$ pour $n < m$.*

On considère l'extension $K = \mathbb{Q}(\xi_m)$.

Lemme 5.9.4. *Les racines primitives de* 1 *contenues dans K constituent groupe, noté μ_m. L'ensemble H des automorphismes de K définis par $\xi_m \to \xi_m^i$ pour $1 \leq i < m$, $(i, m) = 1$ forme un groupe. C'est l'ensemble des automorphismes de μ_m. Il est d'ordre $\phi(m)$.*

Démonstration. 1. Si $(i, m) = (j, m) = 1$, alors $(ij, m) = 1$

2. Si $(i, m) = 1$, il existe j tel que $(j, m) = 1$ et $ij \equiv 1 \pmod{m}$

□

Lemme 5.9.5. *Soit p qui ne divise pas m. Alors $X^m - 1$ ne peut pas avoir de racines doubles modulo p.*

Démonstration. On a déjà vu ce lemme pour m premier. La preuve est la même. On a : $(X^m - 1)' = mX^{m-1}$ et puisque $(m, p) = 1$, $m\overline{a} \neq 0$ pour tout $\overline{a} \neq 0$. □

Definition 5.9.6. *On considère le polynôme : $\Phi_m(X) = \prod_{i<m,(i,m)=1}(X - \xi_m^i)$. Il est bien entendu de degré $\phi(m)$.*

Théoreme 5.9.7. *Le groupe de Galois, $G = Gal(K : \mathbb{Q})$ est égal à H et le degré de l'extension est égal à $\phi(m)$.*

Démonstration. 1. G est contenu dans H. En effet, un élément du groupe de Galois est défini par sa valeur en ξ_m. Et l'image d'une racine primitive par élément du groupe de Galois est une racine primitive.

2. Φ_m est à coefficients entiers. En effet, il est invariant par les éléments de H donc par les éléments de G. Il est donc dans $K[X]$. Mais ses racines sont dans O_K. Il est donc dans $\mathbb{Z}[X]$

3. Φ_m est le polynôme minimal de ξ_m. La démonstration est la suivante. Soit $f \in \mathbb{Z}[X]$ le polynôme minimal de ξ_m. Il divise $X^m - 1$; on a $X^m - 1 = f(X)g(X)$ où $g \in \mathbb{Z}[X]$. Supposons que le degré de g soit supérieur à 1. Soit p un nombre premier ne divisant pas m. Comme $f(\xi_m^p) \neq 0$, et $(\xi_m^p)^m - 1 = 0$, on a $g(\xi_m^p) = 0$; par définition du polynôme minimal, on peut écrire $g(X^p) = f(X)h(X)$ avec $h \in \mathbb{Z}[X]$. Dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a : $\overline{g}(X^p) = (\overline{g}(X))^p = \overline{f}(X)\overline{h}(X)$. Donc $\overline{g}$ et $\overline{f}$ ont un facteur commun dans une extension de $\mathbb{Z}/p\mathbb{Z}$. Et $X^m - 1$ a une racine double dans cette extension. Mais ceci est impossible d'après le lemme précédent.
4. Donc $G = H$
5. Et $[K : \mathbb{Q}] = \phi(m)$

□

‘

Chapitre 6

Second résultat de Kummer sur le grand théorème de Fermat

6.1 Introduction

On considère les conditions suivantes :

— $\mathbf{A}(l)$: l est un nombre premier régulier

— $\mathbf{B}(l)$: toute unité de O_K qui est congrue à un nombre entier modulo l est une puissance l-ième.

— $\mathbf{C}(l)$: aucun des nombres de Bernoulli $B_2, B_4, \ldots, B_{l-3}$ n'est divisible par l.

Le but de ce chapitre final est de prouver que $\mathbf{A}(l)$ et que $\mathbf{C}(l)$ sont équivalents et $\mathbf{C}(l)$ implique $\mathbf{B}(l)$. Donc, avec les résultats du chapitre 3, que $\mathbf{C}(l)$ implique le théorème de Fermat pour l.

Nous utilisons la formulation du nombre de classes démontrée dans un chapitre précédent : $h_0 \times h_1$, h_0 et h_1 étant donnés par :

$$
\begin{aligned}
h_0 &= \frac{2^{m-1}}{\mathcal{R}} \prod_{k=1}^{m-1} \left| \sum_{p=0}^{m-1} \theta^{2kr} \log |1 - \xi^{q^p}| \right| \\
h_1 &= \frac{1}{(2l)^m} \prod_{k=1,m-1} \left| F(\theta^{2k-1}) \right|
\end{aligned}
$$

Rappelons que les termes apparaissant dans cette formule sont :

1. m est le nombre $(l-1)/2$;
2. $\mathcal{R}$ est le régulateur de l'extension $[K : \mathbb{Q}]$.
3. $q \in \mathbb{Z}$ est une racine primitive $l-1$-ième. On a $q^{l-1} \equiv 1 \pmod{l}$ et $q^j \not\equiv 1 \pmod{l}$ pour $1 \leq j \leq l$. Modulo l, les deux ensembles $0, 1, 2, \ldots, l-1$ et $1, q, q^2, q^3, \ldots, q^{l-2}$ sont les mêmes.
4. q_s est le plus petit résidu de q^s modulo m et F est le polynôme $F(X) = \sum_{k=0}^{l-2} q_s X^k$.
5. $\theta \in \mathbb{C}$ est une racine de 1 d'ordre $l-1$.

Nous devons donc étudier la divisibilité par l des deux nombres h_0 et h_1.

6.2 h_0 est entier

On a :

$$h_0 = \frac{2^{m-1}}{\mathcal{R}} \prod_{k=1}^{m-1} \left| \sum_{p=0}^{m-1} \theta^{2kr} \log |1 - \xi^{q^p}| \right|$$

La démonstration repose sur les propriétés des entiers du corps cyclotomique. On note $\mathfrak{U}$ le groupe des unités de K ; on sait que c'est le produit d'un groupe fini et d'un groupe libre de rang $m-1$; celui-ci est engendré par $m-1$ unités fondamentales ϵ_k, $k = 1, m-1$. On a distingué les $m-1$ unités cyclotomiques η_k, $k, 1, m-1$; on peut les écrire :

$$\eta_k = \xi^{m(1-k)}(-1)^{1-k} \frac{\xi^k - 1}{\xi - 1}$$

On peut les décomposer en fonction des unités fondamentales :

$$\eta_k = \pm \xi^g \prod_j \epsilon_j^{c_{kj}}$$

Notation 6.2.1. *On note :*

1. *C la matrice* (c_{kj})
2. $\mu_r = \log |1 - \xi^{q^r}|$ *; on a* $\mu_{m+r} = \mu_r$.

3. *Soit :*

$$S = \prod_{k=1}^{m-1} \left| \sum_{p=0}^{m-1} \theta^{2kr} \mu_r \right|$$

On a : $S = h_0 \mathcal{R} / 2^{m-1}$.

4. *Soit :*

$$\mathcal{A} = \begin{pmatrix} \mu_0 & \mu_1 & \dots & \mu_{m-1} \\ \mu_1 & \mu_2 & \dots & \mu_0 \\ \dots & \dots & \dots & \dots \\ \mu_{m-1} & \mu_0 & \dots & \mu_{m-2} \end{pmatrix}$$

Le terme général est $\mathcal{A}_{ij} = \mu_{(i+j-2) \mod m}$.

Lemme 6.2.2. *On a :*

$$S = \pm \det \mathcal{A} \, / \sum_{i=0}^{m-1} \mu_i$$

Démonstration. On applique 6.8.1 donné en appendice en prenant pour G le groupe engendré par θ^2, dont les caractères sont de la forme χ_k avec $\chi_k(\theta^{2r}) = \theta^{2kr}$ et en posant $f(\theta^{2r}) = \mu_r$. On a à la fois :

$$\prod_{k=0}^{m-1} \sum_{p=0}^{m-1} \chi_k(\theta^{2r}) \mu_i = \det \left(\chi_{i-j} \right)_{0 \le i,j \le m-1} = \det \left(\mu_{i+j} \right)_{0 \le i,j \le m-1}$$

Et

$$\prod_{k=0}^{m-1}\sum_{i=0}^{m-1}\chi_k(\theta^{2r})\mu_i \quad = \quad \sum_{i=0}^{m-1}\chi_0(\theta^{2r})\mu_i \times \prod_{k=1}^{m-1}\sum_{i=0}^{m-1}\chi_k(\theta^{2r}) = \sum_{i=0}^{m-1}\mu_i \times S$$

□

Notation 6.2.3. *$\mathcal{B}$ est la matrice de terme général $\mathcal{B}_{ij} = \mu_{i+1 \pmod m} - \mu_j$, pour $i = 1, m-1$, $j = 1, m-1$*

$$\mathcal{B} \quad = \quad \begin{pmatrix} \mu_2 - \mu_1 & \mu_3 - \mu_2 & \dots & \mu_0 - \mu_{m-1} \\ \dots & \dots & \dots & \dots \\ \mu_0 - \mu_1 & \mu_1 - \mu_2 & \dots & \mu_{n-2} - \mu_{m-1} \end{pmatrix}$$

Lemme 6.2.4. *On a :*

$$\det \mathcal{A} = \det \mathcal{B} \sum_{i=0}^{n-1} \mu_i$$

Démonstration.

$$\det \mathcal{A} \quad = \quad \begin{vmatrix} \mu_0 & \mu_1 & \dots & \mu_{m-1} \\ \mu_1 & \mu_2 & \dots & \mu_0 \\ \dots & \dots & \dots & \dots \\ \mu_{n-1} & \mu_0 & \dots & \mu_{n-2} \end{vmatrix}$$

$$\det \mathcal{A} = \begin{vmatrix} \mu_0 + \mu_1 + \cdots + \mu_{n-1} & \mu_1 & \dots & \mu_{n-1} \\ \mu_0 + \mu_1 + \cdots + \mu_{n-1} & \mu_2 & \dots & \mu_0 \\ \cdots & \cdots & \cdots & \cdots \\ \mu_0 + \mu_1 + \cdots + \mu_{m-1} & \mu_0 & \dots & \mu_{n-2} \end{vmatrix}$$

$$\det \mathcal{A} = \left(\sum_{i=0}^{n-1} \mu_i \right) \begin{vmatrix} 1 & \mu_1 & \mu_2 & \dots & \mu_{n-1} \\ 1 & \mu_2 & \mu_3 & \dots & \mu_0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \mu_0 & \mu_1 & \dots & \mu_{n-2} \end{vmatrix}$$

$$\begin{aligned} \det \mathcal{A} &= \left(\sum_{i=0}^{n-1} \mu_i \right) \begin{vmatrix} 1 & \mu_1 & \mu_2 & \dots & \mu_{n-1} \\ 0 & \mu_2 - \mu_1 & \mu_3 - \mu_2 & \dots & \mu_0 - \mu_{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \mu_0 - \mu_1 & \mu_1 - \mu_2 & \dots & \mu_{n-2} - \mu_{n-1} \end{vmatrix} \\ &= \left(\sum_{i=0}^{n-1} \mu_i \right) \times \det \mathcal{B} \end{aligned}$$

□

Lemme 6.2.5.

$$\frac{\xi^{kq^j} - 1}{\xi^{q^j} - 1} = (-1)^{1-k} \xi^{m(k-1)q^j} \sigma_j(\eta_k)$$

Démonstration. On a : $\sigma_j(\xi) = \xi^{q^j}, \sigma_j(\xi^k) = \xi^{kq^j}$;

$$\begin{aligned}
\sigma_j(\eta_k) &= \sigma_j\left(\xi^{m(1-k)}(-1)^{1-k}\frac{\xi^k-1}{\xi-1}\right) \\
&= (-1)^{1-k}\left(\sigma_j(\xi)^{m(1-k)}\frac{\sigma_j(\xi)^k-1}{\sigma_j(\xi)-1}\right) \\
&= (-1)^{1-k}\left(\xi^{m(1-k)q^j}\frac{\xi^{kq^j}-1}{\xi^{q^j}-1}\right)
\end{aligned}$$

Et :

$$\frac{\xi^{kq^j}-1}{\xi^{q^j}-1} = (-1)^{1-k}\xi^{m(k-1)q^j}\sigma_j(\eta_k)$$

□

Lemme 6.2.6. *On a :*

$$\mu_{k+j} - \mu_j = \log|\sigma_j(\eta_{q_j})|$$

Démonstration.

$$\begin{aligned}
\mu_{k+j} - \mu_j &= \log|1-\xi^{q^{k+j}}| - \log|1-\xi^{q^j}| \\
&= \log\left|\frac{1-\xi^{q^{k+j}}}{1-\xi^{q^j}}\right| \\
&= \log|(-1)^{1-k}\xi^{m(k-1)q^j}\sigma_j(\eta_k)| = \log|\sigma_j(\eta_k)|
\end{aligned}$$

□

Lemme 6.2.7. *On a :*

$$\det \mathcal{B} \quad = \quad \pm \det C \frac{\mathcal{R}}{2^{m-1}}$$

Démonstration. Rappelons la formule donnant le régulateur :

$$\mathcal{R} \quad = \quad 2^{m-1} \begin{vmatrix} \log|\sigma_1(\epsilon_1)| & \log|\sigma_1(\epsilon_2)| & \dots & \log|\sigma_1(\epsilon_{m-1})| \\ \log|\sigma_2(\epsilon_1)| & \log|\sigma_2(\epsilon_2)| & \dots & \log|\sigma_2(\epsilon_{m-1})| \\ \dots & \dots & \dots & \dots \\ \log|\sigma_{m-1}(\epsilon_1)| & \log|\sigma_{m-1}(\epsilon_2)| & \dots & \log|\sigma_{m-1}(\epsilon_{m-1})| \end{vmatrix}$$

1. D'après le lemme précédent :

$$\mu_{k+j} - \mu_j \quad = \quad \log|\sigma_j(\eta_{\overline{k}})|$$

2. Lorsque k prend les valeurs $1, 2, \dots, m-1$, $\overline{k}$ prend les valeurs $2, 3, \dots, m$.
3. Les matrices $\mathcal{M}$ et $\log|\sigma_j(\mu_i)|$, $2 \leq i \leq m$, $0 \leq j \leq m-2$ ne diffèrent que par l'ordre des lignes.
4. On a successivement :

$$\eta_k = \prod_{i=1}^{m-1} \epsilon_i^{c_{ki}} \qquad |\eta_k| = \prod_{i=1}^{m-1} |\epsilon_i|^{c_{ki}}$$

$$|\sigma_j(\eta_k)| = \prod_{i=1}^{m-1} |\sigma_j(\epsilon_i)|^{c_{ki}} \qquad \log|\sigma_j(\eta_k)| = \sum_{i=1}^{m-1} c_{ki} \log|\sigma_j(\epsilon_i)|$$

5. On prend les mineurs. Et on utilise la définition 4.1.7 du régulateur.

□

Théoreme 6.2.8. *h_0 est entier. En fait :$h_0 = \pm \det C$et C est à coefficients entiers.*

Démonstration.

$$\begin{aligned} h_0 &= \frac{2^{m-1}}{\mathcal{R}} \times S \text{ par définition de } S \\ &= \pm\frac{2^{m-1}}{\mathcal{R}} \times \frac{1}{\sum_{i=0}^{m-1} \mu_i} \times \det \mathcal{A} \text{ d'après 6.2.2} \\ &= \pm\frac{2^{m-1}}{\mathcal{R}} \times \mathcal{B} \text{ d'après 6.2.4} \\ &= \pm\frac{2^{m-1}}{\mathcal{R}} \times \det C \times \frac{\mathcal{R}}{2^{m-1}} \text{ d'après 6.2.7} \\ &= \pm \det C \end{aligned}$$

□

Lemme 6.2.9. *Les unités cyclotomiques engendrent sous groupe d'indice fini dans le groupe des unités de K.*

Démonstration. Le groupe des unités est le produit d'un groupe fini par un groupe de rang $m-1$. Les unités cyclotomiques engendrent un sous groupe de rang $m-1$. L'indice du premier dans le second est fini. □

Théoreme 6.2.10. *h_0 est égal à l'indice du sous groupe engendré par les unités cyclotomiques dans le groupe des unités de K. Par nature celui-ci est un nombre entier,*

Démonstration. D'après la définition des c_{ki} comme coefficients de $\eta_k = \prod_i \epsilon_i^{c_{ki}}$, l'indice du sous-groupe engendré par les unités cyclotomiques η_k vaut $\det C$. Et on vient de voir que $h_0 = \pm \det C$. □

6.3 h_1 est entier

On a :

$$h_1 = \frac{1}{(2l)^{m-1}} \prod_{k=1,m} \left|F(\theta^{2k-1})\right|$$

On écrit, pour deux nombres rationnels $r \equiv s \pmod{l}$ si $r - s = l(a/b)$ avec $(l, b) = 1$

Lemme 6.3.1. *Soit $P(X) \in \mathbb{Z}[X]$ tel que $P(\theta) \in \mathbb{Z}[\theta]$ est un entier ; alors : $P(\theta) \equiv P(q) \mod p$.*

Démonstration. $\mathbb{Q}(\theta)$ est une extension de dimension $\varphi(p-1)$. $\mathbb{Z}[\theta]$ en est l'anneau des entiers. On note : $\Phi_{p-1}(X) = \prod_{\substack{1 \le k \le p-1 \\ (k,p-1)=1}} (X - \theta^k)$. Les puissances q^k pour $\gcd(k, p-1) = 1$ parcourent toutes les racines primitives modulo p ; par conséquent : $\Phi_{p-1}(q) \equiv 0 \mod p$. On en déduit qu'il existe un morphisme : $\mathbb{Z}[X]/(\Phi_{p-1}(X)) \to \mathbb{F}_p, \quad X \mapsto q$ qui induit un morphisme : $\Phi : \mathbb{Z}[\theta] \to \mathbb{F}_p, \quad \theta \mapsto q$; on a :

$\Phi\left(\sum a_k\theta^k\right) = \sum a_k q^k \in \mathbb{F}_p$; si $P(X) = \sum a_k X^k \in \mathbb{Z}[X]$, alors : $P(\theta) = \sum a_k\theta^k \in \mathbb{Z}[\theta]$; et $F(P(\theta)) = \sum a_k q^k = F(q) \in \mathbb{F}_p$. Donc la réduction modulo p de $P(\theta)$ est égale à $P(q) \in \mathbb{F}_p$. □

6.3.1 Notation exponentielle

Notation 6.3.2. *Nous utilisons à partir de cette section, une* ***notation exponentielle*** *: soit σ un générateur du groupe de Galois de K sur Q ; à un polynôme $P(X) \in K[X]$, on associe un homomorphisme de corps $P^\sigma : K \to K$: si $P(X) = \sum_i a_i X^i \in K[X]$, P^σ est tel que $P^\sigma(\alpha) = \sum_i a_i\sigma^i(\alpha)$.*

Lemme 6.3.3. *On a : $P^\sigma Q^\sigma = Q^\sigma P^\sigma = (PQ)^\sigma$. On note Q_m le polynôme $Q_m(X) = X^m$. On a $Q_m^\sigma(\alpha) = \sigma^m(\alpha)$*

6.3.2 Les nombre b_k et le polynôme G

Lemme 6.3.4. *$q_j - qq_{j-1}$ est divisible par l.*

Démonstration. $q_j - qq_{j-1} \equiv q^j - qq^{j-1} \equiv 0 \pmod{l}$ □

Notation 6.3.5. *On pose : $b_k = (q_k - qq_{k-1})/l$ et $G(X) = \sum_{k=1}^{l-1} b_k X^k$*

Lemme 6.3.6. *Rappelons que $F(X) = \sum_{k=0}^{l-2} q_k X^k$. L'identité suivante est vérifiée : $(qX-1)F(X) = -lG(X) + X^{l-1} - 1$.*

Démonstration. On développe les deux membres de l'égalité à prou-

ver :

$$\begin{aligned} MG &= (qX-1)F(X) = (qX-1)\sum_{j=0}^{l-2} q_j X^j \\ &= \sum_{j=0}^{l-2} qq_j X^{j+1} - \sum_{j=0}^{l-2} q_j X^j = \sum_{j=1}^{l-1} qq_{j-1} X^j - \sum_{j=0}^{l-2} q_j X^j \\ &= \sum_{j=1}^{l-2} qq_{j-1} X^j + qq_{l-2} X^{l-1} - \sum_{j=1}^{l-2} q_j X^j - q_0 X^0 \\ &= \sum_{j=1}^{l-2} (qq_{j-1} - q_j) X^j + qq_{l-2} X^{l-1} - 1 \end{aligned}$$

Et

$$\begin{aligned} MD &= -lG(X) + X^{l-1} - 1 = \sum_{j=1}^{l-1} (qq_{j-1} - q_j) X^j + X^{l-1} - 1 \\ &= \sum_{j=1}^{l-2} (qq_{j-1} - q_j) X^j + (qq_{l-2} - q_{l-1}) X^{l-1} + X^{l-1} - 1 \end{aligned}$$

Et

$$MG - MD = -q_{l-1} X^{l-1} + X^{l-1} = 0 \; car \; q_{l-1} = 1$$

□

Lemme 6.3.7. *On a :*

$$\frac{l}{\xi - 1} = F^{\sigma}(\xi)$$

Démonstration. On a l'identité : $X^l - 1 = (X-1)(1 + X + X^2 + \cdots + X^{l-1})$. On prend la dérivée des deux termes, on fait $X = \xi$, on tient compte de ce que $\xi^{-l} = 1$, $1 + \xi + \cdots + \xi^{l-1} = 0$, et on obtient :

$$l\xi^{l-1} = (\xi - 1)(1 + 2\xi + \cdots + (l-1)\xi^{l-2})$$

Soit :

$$\begin{aligned} \frac{l}{\xi - 1} &= \xi^{1-l}\left(1 + 2\xi + + \cdots + (l-1)\xi^{l-2}\right) \\ &= \xi + 2\xi^2 + \cdots + (l-1)\xi^{l-1} \\ &= \xi + q_1\xi^q + q_2\xi^{q^2} + \cdots + q_{l-2}\xi^{q^{l-2}} = F^{\sigma}(\xi) \end{aligned}$$

□

Lemme 6.3.8. *On a :*

$$\frac{\xi}{1 - \xi} = -\frac{1}{l}Q_m^{\sigma}F^{\sigma}(\xi) = -\frac{1}{l}(Q_m F)^{\sigma}(\xi)$$

Démonstration. Puisque $\xi^{-1} = \sigma^m(\xi) = Q_m^{\sigma}(\xi)$, on a :

$$\frac{\xi}{\xi - 1} = \frac{1}{1 - \xi^{-1}} = \frac{1}{1 - \sigma^m(\xi)} = -\sigma^m(\frac{1}{\xi - 1}) = -\frac{1}{l}Q_m^{\sigma}F^{\sigma}(\xi)$$

□

6.3.3 Conclusion

Notation 6.3.9. *Soit* $b = \prod_{k=1,m} F(\theta^{2k-1})$.

Lemme 6.3.10. *b est entier.*

Démonstration. C'est un entier algébrique sur $\mathbb{Q}(\theta)$. Il est rationnel parce que $b = \pm(2l)^{l-1}h_1$, h et h_0 sont entiers, et $h_1 = h/h_0$. Un entier algébrique qui est rationnel est entier. □

Lemme 6.3.11. 2^{m-1} *divise b.*

Démonstration. 1. On a :

$$q_{m+s} + q_s \equiv q^{m+s} + q^s \equiv q^s(q^{\frac{l-1}{2}} + 1) \equiv 0 \pmod{l}$$

Donc $q_{s+m} + q_s = l$. Donc, l étant impair, q_{s+m} et q_s sont de parités différentes.

2. Puisque $\theta^m = -1$, on a, pour $k = 1, 3, \ldots, l-2$:

$$\begin{aligned} F(\theta^k) &\equiv \sum_{s=0}^{m-1} \left(q_s\theta^{ks} + q_{m+s}\theta^{k(ms+s)} \right) \pmod 2 \\ &\equiv \sum_{s=0}^{m-1} (q_s - q_{m+s})\,\theta^{ks} \equiv \sum_{s=0}^{m-1} \theta^{ks} \pmod 2 \end{aligned}$$

Donc :

$$F(\theta^k)(1-\theta^k) \equiv 0 \pmod 2$$

3. Et le produit $b(1-\theta)(1-\theta^3)\dots(1-\theta^{l-2})$ est divisible par 2^m.
4. Mais θ est une racine primitive de 1 d'ordre $l-1$; on écrit :

   $$X^{l-2}+X^{l-1}+\cdots+X+1=(X^{l-1}-1)/(X-1)=(X-\theta)\dots(X-\theta^{l-2})$$

   on fait $X=1$, on a :

   $$\prod_{k=1}^{l-2}(1-\theta^k)=l-1$$

5. De la même façon, θ^2 est une racine d'ordre $m=(l-1)/2$; et :

   $$\prod_{k=1}^{m-1}(1-\theta^{2k})=\frac{l-1}{2}$$

6. Donc $(1-\theta)(1-\theta^3)\dots(1-\theta^{l-2})=2$ et b est divisible par 2^{m-1}.

□

Lemme 6.3.12.

$$\prod_{j=1}^{m}(q\theta^{2j-1}-1)b=(-l)^{m-1}\prod_{j=1}^{m}G(\theta^{2j-1})$$

Démonstration. D'après 6.3.6, $(qX-1)F(X)=-lG(X)+X^{l-1}-1$.

On multiplie les égalités obtenues en faisant $X = \theta^{2j-1}$, $j = 1, m$:

$$\begin{aligned}\prod_{j=1,m}(q\theta^{2j-1}-1)F(\theta^{2j-1}) &= \prod_{j=1,m}\left(-lG(\theta^{2j-1})+(\theta^{2j-1})^{l-1}-1\right)\\ b\prod_{j=1,m}(q\theta^{2j-1}) &= (-l)^m\prod_{j=1,m-1}G(\theta^{2j-1})\ car\ \theta^{l-1}=1\end{aligned}$$

□

Lemme 6.3.13. *On peut choisir q en sorte que* $q^m+1 \not\equiv -1 \pmod{l^2}$

Démonstration. Soit q une racine primitive modulo l ; si on a $q^m + 1 \equiv 0 \pmod{l}^2$, on considère $q + l$; on a :

$$\begin{aligned}(q+l)^m+1 &\equiv q^m+mq^{m-1}l+1 \pmod{l^2}\\ &\equiv -1+mq^{m-1}l+1 \pmod{l^2}\\ &\equiv mq^{m-1}l \pmod{l^2}\\ &\not\equiv 0 \pmod{l^2}\end{aligned}$$

□

Lemme 6.3.14. $\prod_{j=1}^{m}(q\theta^{2j-1}-1)$ *est un entier qui n'est pas divisible par* l^2.

Démonstration. On a : $\prod_{j=1}^{m-1}(X-\theta^{2j-1}) = X^m - 1$. En effet les deux

polynômes ont les mêmes racines. On en déduit successivement que :

$$\begin{aligned}\prod_{j=1}^{m}(X-\theta^{2j-1}Y) &= X^m - Y^m \\ \prod_{j=1}^{m}(q\theta^{2j-1}-1) &= 1+q^m\end{aligned}$$

Mais on a choisi q en sorte que $q^m + 1 \not\equiv -1 \pmod{l}^2$ □

Lemme 6.3.15. *l^{m-1} divise $b = \prod_{j=1}^{m} F(\theta^{2j-1})$*

Démonstration. Conséquence de 6.3.12 et de 6.3.14. □

Lemme 6.3.16. *h_1 est entier.*

Démonstration. Conséquence de la définition de h_1, 6.3.11 et 6.3.15. □

6.4 Condition de divisibilité de h_1 par l

Lemme 6.4.1. *l divise h_1 si et seulement s'il divise $\prod_{j=1}^{m} G(\theta^{2j-1})$*

Démonstration. Conséquence de 6.3.12 et 6.3.15. □

Lemme 6.4.2. *On a :*

$$G(\theta)G(\theta^3)\dots G(\theta^{l-2}) \equiv G(q)G(q^3)\dots G(q^{l-2}) \pmod{l}$$

Démonstration. On applique 6.3.1 : si $P(X) \in \mathbb{Z}[X]$ est tel que $P(\theta) \in \mathbb{Z}[\theta]$ est entier ; alors, $P(\theta) \equiv P(q) \mod p$.

□

6.4.1 Lien avec les nombres de Bernoulli

Soit $B_n(t)$ le n-ième polynôme de Bernoulli défini dans l'appendice 6.9.

Notation 6.4.3. *Soit $k \in [0, l-1]$. Soit t_k le plus petit entier plus grand que kl/q.*

Lemme 6.4.4. *Alors $j-1 \in [t_k, t_k+1[$ équivaut à $b_j = k$.*

Démonstration. On a : $lb_j = q_j - qq_{j-1} \in]-l, ql[$. Donc $b_j \in]-1, q[$. En fait $b_j \in [0, q-1]$. Alors $b_j = k \Leftrightarrow qq_{j-1} = lk + q_j \in [kl, (k+1)l]$ $\Leftrightarrow q_{j-1} \in [kl/q, (k+1)l/q] \Leftrightarrow j-1 \in [t_k, t_k+1]$. □

Lemme 6.4.5. *Pour chaque entier $k = 1, l-1$, il existe un et seul entier $j = 1, l-1$ tel que $t_k \equiv j/l \pmod{l}$*

Démonstration. Soit $r \in]0, l[$. Il existe un unique $t \in]0, l[$ tel que $tq \equiv r \pmod{l}$. Alors $tq - r$ peut s'écrire kl pour un entier $k \in]0, q[$ (parce que $tq - r > 0$ et $tq - r < tq < lq$). Alors t qui s'écrit $(kl + r)/q$ est le plus petit entier plus grand que kl/q. □

Lemme 6.4.6. *Soit j défini à partir de k comme dans le lemme précédent. Alors $B_{n+1}(t_k) \equiv B_{n+1}(\frac{j}{q}) \pmod{l}$*

Démonstration. En effet, l/q divise $t_k - k/q$ et l n'apparaît pas dans les dénominateurs du polynôme de Bernoulli B_{n+1}. □

Lemme 6.4.7. *Lorsque $n \neq l-2$:*

$$\sum_{k=0}^{q} (B_{n+1}(l) - B_{n+1}(t_k)) \equiv \sum_{j=1}^{q-1} \left(B_{n+1}(l) - B_{n+1}(\frac{j}{q}) \right) \pmod{l}$$

Démonstration. Conséquence de 6.4.5 et 6.4.6. □

Lemme 6.4.8. *Lorsque $n \neq l-2$:*

$$G(q^n) \equiv \frac{1}{n+1} \sum_{k=0}^{q} (B_{n+1}(l) - B_{n+1}(t_k)) \pmod{l}$$

Démonstration.

$$\begin{aligned} G(q^n) &= \sum_{i=1}^{l-1} b_i q^{ni} \equiv \sum_{i=1}^{l-1} b_i q_i^n \pmod{l} \\ &\equiv q_n \sum_{i=1}^{l-1} b_{i-1} q_i^n \pmod{l} \end{aligned}$$

Comme les q_i parcourent l'ensemble $0, 1, \ldots, l-1$, on a :

$$\begin{aligned}\sum_{i=1}^{l-1} b_{i-1} q_i^n &= \sum_{k=0}^{l-1} \sum_{t_k \leq i < t_{k+1}} b_{i-1} q_i^n = \sum_{k=0}^{q} \sum_{t_k \leq i < t_{k+1}} k\, i^k \\ &= \sum_{k=0}^{q} \sum_{t_k \leq i < l} i^k = \frac{1}{n+1} \sum_{k=0}^{q} (B_{n+1}(l) - B_{n+1}(t_k))\end{aligned}$$

Et, en utilisant 6.4.7 :

$$G(q^n) \equiv \frac{1}{n+1} \sum_{k=0}^{q} (B_{n+1}(l) - B_{n+1}(t_k)) \pmod{l}$$

□

Lemme 6.4.9. *Lorsque $n \neq l-2$:*

$$G(q^n) \equiv \frac{1}{n+1} \left(q^{n+1} - 1\right) B_{n+1} \pmod{l}$$

Démonstration. Il est montré, en 6.9.17, dans l'appendice sur les nombre de Bernoulli, que :

$$B_{n+1} + \sum_{k=1}^{q-1} B_{n+1}(\frac{k}{q}) = q^{-n} B_{n+1}$$

On développe :

$$\begin{aligned} G(q^n) &\equiv \tfrac{q_n}{n+1}\left((q-1)B_{n+1} - \textstyle\sum_{k=1}^{q-1} B_{n+1}(\tfrac{k}{q})\right) \pmod{l} \\ &\equiv \tfrac{q_n}{n+1}\left(qB_{n+1} - q^{-n}B_{n+1}\right) \pmod{l} \\ &\equiv \tfrac{1}{n+1}\left(q^{n+1}-1\right)B_{n+1} \pmod{l} \end{aligned}$$

□

Lemme 6.4.10. $G(q^{l-2}) \not\equiv 0 \pmod{l}$

Démonstration. On a $q^{l-1} \equiv 1 \pmod{l}$. Soit ν tel que $q^{l-1} - 1 = l\nu$. Avec $b_k = (q_k - qq_{k-1})/l$. On écrit $k(l-2) = k(l-1) - k$. Alors $q^{(l-2)k} \equiv q^{l-1-k} \pmod{l}$. On développe

$$G(q^{l-2}) = \sum_{k=1}^{l-1} b_k q^{(l-2)k} \equiv \sum_{k=1}^{l-1} b_k q^{l-1-k} \pmod{l}$$

On a : $G(q^{l-2}) \equiv \nu \pmod{l}$ où ν est défini par : . On a donc $\nu \equiv 0 \pmod{l}$. Donc $G(q^{l-2}) + q^{l-2}F(q^{l-2}) \equiv q^{l-2}F(q^{l-2}) \equiv q^{-1}(-1) \not\equiv 0 \pmod{l}$. □

Lemme 6.4.11. *l divise $G(q^n)$ si et seulement si l divise le numérateur de de B_{n+1}*

Démonstration. On a $q^{l-1} \equiv 1 \pmod{l}$ et $q^n \not\equiv 1 \pmod{l}$ pour $n < l-1$. Alors

1. D'après 6.4.9 et 6.4.10, l divise $G(q^n)$ si et seulement si $n \neq l-2$ et l divise $(q^{n+1}-1)B_{n+1}/(n+1)$

2. Et est donc équivalent à : l divise le numérateur de B_{n+1} puisque, d'après remarque ci-dessus, l ne divise pas $q^{n+1}-1) = 1$ pour $n < l-2$.

□

Théoreme 6.4.12. *Les propositions suivantes sont équivalentes :*

1. *l divise h_1*
2. *il existe $k \in [3, 5, \ldots, l-2]$ tel que l divise le numérateur de de B_k*

Démonstration.

1. D'après 6.4.1, l divise h_1 si et seulement s'il divise $\prod_{j=1}^{m} G(\theta^{2j-1})$
2. Donc si et seulement si il existe $k \in [1, m]$ tel que l divise $G(q^n)$
3. Donc, d'après 6.4.11, si et seulement il existe $k \in [3, 5, \ldots, l-2]$ tel que l divise le numérateur de de B_k

□

6.5 Si l divise h_0, alors l divise h_1

6.5.1 Unités cyclotomiques et congruences

Dans cette partie, l est un nombre premier régulier ; F, G, Q_m sont les polynômes définis plus haut. On considère une unité cyclotomique de la forme $\mu = \xi^g \prod_{k=1}^{m} \left(1-\xi^{p^k}\right)^{n_k}$ avec $\sum_{k=1}^{m} n_k = 0$; μ

est supposée congrue modulo l à un entier c. Le but de cette section est de monter que μ est une puissance l-ième.

Notation 6.5.1. *On considère les polynômes suivants dans $\mathbb{Z}[X]$:*

1. $R(X) = \sum_{k=1}^{m} n_k q^k X^k$.
2. $S(X) = X^g \prod_{k=1}^{m} \left(1 - X^{p^k}\right)^{n_k}$ *en sorte que :* $S(\xi) = \mu$.
3. $T(X) = \sum_{k=1}^{l-1} X^k$. *On a* $T(\xi) = 0$.

Lemme 6.5.2. *On peut écrire $S(X)$ sous la forme :*

$$S(X) \quad = \quad c + lU(X) + T(X)V(X)$$

Où U, V sont deux polynômes à coefficients entiers.

Démonstration. Soit $V(X)$ le quotient de la division euclidienne de $S(X) - c$ par $T(X)$. Le reste est $S(X) - c - T(X)V(X)$. Soit $U(X)$ le quotient de ce reste par l et $r < l$ le reste de cette division. On a : $S(X) - c - T(X)V(X) = r + lF(X)$. On fait $X = \xi$. On a : $\mu - c = r + lF(\xi)$. Comme $\mu \equiv c \pmod{l}$, on a : $r = 0$. Et le lemme est prouvé. □

Lemme 6.5.3. *On a :*

$$c - \sum_{k=1}^{m} n_k \frac{q^k \xi^{q^k}}{1 - \xi^{q^k}} \quad \equiv \quad \frac{\left(\sum_{k=1}^{l-1} k\xi^k\right) V(\xi)}{\mu} \pmod{l}$$

Démonstration. On prend la dérivée logarithmique de 6.5.2 :

$$\begin{aligned}\frac{S'(X)}{S(X)} &= \frac{c}{X} - \sum_{k=1}^{m} n_k \frac{q^k X^{q^k-1}}{1-X^{q^k}} \\ &= \frac{lU'(X) + \left(\sum_{k=0}^{l-1} X^k\right) V'(X) + \left(\sum_{k=1}^{l-1} kX^{k-1}\right) V(X)}{c + lU(X) + \sum_{k=0}^{l-1} X^k V(X)}\end{aligned}$$

On fait $X = \xi$:

$$\begin{aligned}&\frac{c}{\xi} - \sum_{k=1}^{m} n_k \frac{q^k \xi^{q^k-1}}{1-\xi^{q^k}} \\ = &\frac{lU'(\xi) + \left(\sum_{k=0}^{l-1} \xi^k\right) V'(\xi) + \left(\sum_{k=1}^{l-1} k\xi^{k-1}\right) V(\xi)}{c + lU(\xi) + \sum_{k=0}^{l-1} \xi^k V(\xi)}\end{aligned}$$

Soit :

$$\begin{aligned}\frac{c}{\xi} - \sum_{k=1}^{m} n_k \frac{q^k \xi^{q^k-1}}{1-\xi^{q^k}} &\equiv \frac{\left(\sum_{k=1}^{l-1} k\xi^{k-1}\right) V(\xi)}{\mu} \pmod{l} \\ c - \sum_{k=1}^{m} n_k \frac{q^k \xi^{q^k}}{1-\xi^{q^k}} &\equiv \frac{\left(\sum_{k=1}^{l-1} k\xi^{k}\right) V(\xi)}{\mu} \pmod{l}\end{aligned}$$

□

Lemme 6.5.4. *Le membre de gauche de 6.5.3 peut s'écrire :*

$$c + \frac{1}{l} R^{\sigma} Q_m^{\sigma} F^{\sigma}(\xi) = c + \frac{1}{l} (R Q_m F)^{\sigma}(\xi)$$

Démonstration.

$$\begin{aligned} c - \sum_{k=1}^{m} n_k \frac{q^k \xi^{q^k}}{1 - \xi^{q^k}} &= c - \sum_{k=1}^{m} n_k \frac{q^k \sigma^k(\xi)}{1 - \sigma^k(\xi)} \\ &= c - R^{\sigma}\left(\frac{\xi}{1-\xi}\right) \\ &= c + \frac{1}{l} R^{\sigma} Q_m^{\sigma} F^{\sigma}(\xi) \text{ d'après 6.3.8} \end{aligned}$$

□

Lemme 6.5.5. *Le membre de droite de 6.5.3 est congru modulo l, à un nombre de la forme $aF^{\sigma}(\xi)$, a étant entier.*

Démonstration. On peut écrire l'entier algébrique $V(\xi)/\mu$ sous la forme $a + Q(\xi)(1-\xi)$ où Q est un polynôme à coefficients entiers et a est entier. On a :

$$\begin{aligned} \frac{1}{\mu} \frac{l}{\xi - 1} V(\xi) &= \frac{l}{\xi - 1} (a + Q(\xi)(1 - \xi)) \\ &= a \frac{l}{\xi - 1} - l Q(\xi) \\ &\equiv a \frac{l}{\xi - 1} \pmod{l} \\ &\equiv a F^{\sigma}(\xi) \pmod{l} \text{ en utilisant 6.3.7.} \end{aligned}$$

□

Lemme 6.5.6.

$$c + \frac{1}{l} R^\sigma Q_m^\sigma F^\sigma(\xi) = c + \frac{1}{l}(RQ_mF)^\sigma(\xi) \quad \equiv \quad aF^\sigma(\xi) \pmod{l}$$

Démonstration. Conséquence de 6.5.4 et 6.5.5. □

Lemme 6.5.7. *$R^\sigma G^\sigma(\xi) = (RG)^\sigma(\xi)$ est un entier n modulo l.*

Démonstration. On applique $q\sigma - 1$ aux deux membres de 6.5.6 ; d'un côté :

$$(q\sigma - 1)(c + \frac{1}{l} R^\sigma Q_m^\sigma F^\sigma(\xi) \quad \equiv \quad qg - c + \frac{1}{l} R^\sigma Q_m^\sigma (q\sigma - 1)F^\sigma(\xi)$$

On a vu en 6.3.6 que : $(qX - 1)F(X) = lG(X) + X^{l-1} - 1$. En faisant $X = \sigma$, on obtient : $(q\sigma - 1)F(\sigma) = lG(\sigma) + \sigma^{l-1} - 1$. Soit, en notation exponentielle : $(q\sigma - 1)F^\sigma = lG^\sigma - 1$.

$$\begin{aligned}(q\sigma - 1)(c + \frac{1}{l} R^\sigma Q_m^\sigma F^\sigma(\xi) \quad &\equiv \quad qg - c + \frac{1}{l} R^\sigma Q_m^\sigma \left((\sigma^{l-1} - 1) + lG^\sigma\right)(\xi) \\ &\equiv \quad qg - c + R^\sigma Q_m^\sigma G^\sigma(\xi)\end{aligned}$$

De l'autre :

$$\begin{aligned}(q\sigma - 1)(aF^\sigma(\xi) \quad &\equiv \quad a\left((\sigma^{l-1} - 1) + lG^\sigma\right) \pmod{l} \\ &\equiv \quad 0 \pmod{l}\end{aligned}$$

Donc

$$qg - c + R^\sigma Q_m^\sigma G^\sigma(\xi) \equiv 0 \pmod{l}$$

On en déduit que $R^\sigma G^\sigma(\xi) \equiv (c - qg) \pmod{l}$. On pose $n = c - qg$ et on conclut. □

Lemme 6.5.8. *$(RG)^\sigma(\sigma^j\xi) = R^\sigma G^\sigma(\sigma^j\xi) \equiv n \pmod{l}$ où n est le même que dans le lemme précédent.*

Démonstration. On sait que $(\sigma - 1)F^\sigma = 0$, donc : $(\sigma^j - 1)F^\sigma = (\sigma - 1)(1 + \sigma + \cdots + \sigma^{j-1})F^\sigma = 0$; on développe :

$$\begin{aligned} R^\sigma G^\sigma(\sigma^j\xi) - R^\sigma G^\sigma(\xi) &= R^\sigma\left((\sigma^j - 1)F^\sigma\right)(\xi) \\ &\equiv R^\sigma(0)(\xi) \pmod{l} \end{aligned}$$

□

6.5.2 La base κ_j

Notation 6.5.9. *On note : $\kappa_j = \sum_{k=0}^{l-1} k^j \xi^k$*

Lemme 6.5.10.

$$\kappa_j = \sum_{i=1}^{l-1} q^{ij}\sigma^i(\xi)$$

On a :

$$\kappa_j = \sum_{k=0}^{l-1} k^j \xi^k = \sum_{k=1}^{l-1} k^j \xi^k = \sum_{i=1}^{l-1} (q^i)^j \xi^{q^i} = \sum_{i=1}^{l-1} q^{ij} \sigma^i(\xi)$$

Démonstration. □

Lemme 6.5.11. *Modulo l, les entiers cyclotomiques s'écrivent de façon unique comme des combinaisons linéaires à coefficients entiers des nombres κ_j.*

Démonstration. Dans la base naturelle : $1, \xi, \xi^2, \xi^{l-1}$, la matrice qui exprime les κ_j est une matrice de Vandermonde :

$$\begin{pmatrix} 1^1 & 2^1 & 3^1 & \dots & (l-1)^1 \\ 1^2 & 2^2 & 3^2 & \dots & (l-1)^2 \\ \dots & \dots & \dots & \dots & \dots \\ 1^{l-1} & 2^{l-1} & 3^{l-1} & \dots & (l-1)^{l-1} \end{pmatrix}$$

Elle est inversible modulo l : son déterminant $\prod_{1 \le i < j \le l-1} (i-j)$ est le produit de termes qui sont tous non nuls modulo l. □

Lemme 6.5.12. *On a : $\sigma(\kappa_j) \equiv q^{-j} \kappa_j \pmod{l}$*

Démonstration.

$$\begin{aligned} \sigma(\kappa_j) &= \sigma\left(\xi + q^j \sigma^j(\xi) + q^{2j} \sigma^{2j}(\xi) + \dots + q^{(l-1)j} \sigma^{(l-1)j}(\xi)\right) \\ &= \sigma(\xi) + q^j \sigma^{j+1}(\xi) + q^{2j} \sigma^{2j+1}(\xi) + \dots + q^{(l-1)j} \sigma^{(l-1)j+1}(\xi) \\ &\equiv q^{-j} \kappa_j \pmod{l} \end{aligned}$$

□

Lemme 6.5.13. $(RG)^\sigma(\kappa_j) = R^\sigma G^\sigma(\kappa_j) \equiv R(q^{-j})G(q^{-j})\kappa_j \pmod{l}$

Démonstration. On développe. □

Lemme 6.5.14. $(RG)^\sigma(\kappa_j) = R^\sigma G^\sigma(\kappa_j) \equiv 0 \pmod{l}$

Démonstration.

$$\begin{aligned} R^\sigma G^\sigma(\kappa_j) &= R^\sigma G^\sigma\left(\xi + q^j\sigma^j(\xi) + \cdots + q^{(l-1)j}\sigma^{(l-1)j}(\xi)\right) \\ &= R^\sigma G^\sigma(\xi) + q^j R^\sigma G^\sigma(\sigma^j(\xi)) + \cdots + (q^{(l-1)j} R^\sigma G^\sigma \sigma^{(l-1)j}(\xi)) \\ &\equiv n + q^j n \cdots + (q^{(l-1)j} n \pmod{l} \text{ en utilisant 6.5.8.} \\ &\equiv n(1 + q^j \cdots + (q^{(l-1)j}) \pmod{l} \equiv 0 \pmod{l} \end{aligned}$$

□

Lemme 6.5.15. $R(q^{-j})G(q^{-j}) \equiv 0 \pmod{l}$

Démonstration. Conséquence de 6.5.13 et 6.5.14 □

6.5.3 Conclusion

Théoreme 6.5.16. *Soit* $\mu = \xi^g \prod_{k=1}^m \left(1 - \xi^{p^k}\right)^{n_k}$, *avec* $\sum_{k=1}^m n_k = 0$ *une unité cyclotomique. Si* μ *est congrue à un entier modulo* l *et si* l *est régulier, alors les nombres* n_k *sont divisibles par* l *et* μ *est une puissance* l*-ième.*

Démonstration. On a vu que l divise le numérateur de B_{n+1} si et seulement si il divise $G(q^n)$. Donc si l ne divise pas les numérateurs des B_{n+1}, $G(q^n)$ est différent de 0 modulo l. Les $R(q^{-j})$ sont nuls modulo l.

$$\sum_{k=1}^{m} n_k q^k q^{-jk} \equiv 0 \pmod{l}$$

En utilisant 6.5.11, on conclut que les nombres n_k sont nuls modulo l. □

Lemme 6.5.17. *Si l divise h_0, il existe une unité $\mu \notin C$ telle que $\mu^l \in C$, i.e. des entiers g et n_k, $k = 1, m$ tels que $\sum_k n_k = 0$ et :*

$$\mu^l = \pm\xi^g \sum_{k=1}^{m} \left(1 - \xi^{p^k}\right)^{n_k}$$

Démonstration. Si l divise h_0, le groupe quotient $\mathcal{U}/C$ contient un élément d'ordre l, ou ce qui est équivalent : il existe une unité $\mu \notin C$ telle que $\mu^l \in C$. □

Lemme 6.5.18. *Il existe c tel que $\mu^l \equiv c \pmod{l}$.*

Démonstration. C'est vrai pour tout entier algébrique de K :

$$\left(\sum a_i \xi^i\right)^l \equiv \sum a_i^l \pmod{l}$$

□

Théoreme 6.5.19. *Si l divise h_0, il divise h_1*

Démonstration. On suppose que l divise h_0 et ne divise pas h_1

1. Puisque l divise h_0, il existe une unité μ qui n'est pas cyclotomique mais telle que μ^l l'est. On écrit $\mu^l = \xi^g \prod_{k=1}^{m}(1-\xi^{q^k})^{n_k}$.
2. D'après 6.5.18, μ^l est congrue à un entier modulo l.
3. D'après 6.5.16, tous les n_k sont divisibles par l : $n_k = lm_k$.
4. Mais on a : $\xi^g = \mu^l \prod_{k=1}^{m}(1-\xi^{q^k})^{-lm_k}$; c'est donc une puissance l-ième : $\xi^g = \beta^l$. β est une unité ; d'après 4.1.5, elle se met sous la forme $r\xi^i$ où $r \in \mathbb{R}$, on a donc $r^i\xi^{il} = \xi^g$; on en déduit que $r = \pm 1$ et $g \equiv il \pmod{l}$.
5. $\mu^l = \pm\xi^{il} \prod_{k=1}^{m}(1-\xi^{q^k})^{ln_k} = \pm\left(\xi^l \prod_{k=1}^{m}(1-\xi^{q^k})^{n_k}\right)^l$.
6. Donc $\mu = \pm\xi^l \prod_{k=1}^{m}(1-\xi^{q^k})^{n_k}$ et est une unité cyclotomique. Ce qui est en contradiction avec sa définition.
7. Donc l divise h_1.

□

6.6 Lemme de Kummer

Il s'agit ici de la démonstration que $\mathbf{C}(l) \Rightarrow \mathbf{B}(l)$. On a vu en 6.5.18 que si l est régulier et si μ est une unité cyclotomique congrue modulo l à un entier, alors μ est une puissance l-ième. Il faut montrer ce résultat pour toute unité.

Lemme 6.6.1. *Si ξ^k est congru à une unité modulo l, alors $k \equiv 0 \pmod{l}$*

Démonstration. Si $\xi^k \equiv n \pmod{l}$ avec $n \not\equiv 0 \pmod{l}$; dans $(\mathbb{Z}/l\mathbb{Z})[\xi]$, on a : $\overline{\xi^k} = \overline{n}$. Soit σ un élément du groupe de Galois de $(\mathbb{Z}/l\mathbb{Z})[\xi]$ sur $\mathbb{Z}/l\mathbb{Z}$; on a : $\sigma(\overline{\xi^k}) = \sigma(\overline{n}) = \overline{n} = \overline{\xi^k}$; ceci n'est possible que si $\overline{\xi^k} \in \mathbb{Z}/l\mathbb{Z}$; donc si $k \equiv 0 \pmod{l}$ et alors $\xi^k \equiv 1 \pmod{l}$.

□

Théoreme 6.6.2. *Si l est régulier, alors, si ν est une unité congrue à un entier modulo l, c'est une puissance l-ième.*

Démonstration.

1. ν^{h_0} est une unité cyclotomique. On a :

$$\nu^{h_0} \equiv \pm\xi^j \prod_{k=1,m} (1-\sigma^k(\xi))^{n_k}$$

2. D'après 6.5.16, tous les n_k sont divisibles par l : $n_k = lm_k$.
3. l est régulier, h_0 n'est pas divisible par l, et il existe a et b tels que $ah_0 + bl = 1$. Alors :

$$\nu = \nu^{ah_0+bl} = (\nu^{h_0})^a \nu^{bl} = \pm\xi^{aj} \prod_{k=1,m} (1-\sigma^k(\xi))^{alm_k} \nu^{bl}$$
$$\xi^{aj} = \pm \prod_{k=1,m} (1-\sigma^k(\xi))^{alm_k} \nu^{bl-1}$$

4. $\prod_{k=1,m}(1-\sigma^k(\xi))^{alm_k}$ est une unité de K qui est congrue à un entier modulo l parce que c'est la puissance l-ième d'un

entier cyclotomique.

5. ν^{bl-1} est congru à un entier modulo l parce que ν l'est. On en déduit que ξ^{aj} est congru à une unité modulo l, donc, en utilisant 6.6.1 que $aj \equiv 0 \pmod{l}$, et que $\xi^{aj} = 1$.
6. Donc

$$\begin{aligned} \nu &= (\nu^{h_0})^a \mu^{bl} \\ &= \left(\prod_{k=1,m} (1 - \sigma^k(\xi))^{am_k} \nu^b \right)^l \end{aligned}$$

ν est une puissance l-ième.

□

6.7 Le second théorème de Kummer

Lemme 6.7.1. *On a : $\boldsymbol{A}(l) \Leftrightarrow \boldsymbol{C}(l)$: l divise h, si et seulement si il divise le numérateur d'un des B_i, $i \leq l-2$.*

Démonstration.

1. $A \Rightarrow C$: Si l est régulier, il ne divise pas h, il ne divise pas h_1, aucun des numérateurs des nombres de Bernoulli $B_2, B_4, \ldots, B_{l-3}$ n'est divisible par l
2. $C \Rightarrow A$: si aucun des numérateurs des nombres de Bernoulli $B_2, B_4, \ldots, B_{l-3}$ n'est divisible par l, l ne divise pas h_1, il ne divise pas h_0 d'après 6.5.19, il ne divise donc pas h, et il est régulier.

□

Théoreme 6.7.2. *Si l ne divise pas le numérateur des nombres de Bernoulli B_i, $i \leq l-2$, l'équation $x^l + y^l = z^l$ n'a pas de solutions en nombres entiers.*

Démonstration. On a vu que :

1. Si $\mathbf{C}(l)$: l divise le numérateur d'un des B_i, $i \leq l-2$, alors $\mathbf{A}(l)$: l est régulier (6.7.1)
2. Si $\mathbf{A}(l)$, alors $\mathbf{B}(l)$: le lemme de Kummer est vrai (6.6.2).
3. Si $\mathbf{A}(l)$ et si $\mathbf{B}(l)$, l'équation $x^l + y^l = z^l$ n'a pas de solution (3.3.13).

□

6.8 Appendice : lemme algébrique

Lemme 6.8.1. *Soit G un sous groupe de $(\mathbb{Z}/l\mathbb{Z})^*$. Soit G^* l'ensemble de ses caractères. Soit une fonction $f : G \to \mathbb{C}$. Soit $\mathcal{M}$ la matrice définie par $M_{\sigma,\tau} = f(\sigma\tau^{-1})$. Alors*

$$\det \mathcal{M} = \prod_{\chi \in G^*} \sum_{\sigma} f^\sigma \chi^\sigma$$

Démonstration.

1. Soit $f \to T_\omega f$ défini par $T_\omega f^\sigma = f(\omega\sigma)$
2. Les caractères de G sont vecteurs propres de T_ω : $T_\omega \chi^\sigma = \chi(\omega\sigma) = \chi(\omega)\chi^\sigma$. La valeur propre associée à χ est $\chi(\omega)$
3. La matrice $\mathcal{M}$ de l'énoncé est la matrice de l'operateur $T = \sum_\omega f(\omega)T_\omega$ dans la base formée des fonctions L_σ définies par

$L_\sigma(\tau) = 1$ si $\sigma = \tau$ et $= 0$ sinon.

4. Soit χ un caractère. On a :

$$\begin{aligned} T(\chi) &= \sum_\omega f(\omega) T_\omega(\chi) = \sum_\omega f(\omega)\chi(\omega)\chi \\ &= \left(\sum_\omega f(\omega)\chi(\omega)\right)\chi \end{aligned}$$

χ est un vecteur propre de T associé à $\sum_\omega f(\omega)\chi(\omega)$.

5. Le déterminant de $\mathcal{M}$ est égal au produit des valeurs propres.

□

6.9 Appendice : nombres et polynômes de Bernoulli

Definition 6.9.1. *Les **nombres de Bernoulli** sont définis par :*

$$\sum_{n\geq 0} B_n \frac{t^n}{n!} = \frac{t}{e^t - 1}$$

Lemme 6.9.2. $B_0 = 1$, $B_1 = -1/2$.

Démonstration. Au voisinage de 0, $e^t = 1 + t + (1/2)t^2 + t^2 s(t)$, où $s(t)$ est continue et telle que $\lim_{t\to 0} s(t) = 0$.

$$B_0 = \lim_{t\to 0} \frac{t}{e^t - 1} = 1 \qquad B_1 = \lim_{t\to 0} \left(\frac{t}{e^t - 1}\right)' = -1/2$$

□

Lemme 6.9.3.

$$t \to y(t) \quad = \quad \frac{t}{e^t - 1} - (1 - \frac{1}{2}t)$$

est une fonction paire.

Démonstration. On développe $y(t) - y(-t)$.

$$\begin{aligned} y(t) - y(-t) &= \left(\frac{t}{e^t - 1} - (1 - \frac{1}{2}t)\right) - \left(\frac{-t}{e^{-t} - 1} - (1 + \frac{1}{2}t)\right) \\ &= \frac{t}{e^t - 1} + \frac{t}{e^{-t} - 1} + t = \frac{t}{e^t - 1} + \frac{te^t}{1 - e^t} + t = -t + t = 0 \end{aligned}$$

□

Lemme 6.9.4. *Pour n impair* ≥ 3, $B_n = 0$.

Démonstration. Corollaire des lemmes précédents . □

Definition 6.9.5. *Les* ***polynômes de Bernoulli*** *sont les coefficients de*

$$\sum_n B_n(x)\frac{t^n}{n!} \quad = \quad \frac{te^{xt}}{e^t - 1}$$

Lemme 6.9.6. $B_n = B_n(0)$

Démonstration. Découle des définitions. □

Lemme 6.9.7. *$B_n(x)$ est un polynôme en x de degré n.*

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$$

Démonstration.

$$\begin{aligned}
\sum_n B_n(x)\frac{t^n}{n!} &= \frac{te^{xt}}{e^t-1} = \frac{t}{e^t-1}e^{xt} \\
&= \sum_{k\geq 0} B_k \frac{t^k}{k!} \sum_{j\geq 0} x^j \frac{t^j}{j!} \\
&= \sum_{n\geq 0} \left(\sum_{k+j=n} B_k x^j \frac{n!}{k!j!} \right) \frac{t^n}{n!} \\
&= \sum_{n\geq 0} \left(\sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k} \right) \frac{t^n}{n!}
\end{aligned}$$

On égalise les coefficients. □

Lemme 6.9.8. *$B_n(x)$ vérifie :*

$$\int_y^{y+1} B_n(x)dx = y^n$$

Démonstration. On a :

$$\frac{\partial}{\partial x}\left(\frac{e^{xt}}{e^t-1}\right) = \frac{te^{xt}}{e^t-1}$$

$$\left[\frac{e^{xt}}{e^t-1}\right]_y^{y+1} = \frac{e^{(y+1)t}}{e^t-1} - \frac{e^{yt}}{e^t-1} = e^{yt}$$

Et :

$$\int_y^{y+1} \sum_n B_n(x)\frac{t^n}{n!}dx = \int_y^{y+1} \frac{te^{xt}}{e^t-1}dx$$

On égalise les coefficients. □

Lemme 6.9.9. $B_n(x+1) - B_n(x) = nx^{n-1}$

Démonstration. On dérive l'égalité de 6.9.8. □

Lemme 6.9.10.

$$B_n = -\frac{1}{n+1}\sum_{k=0}^{n-1}\binom{n+1}{k}B_k$$

Démonstration.

1. $B_n = B_n(0)$ par définition.
2. $B_n(1) = B_n(0)$ d'après 6.9.9.
3. En utilisant 6.9.7, on a :

$$\begin{aligned} B_{n+1} = B_{n+1}(1) &= \sum_{k=0}^{n+1}\binom{n+1}{k}B_k \\ &= \sum_{k=0}^{n}\binom{n+1}{k}B_k + B_{n+1} \end{aligned}$$

Soit

$$\begin{aligned}\sum_{k=0}^{n}\binom{n+1}{k}B_k &= 0\\ \sum_{k=0}^{n-1}\binom{n+1}{k}B_k+(n+1)B_n &= 0\end{aligned}$$

□

Lemme 6.9.11. *Soit l un nombre premier. Si $1 \leq n < l-1$, le dénominateur de B_n n'est pas divisible par l.*

Démonstration. Corollaire du précédent. □

Notation 6.9.12. *Soit l un nombre premier. On pose :*

$$S_k = \sum_{i=1}^{l-1} i^k$$

Lemme 6.9.13. *On a :*

$$S_k = \frac{1}{k+1}\left(\sum_{h=0}^{k}\binom{k+1}{h}B_h l^{k+1-h}\right)$$

Démonstration.

$$\begin{aligned} S_k &= \sum_{i=1}^{l-1} i^k = \sum_{i=1}^{l-1} \frac{1}{k+1} \left(B_{k+1}(i+1) - B_{k+1}(i)\right) \\ &= \frac{1}{k+1} \left(B_{k+1}(l) - B_{k+1}(1)\right) \\ &= \frac{1}{k+1} \left(\sum_{h=0}^{k+1} \binom{k+1}{h} B_h l^{k+1-h} - B_{k+1} \right) \\ &= \frac{1}{k+1} \left(\sum_{h=0}^{k} \binom{k+1}{h} B_h l^{k+1-h} \right) \end{aligned}$$

□

Lemme 6.9.14. *Soit l un nombre premier. Soit $k \in \{2, 4, 6, \ldots, l-3\}$. S_k n'est pas divisible par l^2 si et seulement si le numérateur d'un de B_k n'est pas divisible par l.*

Démonstration. D'apres 6.9.11, l ne divise pas le dénominateur des nombres B_k. On écrit $B_k = A_k/C_k$ avec $(C_k, l) = 1$. Soit le nombre entier $D_h = \prod_{i=0}^{k} C_i/C_h$. D'après le lemme précédent :

$$\begin{aligned} S_k &= \frac{1}{k+1} \left(\sum_{h=0}^{k} \binom{k+1}{h} \frac{A_h}{C_h} l^{k+1-h} \right) \\ (k+1) S_k \prod_{h=0}^{k} C_h &= \left(\sum_{h=0}^{k} \binom{k+1}{h} A_h D_h l^{k+1-h} \right) \\ &= \binom{k+1}{0} A_0 D_0 l^{k+1} + \binom{k+1}{1} A_1 D_1 l^k + \cdots + \binom{k+1}{k} A_k D_k l \end{aligned}$$

Puisque $k+1$, C_h et D_h sont premiers avec l, S_k est nul modulo l^2 si est seulement si A_k est nul modulo l. □

Lemme 6.9.15. *Soit l un nombre premier. Si* $(l-1)$ *divise m,* $S_m \equiv -1 \pmod{l}$.

Démonstration. D'après le petit théorème de Fermat $i^m \equiv -1 \pmod{l}$.

$$S_m = \sum_{i=1}^{l-1} i^m \equiv \sum_{i=0}^{l-1} 1 \equiv l-1 \equiv -1 \pmod{l}$$

□

Lemme 6.9.16. *Soit l un nombre premier. Si* $(l-1)$ *ne divise pas m,* $S_m \equiv 0 \pmod{l}$

Démonstration.

$$S_m = \sum_{i=1}^{l-1} i^m \equiv \sum_{j=0}^{l-2} g^{mj} \equiv \frac{g^{(l-1)m}-1}{g^m-1} \equiv 0 \pmod{l}$$

□

Lemme 6.9.17.

$$B_{n+1}(0) + B_{n+1}(\frac{1}{q}) + B_{n+1}(\frac{2}{q}) + \cdots + B_{n+1}(\frac{q-1}{q}) = q^{-n} B_{n+1}(0)$$

Démonstration. D'une part :

$$(qx)^{n+1} = \int_{qx}^{qx+1} B_{n+1}(t)dt = q \int_{x}^{x+1/q} B_{n+1}(y)du$$

D'autre part :

$$\begin{aligned}(qx)^{n+1} &= q^{n+1}\int_x^{x+1} B_{n+1}(t)dt = q^{n+1}\int_x^{x+1/q} B_{n+1}(y)du \\ &= q^{n+1}\sum_{j=0}^{q-1}\int_{x+j/q}^{x+(j+1)/q} B_{n+1}(y)du = q^{n+1}\int_x^{x+1/q}\sum_{j=0}^{q-1} B_{n+1}(y+j/q)du\end{aligned}$$

Comme c'est valable pour tout x on égalise les termes intégrés :

$$qB_{n+1}(y) = q^{n+1}\sum_{j=0}^{q-1} B_{n+1}(y+j/q)$$

On fait $y = 0$. □

On pose :

$$A_m = B_m + \sum_{l-1|m}\frac{1}{l}$$

Lemme 6.9.18. *Théorème de von Staudt. A_m est entier.*

Démonstration. Par récurrence. Le problème ne se pose que lorsque m est pair.

1. On a :

$$lB_m = S_m(l) - \sum_{k=0}^{m-1}\frac{1}{m+1}\binom{m+1}{k}l^{m-k}lB_k$$

2. Par hypothèse de récurrence, l ne divise pas le numérateur de

lB_k.

3. Soit

$$A_{m,k} = \frac{1}{m+1}\binom{m+1}{m+1-k}l^{m-k}$$

4. 2 ne divise pas le dénominateur de $A_{m,k}$ parce que $m+1$ est impair.

5. Si $l > 2$:

$$\begin{aligned} A_{m,k}l &= \frac{1}{m+1}\binom{m+1}{m+1-k}l^{m-k} \\ &= \frac{m(m-1)\dots(k+1)}{(m-k+1)!}l^{m-k} \end{aligned}$$

l figure dans $(m-k+1)! = r!$ avec l'exposant $[r/l] + [r/l^2] + \cdots \leq r/2 \leq r-1 = m-k$. Donc l ne divise pas le numérateur de $A_{m,k}$.

6. Donc l ne divise pas le numérateur de pB_m et $pB_m \equiv S_m(l) \mod l$.

7. D'où le résultat

□

Lemme 6.9.19. *Congruences de Fermat. Soit l un nombre premier. Si m − n est un multiple de l − 1, alors :*

$$\frac{B_n}{n} - \frac{B_m}{m}$$

est un multiple de l

Démonstration. Soit g une racine primitive modulo l. On pose $u = e^t - 1$.

1. On considère :

$$\begin{aligned} F(t) &= \frac{gt}{e^{gt}-1} - \frac{t}{e^t-1} = \sum_{n\geq 1} \frac{B_m(g^m-1)}{m!} t^m \\ &= \frac{gt}{(1+u)^g - 1} - \frac{t}{u} = t\left(\frac{1}{(1+u)^g-1} - \frac{1}{u}\right) \\ &= t\left(\sum_{k\geq 0} c_k u^k\right) = t\left(\sum_{k\geq 0} c_k (e^t-1)^k\right) = t\left(\sum_{m\geq 0} \frac{A_m}{m!} t^m\right) \end{aligned}$$

2. Montrons que l ne divise pas le dénominateur des nombres A_n et que, modulo l, ils sont périodiques de période $l-1$. D'après le petit théorème de Fermat $r^{n+l-1} \equiv r^n \mod l$; $e^{rt} = \sum_n r^n t^n / n!$ et la propriété est vérifié pour e^{rt}. Elle est également vérifiée pour $(e^t-1)^k$ qui est une combinaison linaire de fonctions e^{rt}. Les coefficients c_k étant entiers, elle est donc vérifiée pour les nombres A_n.

3. On égalise les coefficients dans l'équation ci-dessus :

$$\begin{aligned} \frac{B_m(g^m-1)}{m!} &= \frac{A_{m-1}}{(m-1)!} \\ \frac{B_m}{m!}(g^m-1) &= A_{m-1} \end{aligned}$$

4. D'après le petit théorème de Fermat, les nombres $g^m - 1$ sont,

modulo l, périodiques de période $l - 1$. Il en est de même des nombres B_m/m. Ce qui est le résultat cherché.

□

Annexe A

Nombres algébriques

A.1 Corps de nombres algébriques

A.1.1 Extensions algébriques

Definition A.1.1. *Un **corps de nombres algébriques** est un corps contenant $\mathbb{Q}$, contenu dans $\mathbb{C}$, et qui est un espace vectoriel de dimension finie sur $\mathbb{Q}$.*

Definition A.1.2. *Soient $K \subset L$ deux corps de nombres algébriques. On dit que L est une **extension algébrique** de K. On la note L/K. On note $[L : K]$, la dimension de L espace vectoriel sur K.*

Lemme A.1.3. *Soit L/K une extension algébrique et $\alpha \in L$. Il existe un polynôme $P \in K[X]$ tel que $P(\alpha) = 0$.*

Démonstration. Soit n la dimension de L sur K. La série $1, \alpha, \alpha^2, \ldots, \alpha^n$ est liée. □

Lemme A.1.4. *Soit L/K une extension algébrique et $\alpha \in L$. Il existe un polynôme de plus petit degré tel que $P(\alpha) = 0$. Ce polynôme est irréductible.*

Démonstration. On procède par division euclidienne, jusqu'à ce qu'on ne le puisse plus. Soient P et Q deux polynômes unitaires, tels que $P(\alpha) = Q(\alpha) = 0$. Si $d(P) > d(Q)$, on divise P par Q, $P = QR + S$. Alors $S(\alpha) = 0$ et S est de degré inférieur à $d(Q)$. □

Definition A.1.5. *Un tel polynôme est le **polynôme minimal** de α.*

Lemme A.1.6. *Le plus petit sous corps de L contenant α, noté $= K(\alpha)$, est constituée de polynômes en α de degré inférieur à celui de de son polynôme minimal.*

Démonstration. 1. Par définition :

$$L = \{\gamma = Q(\alpha)/R(\alpha) \text{ avec } Q, R \in K[X] \text{ et } R(\alpha) \neq 0\}$$

2. Soit : $\gamma = Q(\alpha)/R(\alpha)$. Comme P est irréductible, R et P sont premiers entre eux. Il existe $U, V \in K[X]$ tels que $U(X)P(X) + V(X)R(X) = 1$. On écrit :

$$\gamma = \frac{Q(\alpha)}{R(\alpha)} = \frac{Q(\alpha)(U(\alpha)P(\alpha) + V(\alpha)R(\alpha))}{R(\alpha)} = Q(\alpha)V(\alpha)$$

3. Donc L est constituée de polynômes en α
4. On écrit $P(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_0 = 0$. On en déduit une égalité : $\alpha^n = -(a_{n-1}\alpha^{n-1} + a_0)/a_n$. Donc, dans un polynôme

en α, les termes de degré $\geq n$ se transforment en des termes de degré $< n$.

□

Lemme A.1.7. *Soit $L = K(\alpha, \beta)$. Il existe $\gamma \in L$ tel que $L = K(\gamma)$*

Démonstration. 1. Soient $A, B \in K[X]$ les polynômes minimaux de α et β. Soient $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ les racines de A. Soient $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ les racines de A. Soit $M = K(\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n)$

2. On considère l'ensemble :

$$\Gamma = \{\frac{\alpha_i - \alpha_{i'}}{\beta_j - \beta_{j'}}\} \text{ avec } j \neq j'$$

3. $\Gamma \subset M$ est fini et $K \subset M$ est infini. Soit $\theta \in K, \theta \notin \Gamma$. On pose $\gamma = \alpha + \theta\beta$.
4. On a $K(\gamma) \subset K(\alpha, \beta)$.
5. Montrons la réciproque.
   a) On considère les polynômes $B(X) \in K(\gamma)[X]$ et $C(X) = A(\gamma - \theta X) \in K(\gamma)[X]$.
   b) Ils ont une racine commune : $B(\beta) = 0$ et $C(\beta) = A(\gamma - \theta\beta) = A(\alpha) = 0$.
   c) S'ils ont une autre racine commune, c'est une des racines de B et elle correspond à une racine de A. En considérant les égalités obtenues, et en les soustrayant, on obtient que $\theta \in \Gamma$, ce qui n'est pas.

d) Le PGCD de A et C dans $M(\gamma)$[X] est donc le polynôme $X - \beta$. Mais, comme on le voit en le calculant avec l'algorithme d'Euclide, c'est aussi le PGCD de A et C dans $K(\gamma)[X]$.

e) Donc $X - \beta \in K(\gamma)[X]$. Donc $\beta \in K(\gamma)$ et $\alpha = \gamma - \theta\beta \in K(\gamma)$.

□

Théoreme A.1.8. ***Théorème de l'élément primitif****. Soit L un corps de nombres algébriques. Il existe $\gamma \in L$ tel que $L = K(\gamma)$*

Démonstration. On écrit $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ et on itère A.1.7.

□

Definition A.1.9. *Le nombre algébrique γ du théorème précédent est un* ***élément primitif*** *de l'extension L.*

A.1.2 Extensions galoisiennes

Soit $\mathbb{Q} \subset K \subset \mathbb{C}$ un corps qui est un espace vectoriel de dimension finie sur $\mathbb{Q}$.

Definition A.1.10. *Soit $P(X) \in K[X]$. Le* ***corps de décomposition*** *L de P est le sous-corps de $\mathbb{C}$ engendré par K et les racines de P : $L = K(\alpha_1, \ldots, \alpha_n)$. L'extension L/K est dite* ***galoisienne****.*

Definition A.1.11. *Le* ***groupe de Galois*** *du polynôme P est constitué des automorphismes σ de son corps de décomposition et invariants sur K, i.e. tels que $\sigma(\alpha) = \alpha$ pour tout $\alpha \in K$. On le note : $Gal(L/K)$.*

Lemme A.1.12. *Soit L une extension galoisienne de K, de groupe de Galois G. Alors K est le sous-corps de L fixé par G.*

Démonstration. Par définition : $G = \{\sigma : L \to L \mid \sigma(\alpha) = \alpha, \forall \alpha \in K\}$; donc K est fixé par G. Réciproquement, soit $\beta \in L$ et $\sigma \in G$ tels que $\sigma(\beta) \neq \beta$; alors, forcément $\beta \notin K$. □

Lemme A.1.13. *L'ordre de $Gal(L/K)$ est fini.*

Démonstration. $Gal(L/K)$ peut être considéré comme un sous groupe du groupe symétrique $S(n)$: il est défini par la façon avec laquelle ses éléments permutent les racines du polynôme P. □

Lemme A.1.14. *$[L : K]$ est égal à l'ordre du groupe $Gal(L/K)$.*

Démonstration.

1. Soit α un élément primitif de l'extension K et P le polynome minimal de α. Il est de degré $[L/K]$ et toutes ses racines sont simples.
2. Un automorphisme $\sigma \in Gal(L/K)$ est déterminé par sa valeur en α : $\sigma(Q(\alpha)) = Q(\sigma(\alpha))$ pour tout $Q \in K[X]$. En particulier $P(\sigma(\alpha)) = \sigma(P(\alpha)) = 0$. Donc $\sigma(\alpha)$ est une des autres racines de P et il y en a $[L : K]$.

□

Lemme A.1.15. *Soit L une extension galoisienne de K, de groupe de Galois $G = \{\gamma_i\}$. S'il existe des coefficients $\alpha_i \in L$ tels que pour tout $\alpha \in L$, $\sum_i \alpha_i \gamma_i(\alpha) = 0$, alors ils sont tous nuls : $\alpha_i = 0$ pour tout i.*

Démonstration. 1. En réordonnant au besoin le groupe G, on considère une relation $\sum_{i=1}^{m} a_i\gamma_i(\alpha) = 0$ où m est le plus petit possible. Du coup, tous les a_i, $1 \leq i \leq m$ sont non nuls.

2. Les γ_i sont différents. Il existe β tel que $\gamma_1(\beta) \neq \gamma_2(\beta)$

$$\sum_{i=1}^{m} a_i\gamma_i(\alpha\beta) = 0$$
$$\sum_{i=1}^{m} a_i\gamma_i(\alpha)\gamma_i(\beta) = 0$$
$$\gamma_1(\beta)\sum_{i=1}^{m} a_i\gamma_i(\alpha) = 0$$
$$\sum_{i=1}^{m} a_i\left(\gamma_i(\beta) - \gamma_1(\beta)\right)\gamma_i(\alpha) = 0$$

3. Et une relation avec un terme de moins, celui correspondant à $i = 1$, et dont le second coefficient $a_2(\gamma_2(\beta) - \gamma_1(\beta)$ est non nul.

□

A.1.3 Norme, trace et discriminant

Lemme A.1.16. *Soit L/K une extension algébrique. Alors la **trace relative** et la **norme relative** de $\beta \in L$ sont la norme et la trace de la multiplication par β considérée comme un endomorphisme de L, espace vectoriel sur K. On les note $T_{L/K}(\beta)$ et $N_{L/K}(\beta)$*

Lemme A.1.17. *Soit $\beta \in L$. Alors $N_{L/K}(\beta) \in K$ et $T_{L/K}(\beta) \in K$*

Démonstration. Par définition. □

Lemme A.1.18. *Soit L/K une extension algébrique. Soit $\beta \in L$. Soit $J = K(\beta)$. Soit $m = [J : K]$. Alors : $T_{L/K}(\beta) = m \times T_{J/K}(\beta)$ et $N_{L/K}(\beta) = \left(N_{J/K}(\beta)\right)^m$.*

Démonstration.

1. Soit λ_i une base de J sur K. Soit ν_j une base de L sur J. Les nombres algébriques $\lambda_i \nu_j$ constituent une base de L sur K.
2. Soit $M = (\mu_{ik})$ la matrice de la multiplication de par α dans J.
3. $\beta\lambda_i = \sum_k \mu_{ik}\lambda_k$.
4. $\beta(\lambda_i\nu_j) = (\beta\lambda_i)\nu_j = \sum_k \mu_{ik}\lambda_k\nu_j = \sum_{kl} \mu_{ik}\delta_{jl}\lambda_k\nu_l$
5. La matrice de la multiplication par α dans L est de la forme :

$$\begin{pmatrix} M & 0 & \dots & 0 \\ 0 & M & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & & 0 \dots & M \end{pmatrix}$$

□

Lemme A.1.19. *Soit L une extension algébrique de la forme $L = K(\alpha)$, α étant un élément primitif. Soit P le poynôme minimal de α : $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Alors $T_{L/K}(\alpha) = -a_{n-1}$, $N_{L_K}(\alpha) = (-1)^n a_0$.*

Démonstration. Dans la base $1, \alpha, \ldots, \alpha^{n-1}$, la matrice de la multiplication par α dans L est

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

□

Lemme A.1.20. *Soit L une extension galoisienne de la forme $L = K(\alpha)$, α étant un élément primitif. Soit $Gal(L/K) = \{\sigma_i\}$ son groupe de Galois. Alors : $T_{L/K}(\alpha) = \sum_i \sigma_i(\alpha)$ et $N_{L/K}(\alpha) = \prod_i \sigma_i(\alpha)$*

Démonstration. On utilise les notations de A.1.19. Le résultat découle de ce que les éléments du groupe de Galois permutent les racines du polynôme minimal de α.

□

Lemme A.1.21. *Soit L/K une extension galoisienne de groupe de Galois $Gal(L/K) = \{\sigma_1, \sigma_2 \ldots, \sigma_n\}$. Alors : $N_{L/K}(\beta) = \sum_i \sigma_i(\beta))$ et $T_{L/K}(\beta) = \prod_i \sigma_i(\beta))$.*

Démonstration. Découle A.1.20 et de A.1.18. □

Definition A.1.22. *Soit L/K une extension algébrique. Soient $(\beta_1, \beta_2, \ldots, \beta_n) \in$*

L^n. Leur ***discriminant relatif*** *de est donné par :*

$$D_{L/K}(\beta_1, \beta_2, \ldots, \beta_n) \quad = \quad \det\left(T_{L/K}(\beta_i\beta_j)\right)$$

Lemme A.1.23. *Soit L/K une extension galoisienne de groupe de Galois $Gal(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. Alors :*

$$D_{L/K}(\beta_1, \ldots, \beta_n) \quad = \quad \left(\det\left(\sigma_k(\beta_i)\right)\right)^2$$

Démonstration.

$$\begin{aligned} D_{L/K}(\beta_1, \beta_2, \ldots, \beta_n) &= \det\left(\sum_k \sigma_k(\beta_i\beta_j)\right) = \det\left(\sum_k \sigma_k(\beta_i)\sigma_k(\beta_j)\right) \\ &= \det\left(\sigma_k(\beta_i)\right).\det\left(\sigma_k(\beta_j)\right) = \left(\det\left(\sigma_k(\beta_i)\right)\right)^2 \end{aligned}$$

□

Lemme A.1.24. *Si $(\beta_1, \ldots, \beta_n) \in L^n$ est une base de L sur K, alors $D_{L/K}(\beta_1, \ldots, \beta_n) \neq 0$.*

Démonstration. Si le discriminant $D_{L/K}(\beta_1, \ldots, \beta_n) = 0$, il existe des nombres $\alpha_i \in K$, tels que $\sum_i \alpha_i\sigma_i(\beta_j) = 0$, pour tout j. On a donc, puisque les β_i forment une base de L, $\sum_i \alpha_i\sigma_i(\beta) = 0$ pour tout $\beta \in L$. Ce qui est contradictoire avec A.1.15. □

Lemme A.1.25. *Si $(\beta_1, \ldots, \beta_n)$ est une base de L sur K, il existe une base $(\gamma_1, \ldots, \gamma_n)$ de L sur K telle que $T_{L/K}(\beta_i\gamma_j) = \delta_{ij}$.*

Démonstration. Découle immédiatement du résultat précédent et de la théorie élémentaire des formes bilinéaires non dégénérées.

1. $T_{L/K}$ est non dégénérée.
2. Si $T_{L/K}(\alpha\beta) = 0$ pour tout $\beta \in L$, alors $\alpha = 0$.
3. Pour $\alpha \in L$, on considère, la forme linéaire $l_\alpha : L \to K$, définie par $l_\alpha(\beta) = T_{L/K}(\alpha\beta)$. L'application $\alpha \to l_\alpha$ est une application linéaire injective de L dans son dual.
4. Comme L est de dimension finie, les nombres γ_i cherchés correspondent à la base duale de $(\beta_1, \ldots, \beta_n)$.

□

A.2 Corps finis

Lemme A.2.1. *Soit K un corps fini. Il existe un nombre premier p tel que $px = 0$ pour tout $x \in K$.*

Démonstration. On considère $1 \in K$. Puis l'application θ du groupe additif de $\mathbb{Z}^+$ dans $K : n \to \theta(n) = 1 + 1 + \cdots + 1$, ($n$ fois). On l'étend facilement à homomorphisme de groupe en posant $\theta(-n) = -\theta(n)$. Son noyau n'est pas vide. C'est en fait un idéal de $\mathbb{Z}$. Il est principal. S'il est de la forme (ab) avec $a > 1, b > 1$, les images de a et b ne seraient pas nulles dans K alors que le produit de leurs images le serait. K ne serait pas intègre. □

Definition A.2.2. *p est la **caractéristique** du corps K.*

Lemme A.2.3. *$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps fini d'ordre p de caractéristique p.*

Démonstration. Soit $\overline{a} \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\overline{a} \neq 0$. Alors a et p sont premiers entre eux. Il existe u et v dans $\mathbb{Z}$ tels que $au + pv = 1$. Alors $\overline{a}\,\overline{u} = \overline{1}$ et $\overline{a}$ est inversible. Donc $\mathbb{Z}/p\mathbb{Z}$ est un corps. Soit $x \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ alors $p.x = 0$, donc $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est de caractéristique p. □

Lemme A.2.4. *Un corps fini de caractéristique p contient $\mathbb{F}_p$ comme sous-corps.*

Démonstration. Comme auparavant, on considère l'injection de $\mathbb{F}_p$ dans K définie par $\overline{n} \longrightarrow \theta(n) = 1 + 1 + \cdots + 1$, ($n$ fois). □

Lemme A.2.5. *Le cardinal d'un corps fini de caractéristique p est de la forme p^n*

Démonstration. Le corps fini K peut être considéré comme un espace vectoriel sur son sous-corps $\mathbb{F}_p$. Si la dimension de cet espace vectoriel est m, le cardinal de K est p^m. □

Lemme A.2.6. *Si K est de cardinal p^n, alors tout élément de K^* est une racine de $X^{p^n-1} - 1$.*

Démonstration. Le groupe multiplicatif K^* a $p^n - 1$ éléments. Donc $\alpha^{p^n-1} = 1$ pour tout $\alpha \in K^*$. □

Lemme A.2.7. *Si K est de cardinal p^n, alors tout élément de K est une racine simple de $X^{p^n} - X$.*

Démonstration. Avec le lemme précédent, il est évident que tout élément de K est une racine de $X^{p^n} - X$. Dans $\mathbb{F}_p[X]$, la dérivée de $X^{p^n} - X$ vaut $p^n X^{p^n-1} - 1 = -1 \neq 0$; donc toute racine est simple □

Lemme A.2.8. *K est le corps de décomposition du polynôme $X^{p^n} - X$.*

Démonstration. Évidente avec le lemme précédent. □

Lemme A.2.9. *Tous les corps finis de cardinal p^m sont isomorphes. On les note $\mathbb{F}_{p^m}$.*

Démonstration. Évidente avec le lemme précédent. □

Lemme A.2.10. *L'extension $[\mathbb{F}_{p^m} : \mathbb{F}_p]$ est Galoisienne de degré m.*

Démonstration. Évidente avec les lemmes précédents. □

Lemme A.2.11. *$Gal(\mathbb{F}_{p^m}/\mathbb{F}_p)$ est cyclique d'ordre m engendré par l'automorphisme $\sigma_p : \alpha \to \alpha^p$.*

Démonstration. En considérant que les coefficients binomiaux impliqués dans le développement à la puissance p, on voit que : $(\alpha+\beta)^p = \alpha^p + \beta^p$. Donc σ_p est un automorphisme. On a $\sigma_p^m(\alpha) = \alpha^{p^m} = \alpha$. L'ordre de σ_p est m : s'il valait $n < m$, le polynôme $X^{p^n} - X$ s'annulerait pour tous les éléments de $\mathbb{F}_{p^m}$ et aurait un

nombre de racines supérieures à son degré. On a donc m automorphismes différents : $1, \sigma_p, \ldots, \sigma_p^{m-1}$, et le degré de l'extension est m □

Lemme A.2.12. $T_{\mathbb{F}_{p^m}/\mathbb{F}_p}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \alpha^{p^{r-1}}$

Démonstration. Soit $G = Gal(\mathbb{F}_{p^m}/\mathbb{F}_p)$. Alors $T_{\mathbb{F}_{p^m}/\mathbb{F}_p}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$. □

Lemme A.2.13. *La fonction trace n'est pas identiquement nulle.*

Démonstration. Dans un corps fini, la fonction trace est un polynôme de degré p^{r-1}. Ce degré est plus petit que la dimension de l'extension p^r. Le polynôme ne peut être identiquement nul. □

A.3 Anneaux d'entiers algébriques

A.3.1 Définitions et généralités

Definition A.3.1. *Un **entier** algébrique α est une solution d'une équation de la forme : $P(\alpha) = 0$, où le polynôme $P(X) \in \mathbb{Z}[X]$ est unitaire : le coefficient de son terme de plus haut degré est* 1.

Lemme A.3.2. *Soit K un corps de nombres algébriques sur $\mathbb{Q}$. Soit $\alpha \in K$. Les propriétés suivantes sont équivalentes :*

1. *α est un entier algébrique.*
2. *$\mathbb{Z}[\alpha]$ est un $\mathbb{Z}$-module de type fini.*

3. *Il existe un sous anneau A de K contenant α et qui est un $\mathbb{Z}$-module de type fini.*

Démonstration. — $1 \to 2$. Comme $\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_0)$, le $\mathbb{Z}$-module engendré par $1, \alpha, \ldots, \alpha^{n-1}$ fait l'affaire.

— $2 \to 3$ est évident.

— $3 \to 1$. Soit un anneau $A \subset K$ qui contient α et qui est un $\mathbb{Z}$-module de type fini. Soient $\beta_1, \ldots, \beta_n$ qui engendrent A sur $\mathbb{Z}$. Pour tout i, $\alpha\beta_i \in A$ et on peut écrire : $\alpha\beta_i = \sum_j a_{ij}\beta_i$, i. e., $\sum_j c_{ij}\beta_i = 0$ avec $c_{ij} = \alpha\delta_{ij} - a_{ij}$. Le déterminant de la matrice c_{ij} est nul. C'est un polynôme en α qui est unitaire et à coefficients entiers.

□

Notation A.3.3. *On note O_K l'ensemble des entiers algébriques sur $\mathbb{Z}$ contenus dans le corps K.*

Lemme A.3.4. *O_K est un anneau.*

Démonstration. Soient $\alpha, \beta \in O_K$. Alors $\mathbb{Z}[\alpha]$ et $\mathbb{Z}[\beta]$ sont de rangs finis sur $\mathbb{Z}$. Donc $\mathbb{Z}[\alpha, \beta]$ est de rang fini sur $\mathbb{Z}$. Donc $\alpha + \beta$ et $\alpha\beta$ appartiennent à O_K. □

Lemme A.3.5. *O_K est un $\mathbb{Z}$-module libre de rang n*

Démonstration. 1. Soit $\{\alpha_1, .., \alpha_n\}$ une base de K sur $\mathbb{Q}$. Chaque α_i satisfait à une équation algébrique à coefficients dans $\mathbb{Q}$, donc par multiplication par le produit de dénominateurs à une équation du type : $a_{i,n}X^n + a_{i,n-1}X^{n-1} + \ldots a_{i,0} = 0$, $a_i \in \mathbb{Z}$.

2. On pose $\beta_i = a_{i,n}\alpha_i$. Chaque β_i est entier sur $\mathbb{Z}$.
3. Donc $\{\beta_1, .., \beta_n\}$ est une base de K sur $\mathbb{Q}$ contenue dans O_K.
4. D'après A.1.25, il existe une autre base $\{\gamma_1, .., \gamma_n\}$ de K sur $\mathbb{Q}$ telle que $T_{K/\mathbb{Q}}(\beta_i\gamma_j) = \delta_{ij}$.
5. Soit $\lambda \in O_K$. On peut l'écrire $\lambda = \sum_i b_i\gamma_i$ avec $b_i \in \mathbb{Q}$.
6. Pour tout i, $\lambda\beta_i \in O_K$. Donc $T_{K/\mathbb{Q}}(\lambda\beta_i) \in \mathbb{Z}$.
7. Or :

$$T_{K/\mathbb{Q}}(\lambda\gamma_j) \quad = \quad T_{K/\mathbb{Q}}(\sum_i b_i\beta_i\gamma_j) = \sum_i b_i T_{K/\mathbb{Q}}(\beta_i\gamma_j) = b_j \in \mathbb{Z}$$

8. Donc λ est contenu dans le sous module libre de base $\{\gamma_1, .., \gamma_n\}$

□

A.3.2 Idéaux fractionnaires

Definition A.3.6. *Dans O_K , le produit $\mathfrak{a}\mathfrak{b}$ de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ est le sous ensemble des sommes finies : $\sum_i \alpha_i\beta_i$ où $\alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{b}$.*

Definition A.3.7. *L'inverse $\mathfrak{a}^{-1}$ d'un idéal $\mathfrak{a} \subset O_K$ est le sous ensemble de K : $\{\mu \in K$ tels que $\alpha\mu \in O_K$ pour tout $\alpha \in \mathfrak{a}\}$*

Definition A.3.8. *Un idéal fractionnaire est de la forme $\mathfrak{a}^{-1}\mathfrak{b}$, où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de A.*

Lemme A.3.9. *Les idéaux fractionnaires forment un groupe multiplicatif.*

Démonstration. On vérifie immédiatement les axiomes de définition d'un groupe.

1. La multiplication est associative
2. L'élément neutre est A lui même.
3. L'inverse de $\mathfrak{a}^{-1}\mathfrak{b}$ est $\mathfrak{b}^{-1}\mathfrak{a}$.

□

A.3.3 Norme absolue

Definition A.3.10. *La norme absolue d'un idéal $\mathfrak{a} \subset O_K$, est donnée par $\|\mathfrak{a}\| = \#(O_K/\mathfrak{a})$.*

Lemme A.3.11. *Soit K un corps de nombres algébriques. Soit $\alpha \in O_K$, et (α) l'idéal qu'il engendre, alors $N_{K/\mathbb{Q}}(\alpha) = \|(O_K/(\alpha)\|$.*

Démonstration.
1. $N_{K/\mathbb{Q}}(\alpha)$ est le déterminant de la multiplication par α dans O_K.
2. C'est l'indice du $\mathbb{Z}$-module engendré par α dans O_K.
3. C'est le cardinal de $O_K/[\alpha]$.

□

Lemme A.3.12. $\|\mathfrak{ab}\| = \|\mathfrak{a}\|\,\|\mathfrak{b}\|$

Démonstration.
1. Si $(\mathfrak{ab}) = 1$, alors $(O_K/\mathfrak{ab}) \simeq (O_K/\mathfrak{a}) \times (O_K/\mathfrak{b})$ et $\|\mathfrak{ab}\| = \|\mathfrak{a}\|\,\|\mathfrak{b}\|$.
2. Si $\mathfrak{p}$ est premier, alors $(O_K/\mathfrak{p}^n)/(O_K/\mathfrak{p}^{n-1}) \simeq (O_K/\mathfrak{p})$ et $\|\mathfrak{p}^n\| = \|\mathfrak{p}\|^n$.

□

A.3.4 Idéaux premiers

Lemme A.3.13. *Tout idéal premier* $\mathfrak{p}$ *de* O_K *différent de* $\{0\}$ *est maximal :* $O_K/\mathfrak{p}$ *est un corps.*

Démonstration. 1. Soit $\beta \in \mathfrak{p}$, $\beta \neq 0$. Soit $P(X) = a_0 + a_1 X + \cdots + X^n \in \mathbb{Z}[X]$ de degré minimal tel que $P(\beta) = 0$. Alors a_0 est différente de 0 et $a_0 = -(a_1\beta + \cdots + \beta^n) \in \mathbb{Z} \bigcap \mathfrak{p}$. Donc $\mathbb{Z} \bigcap \mathfrak{p}$ est différent de $\{0\}$.

2. C'est un idéal premier de $\mathbb{Z}$. Il est de la forme $\mathbb{Z} \bigcap \mathfrak{p} = p\mathbb{Z}$.

   a) $\mathbb{Z} \bigcap \mathfrak{p}$ est le noyau de l'homomorphisme composé suivant : $\mathbb{Z} \to O_K \to O_K/\mathfrak{p}$.

   b) Il y a un homomorphisme injectif : $\mathbb{Z}/\mathbb{Z} \bigcap \mathfrak{p} \to O_K/\mathfrak{p}$.

   c) Il est évident qu'un sous anneau d'un anneau intègre est intègre. Donc $\mathbb{Z} \bigcap \mathfrak{p}$ est premier.

3. Le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un sous anneau de $B = O_K/\mathfrak{p}$. Chaque élément du second anneau est entier sur le premier. Le premier est un corps. Le second est un corps :

   a) Soit $\overline{\beta} \in B$, $\overline{\beta} \neq 0$ avec $\beta \in O_K$. Alors β est solution d'une équation $P(\beta) = 0$ avec $P \in \mathbb{Z}[X]$. On a $\overline{P}(\overline{\beta}) = 0$ et donc $\mathbb{F}_p[\overline{\beta}]$ est un espace vectoriel de dimension finie sur $\mathbb{F}_p$.

   b) L'application linéaire $\overline{\alpha} \to \overline{\alpha}\overline{\beta}$ est une application $\mathbb{F}_p$ linéaire de $\mathbb{F}_p[\overline{\beta}]$ dans lui même. Elle est injective car $\mathbb{F}_p[\overline{\beta}]$ est intègre. Elle est entre espaces vectoriels de

dimension finie. Elle est donc surjective. Et il existe $\overline{\gamma}$ tel que $\overline{\gamma}\overline{\beta} = 1$

c) $\overline{\beta}$ est inversible.

□

Lemme A.3.14. *Tout idéal* $\mathfrak{a}$ *de* O_K *se décompose de façon unique en idéaux premiers :* $\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i}$, $e_i \in \mathbb{N}$.

Démonstration. Existence :

1. Soit $\mathfrak{S}$ l'ensemble des idéaux sans factorisation. Supposons que $\mathfrak{S}$ est non vide.
2. Soit alors $\mathfrak{a}$ un idéal qui est maximal parmi tous les idéaux sans factorisation : tout idéal $\mathfrak{b}$ intermédiaire entre $\mathfrak{a}$ et O_K a une factorisation.
3. Par définition $\mathfrak{a}$ n'est pas premier et est strictement contenu dans un idéal premier $\mathfrak{p}$
4. Soit $\mathfrak{r} = \mathfrak{p}^{-1}\mathfrak{a}$. On a : $\mathfrak{a} \subsetneq \mathfrak{r} \subsetneq O_K$. En effet, $\mathfrak{a} \subset \mathfrak{p}$ implique que $\mathfrak{p}^{-1}\mathfrak{a} \subset O_K$. Et, si $\mathfrak{p}^{-1}\mathfrak{a} = O_K$, alors $\mathfrak{p} = \mathfrak{a}$, ce qui est contradictoire.
5. Donc $\mathfrak{r}$ a une factorisation $\mathfrak{q}_1 \dots \mathfrak{q}_m$. Et $\mathfrak{a}$ a une factorisation : $\mathfrak{r}\mathfrak{q}_1 \dots \mathfrak{q}_m$.
6. $\mathfrak{S}$ est vide.

Unicité :

1. Supposons que l'on ait $\mathfrak{p}_1 \dots \mathfrak{p}_n = \mathfrak{q}_1 \dots \mathfrak{q}_m$ avec $\mathfrak{p}_1 \neq \mathfrak{q}_j$ pour tout j.

2. Soit alors, pour tout j, $\alpha_j \in \mathfrak{q}_j, \notin \mathfrak{p}_1$.
3. Alors $\prod_j \alpha_j \in \prod_j \mathfrak{q}_j = \prod_i \mathfrak{p}_i \subset \mathfrak{p}_1$.
4. Ce qui est contradictoire puisque $\mathfrak{p}_1$ est premier.

□

A.3.5 Décomposition des idéaux premiers

Lemme A.3.15. *Soit $p \in \mathbb{Z}$ un nombre premier. Il existe un nombre fini d'idéaux propres de O_K qui contiennent (p). Et on peut écrire $pO_K = \prod_{i \in I} \mathfrak{p}_i^{e_i}$, $e_i \in \mathbb{N}$*

Démonstration. Cas particulier de A.3.14. □

Definition A.3.16. *L'idéal $\mathfrak{p}_i$ est dit **au dessus de** p. L'entier e_i est l'**indice de ramification** de $\mathfrak{p}_i$.*

Lemme A.3.17. $\mathbb{Z} \bigcap \mathfrak{p}_i = (p)$

Démonstration. Il est évident que $(p) \subset \mathbb{Z} \bigcap \mathfrak{p}_i$. Si $n \in \mathbb{Z} \bigcap \mathfrak{p}_i$ et $n \notin (p)$, alors p et n sont premiers entre eux dans $\mathbb{Z}$; il existe u et v tels que $nu + pv = 1$; on en déduit que $1 \in \mathfrak{p}_i$ et $\mathfrak{p}_i = O_K$. □

Lemme A.3.18. *Le corps $O_K/\mathfrak{p}_i$ est une extension du corps $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Découle immédiatement du précédent. Voir la figure A.1. □

Definition A.3.19. *Le degré de l'extension $[O_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$, noté f_i, est l'**indice de décomposition** de $\mathfrak{p}_i$.*

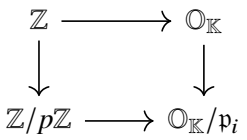

FIGURE A.1 – L'extension $[O_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$

Lemme A.3.20. *Il existe un isomorphisme canonique :*

$$O_K/pO_K \quad \to \quad \prod_i O_K/\mathfrak{p}_i^{e_i}$$

Démonstration. Théorème chinois des restes. □

Lemme A.3.21. *Il existe un isomorphisme canonique :*

$$O_K/\mathfrak{p} \quad \to \quad \mathfrak{p}_j/\mathfrak{p}_{j+1}$$

Lemme A.3.22. *Si l'extension $K : \mathbb{Q}$ est de degré n, $n = \sum_i e_i f_i$.*

Démonstration. Prendre les normes.

$$\begin{aligned} N_K(pO_K) &= \#(O_K/pO_K) = p^n \\ N_K(pO_k) &= \prod_i N(\mathfrak{p}_i)^{e_i} = \prod_i (p^{f_i})^{e_i} = p^{\sum_i f_i e_i} \end{aligned}$$

□

Lemme A.3.23. *Si l'extension $K : \mathbb{Q}$ est galoisienne de degré n, tous les e_i ont la même valeur e, tous les f_i ont la même valeur f et $n = g_p e f$.*

Démonstration. Si $pO_K = \prod_{i \in I} \mathfrak{p}_i^{e_i}$, $e_i \in \mathbb{N}$ et $\sigma \in G$, alors il existe j tel que $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$. Et $e_i = e_j$. Et $O_K/\mathfrak{p}_i$ est isomorphe à $O_K/\mathfrak{p}_j$. Donc $f_i = f_j$. □

Definition A.3.24. *Soit g_p le nombre des idéaux $\mathfrak{p}_i$ au dessus de p.*

1. *lorsque $g_p = 1$ et $e_1 = 1$, p est dit **inerte** dans O_K,*
2. *lorsque $g_p = 1$ et certains e_i sont supérieurs à 1, p est dit **complètement ramifié** dans O_K*
3. *lorsque $g_p > 1$ et certains e_i sont supérieurs à 1, p est dit **ramifié** dans O_K*
4. *lorsque $g_p > 1$ et et tous les e_i sont égaux à 1, p est dit **décomposé** dans O_K*

A.3.6 Discriminant et ramification

Definition A.3.25. *Soit B un anneau qui est A-module libre de rang fini sur A. Pour $b \in B$, on note $T_{B/A}(b)$ la trace de la multiplication par b dans B. Soit $(e_1, \ldots, e_n)$ une base de B sur A. Le **discriminant** de cette base est donné par :*

$$D_{B/A}(e_1, \ldots, e_n) \quad = \quad \det T_{B/A}(e_i e_j)$$

Lemme A.3.26. *Si $(f_1, \ldots, f_n)$ est une autre base de B sur A, et M est la matrice de changement de base, on a :*

$$D_{B/A}(f_1, \ldots, f_n) \quad = \quad (\det M)^2 D_{B/A}(e_1, \ldots, e_n)$$

Démonstration. Même preuve que pour les discriminants sur les corps. □

Definition A.3.27. *Le discriminant de B sur A, $D_A(B)$ est donné par $D_{B/A}(e_1, \ldots, e_n)$ pour une base quelconque. Il est défini au carré d'une unité près.*

Lemme A.3.28. $D_{\mathbb{Z}}(O_K) \equiv D_{\mathbb{Z}/p\mathbb{Z}}(O_K/pO_K) \pmod{p}$.

Démonstration. Soit ω_i une base de O_K sur $\mathbb{Z}$. On a $O_k = \oplus\mathbb{Z}\omega_i$. Alors $\overline{\omega_i}$ est une base de O_K/pO_K sur $\mathbb{Z}/p\mathbb{Z}$. On a $O_K/pO_K = \oplus(\mathbb{Z}/p\mathbb{Z})\overline{\omega}_i$. Soit $x \in O_K$ et m_x la matrice de la multiplication par x dans O_K. Elle se réduit modulo p à la matrice de la multiplication par $\overline{x}$ dans (O_K/pO_k). On applique la définition du discriminant. □

Lemme A.3.29. *Soient B_1 et B_2 deux anneaux qui sont des A modules libres de type fini. Alors $D_A(B_1 \times B_2) = D_A(B_1)D_A(B_2)$.*

Démonstration. On concatène une base $(e_1, \ldots, e_n)$ de B_1 et une base $(f_1, \ldots, f_m)$ de B_2. On a successivement : $T_{(B_1\times B_2)/A}(e_i e_j) = T_{B_1/A}(e_i e_j)$, $T_{(B_1\times B_2)/A}(f_k f_l) = T_{B_2/A}(f_l f_k)$ et $T_{(B_1\times B_2)/A}(e_i f_k) = 0$. On développe les définitions. □

Lemme A.3.30. $D_{\mathbb{Z}/p\mathbb{Z}}(O_K/pO_K) = \prod_i D_{\mathbb{Z}/p\mathbb{Z}}\left(O_K/\mathfrak{p}_i^{e_i}\right)$.

Démonstration. Immédiat à partir du lemme précédent et de A.3.20 □

Lemme A.3.31. *La trace d'un endomorphisme L nilpotent, i.e. tel que $L^m = 0$ pour un entier m, est nulle.*

Démonstration. Il suffit de démontrer ce résultat lorsque l'on considère L comme un endomorphisme d'un espace vectoriel de dimension m sur $\overline{K}$ où $\overline{K}$ est une clôture algébrique de K. Dans ce cadre L est triangulable. Comme $L^m = 0$, toutes les valeurs propres de L sont nulles ; donc la trace de L est nulle. □

Lemme A.3.32. *$D_{\mathbb{Z}/p\mathbb{Z}}(O_K/\mathfrak{p}^e) \equiv 0 \pmod{p}$ si et seulement si $e > 1$.*

Démonstration.

1. Si $e > 1$, soit $\omega \in \mathfrak{p}$, $\omega \notin \mathfrak{p}^e$. Il est clair que $\overline{\omega}$ est nilpotent. Soit $(\overline{\omega}, \overline{\omega}_2, \ldots, \overline{\omega}_n)$ une base de O_K/pO_K sur $\mathbb{Z}/p\mathbb{Z}$ commençant par $\overline{\omega}$. Les nombres $\overline{\omega}\,\overline{\omega}_i$ sont nilpotents. Donc leur trace est nulle. La première colonne de la matrice donnant le discriminant est nulle. Ce discriminant est nul.
2. Si $e = 1$, $O_K/\mathfrak{p}$ est un corps. Si le discriminant est égal à zéro, alors la fonction trace est nulle. Mais ce n'est pas le cas d'après A.2.13.

□

Théoreme A.3.33. *p se ramifie si et seulement si il divise le discriminant $D_{\mathbb{Z}}(O_K)$.*

Démonstration. On met en ordre les lemmes précédents.

1. p divise $D_{\mathbb{Z}}(O_K)$ si et seulement si l'un des $D_{\mathbb{Z}/p\mathbb{Z}}(O_K/\mathfrak{p}^{e_i}) \equiv 0 \pmod{p}$.
2. $D_{\mathbb{Z}/p\mathbb{Z}}(O_K/\mathfrak{p}^e) \equiv 0 \pmod{p}$ si et seulement si $e > 1$.

□

Lemme A.3.34. *Soient α et β deux entiers algébriques tels que $\mathbb{Z}(\alpha) \bigcap \mathbb{Z}(\beta) = \mathbb{Z}$. Soit p un nombre premier. S'il ne se ramifie ni dans $\mathbb{Z}(\alpha)$, ni dans $\mathbb{Z}(\beta)$, il ne se ramifie pas dans $\mathbb{Z}(\alpha,\beta)$*

Démonstration. Soient $O_L = \mathbb{Z}(\alpha)$, $O_K = \mathbb{Z}(\beta)$, $O_{KL} = \mathbb{Z}(\alpha,\beta)$. On écrit $pO_L = \prod_i \mathfrak{p}_i$, $pO_K = \prod_j \mathfrak{q}_j$, $pO_{KL} = \prod_k \mathfrak{r}_k^{e_k}$. Considérons $\mathfrak{r}_k$, il est situé au dessus d'un $\mathfrak{p}_i$ et d'un $\mathfrak{q}_j$: on a $\mathfrak{r}_k \bigcap O_L = \mathfrak{p}_i$ et $\mathfrak{r}_k \bigcap O_K = \mathfrak{q}_j$.

Comme $O_L \bigcap O_K = \mathbb{Z}$, $\mathfrak{r}_k \bigcap \mathbb{Z} = \mathfrak{p}_i \bigcap O_K = \mathfrak{q}_j \bigcap O_L$.

$\mathfrak{r}_k \bigcap \mathbb{Z}$ est un ideal de $\mathbb{Z}$. Soit s tel que que $\mathfrak{r}_k \bigcap \mathbb{Z} = (s)$.

□

A.4 Classes d'idéaux

A.4.1 Idéaux fractionnaires

Lemme A.4.1. *Un idéal fractionnaire $\mathfrak{f}$ de K est de la forme : $\mathfrak{f} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$, où chaque $\mathfrak{p}_i$ est un idéal premier de O_K et $e_i \in \mathbb{Z}$. On a : $\mathfrak{f} \subset K$*

Démonstration. Immédiate d'après la définition des idéaux fractionnaires (A.3.8) et le théorème de décomposition (A.3.14). □

Definition A.4.2. $\alpha \in K$ *engendre un* ***idéal fractionnaire principal*** $(\alpha) = \{\alpha\gamma \mid \gamma \in O_K\}$.

Lemme A.4.3. *Le groupe des idéaux fractionnaires principaux est un sous groupe du groupe des idéaux fractionnaires.*

Démonstration. Évidente. □

Definition A.4.4. *Le* ***groupe des classes d'idéaux*** *est le quotient du groupe des idéaux fractionnaires par le sous groupe des idéaux fractionnaires principaux.*

A.4.2 Finitude du nombre de classes

Soit σ un automorphisme de K. Si $\sigma(K) \subset \mathbb{R}$, σ est dit réel. Soit r le nombre d'automorphisems réels de K. Sinon, il est dit complexe. A tout automorphisme complexe σ est associé son conjugué complexe $\overline{\sigma} : \overline{\sigma}(\alpha) = \sigma(\overline{\alpha})$; on a : $\sigma \neq \overline{\sigma}$. Soit s le nombre de paires $(\sigma, \overline{\sigma})$ d'automorphismes complexes de K. On a $[K : \mathbb{Q}] = n = r + 2s$. On ordonne les automorphimes de K de la façon suivante : $(\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}})$.

Definition A.4.5. *Le* ***plongement canonique*** *est l'application* $C : K \to \mathbb{R}^r \times \mathbb{C}^s$ *définie par* $\alpha \in K \to C(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \ldots, \sigma_{r+s}(\alpha)$

Definition A.4.6. *La **norme géométrique** est l'application* $N : \mathbb{R}^r \times \mathbb{C}^s \to \mathbb{R}$ *définie par* $x = (x_1, \ldots, x_r, x_{r+1}, \ldots, x_{r+s}) \to N(x) = |x_1|..|x_r||x_{r+1}|^2..|x_{r+s}|^2$.

Lemme A.4.7. *Soit M un module libre rang* $n = r + 2s$ *de K. Soit* x_i *une base de M. Alors* $C(M)$ *est un réseau de* $\mathbb{R}^{r+2s}$ *dont le volume est* $\mu(C(M)) = 2^{-s}|\det(\sigma_i(x_j))|$.

Démonstration. Les composants de $C(x_i)$ dans la base canonique de $\mathbb{R}$ sont :

$$\sigma_1(x_i), \ldots, \sigma_r(x_1), \Re(\sigma_{r+1}(x_i)), \ldots, \Re(\sigma_{r+s}(x_i)), \Im(\sigma_{r+1}(x_i)), \ldots, \Im(\sigma_{r+s}(x_i))$$

Le volume de $C(M)$ est le déterminant :

$$\begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_r(x_1) & \Re(\sigma_{r+1}(x_1)) & \ldots & \Re(\sigma_{r+s}(x_1)) & \Im(\sigma_{r+1}(x_1)) & \ldots & \Im(\sigma_{r+s}(x_1)) \\ \ldots & \ldots & \ldots & \ldots & \ldots & & & & \\ \sigma_1(x_1) & \ldots & \sigma_r(x_1) & \Re(\sigma_{r+1}(x_1)) & \ldots & \Re(\sigma_{r+s}(x_1)) & \Im(\sigma_{r+1}(x_1)) & \ldots & \Im(\sigma_{r+s}(x_1)) \end{vmatrix}$$

Pour $n \geq r$, on pose :

$$\Re(\sigma_i(x_k)) = \frac{\sigma_i(x_j) + \overline{\sigma_i(x_j)}}{2} \qquad \Im(\sigma_i(x_j)) = \frac{\sigma_i(x_j) - \overline{\sigma_i(x_j)}}{2}$$

Avec ce changement, le volume de $C(M)$ est donné par :

$$\begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_r(x_1) & \sigma_{r+1}(x_1) & \ldots & \sigma_{r+s}(x_1) & \overline{\sigma_{r+1}}(x_1) & \ldots & \overline{\sigma_{r+s}}(x_1) \\ \ldots & \ldots & \ldots & \ldots & \ldots & & & & \\ \sigma_1(x_n) & \ldots & \sigma_r(x_n) & \sigma_{r+1}(x_n) & \ldots & \sigma_{r+s}(x_n) & \overline{\sigma_{r+1}}(x_n) & \ldots & \overline{\sigma_{r+s}}(x_n) \end{vmatrix}$$

□

Lemme A.4.8. *L'image de* O_K *par C est un réseau de* $\mathbb{R}^{r+2s}$. *Soit* $\mathfrak{a}$

un idéal de O_K, $C(\mathfrak{a})$ est un réseau de $\mathbb{R}^{r+2s}$. Et :

$$\begin{aligned} V(C(O_K)) &= 2^{-s}\sqrt{|D|} \\ V(C(\mathfrak{a})) &= 2^{-s}\sqrt{|D|}\, N(\mathfrak{a})) \end{aligned}$$

Démonstration. O_K et $\mathfrak{a}$ sont des $\mathbb{Z}$ modules libres de rang n. Si (x_i) est une $\mathbb{Z}$-base de O_K, on a $D = \det\left(\sigma_i(x_j)\right)^2$. Donc $V(C(O_K)) = 2^{-m}\sqrt{D}$. Pour la seconde égalité, on utilise le fait que $C(\mathfrak{a})$ est un sous groupe d'indice $N(\mathfrak{a})$ et qu'un domaine fondamental de $C(O_K)$ est obtenue en concaténant $N(\mathfrak{a})$ domaines fondamentaux de $C(\mathfrak{a})$. □

Lemme A.4.9. *Soit $\mathfrak{a}$ un idéal de O_K. Alors $\mathfrak{a}$ contient un élément α tel que*

$$|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{D}N(\mathfrak{a})$$

Démonstration. 1. Pour $x > 0$, soit $B_x \subset \mathbb{R}^r\mathbb{C}^s$ donné par :

$$B_x = \left\{(y_1, \ldots, y_r, z_1, \ldots, z_s,) \mid \sum_i |y_i| + 2\sum_j |z_j| < x\right\}$$

B_x est compact, convexe et symétrique par rapport à l'origine. Son volume est :

$$\mu(B_x) = 2^r \left(\frac{\pi}{2}\right)^s \frac{x^n}{n!}$$

2. Soit x tel que $x^n = 2^{n-r}\pi^{-s}n!\sqrt{|D|}N(\mathfrak{a})$. On a :

$$\mu(B_x) = 2^r\left(\frac{\pi}{2}\right)^s \frac{2^{n-r}\pi^{-s}n!\sqrt{|D|}N(\mathfrak{a})}{n!} = 2^{-s}2^n\sqrt{|D|}N(\mathfrak{a}) = 2^nV(C(\mathfrak{a}))$$

3. D'après A.6.6, il existe $\alpha \in \mathfrak{a}$ tel que $C(\alpha) \in B_x$.

4. On a, en utilisant l'inégalité entre moyenne arithmétique et moyenne géométrique :

$$\begin{aligned} |N(\alpha)| &= \prod_{i=1}^{r}|\sigma_i(\alpha)|\prod_{j=1}^{s}|\sigma_j(\alpha)|^2 \\ &\leq \left(\frac{1}{n}\sum_{j=i}^{r}|\sigma_i(\alpha)| + \frac{2}{n}\sum_{j=1}^{s}|\sigma_j(\alpha)|\right)^n \\ &\leq \frac{x^n}{n^n} \leq \frac{2^{n-r}\pi^{-s}n!\sqrt{|D|}N(\mathfrak{a})}{n^n} = \left(\frac{4}{\pi}\right)^s\frac{n!}{n^n}\sqrt{D}N(\mathfrak{a}) \end{aligned}$$

□

Lemme A.4.10. *Toute classe d'idéaux contient un idéal entier* $\mathfrak{b}$ *tel que*

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^s\frac{n!}{n^n}\sqrt{D}$$

Démonstration. Soit $\mathfrak{a}$ un idéal de la classe donnée tel que $\mathfrak{a}^{-1}$ est entier. Soit α donné par le lemme précédent. Alors $\mathfrak{b} = \alpha\mathfrak{a}^{-1}$ satisfait

l'inégalité cherchée :

$$N(\mathfrak{b}) \quad = \quad N(\alpha)N(\mathfrak{a}^{-1}) \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{D}N(\mathfrak{a})N(\mathfrak{a}^{-1}) = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{D}$$

□

Théoreme A.4.11. $\mathfrak{C}$ *est fini.*

Démonstration.

1. Le nombre des idéaux entiers $\mathfrak{b}$ dont la norme est un entier donné q est fini. En effet on a pour un tel idéal : $\#(A/\mathfrak{b}) = q$. Donc $q \in \mathfrak{b}$. Or ce n'est possible que pour un nombre fini d'idéaux.
2. On applique alors le lemme précédent.

□

Lemme A.4.12. *Soit c l'ordre de C. O_K est principal si et seulement si $c = 1$. Pour tout idéal $\mathfrak{a}$, $\mathfrak{a}^c$ est principal. Si $\mathfrak{a}$ est tel que $\mathfrak{a}^d$ est principal alors, d divise c.*

Démonstration. Immédiat d'après les définitions et les résultats précédents. □

Definition A.4.13. *Le nombre $M_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{D}$ est appelé constante de Minkowski*

A.5 Unités

A.5.1 Théorème des unités

Definition A.5.1. *Le **plongement logarithmique** est l'application* $L : K^* \to \mathbb{R}^{r+s}$ *définie par :*

$$L(\alpha) = (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, \log|\sigma_{r+1}(\alpha)|, \ldots, \log|\sigma_{r+s}(\alpha)|)$$

Dans les démonstrations qui suivent, on utilise les notations suivantes :

1. $H \subset \mathbb{R}^{r+s}$ est l'hyperplan d'équation

$$\sum_{j=1}^{r} x_j + 2\sum_{j=r+1}^{r+s} x_j = 0$$

   Compte tenu cette relation, une forme linéaire sur $H \subset \mathbb{R}^{r+s}$ est définie par $r + s - 1$ nombres : $f(y_1, \ldots y_{r+s}) = e_1 y_1 + \cdots + e_{r+s-1} y_{r+s-1}$.

2. U_K est le groupe des unités de K.
3. $L(U_k)$ est l'image de U_K par le plongement logarithmique L.

Théoreme A.5.2. *U_k est le produit d'un groupe cyclique fini par un groupe abélien d'ordre $r + s - 1$.*

Démonstration. Nous allons prouver les lemmes suivants :

1. La fonction L applique U_K dans H.

2. Son noyau est un groupe cyclique fini.
3. Son image est un sous module de H
4. Si f est une application linéaire non nulle sur W, alors il existe une unité $\nu \in U_K$ telle que $f(L(\nu)) \neq 0$.

Lemme A.5.3.

Le noyau de $L : U_K \to \mathbb{R}^{r+s}$ est constitué des racines de l'unité contenues dans O_K.

Démonstration. Pour tout σ et toute unité V, on a $|\sigma(\nu)| = 1$. Le noyau de $L : U_K \to \mathbb{R}^{r+s}$ est borné, donc il est fini. Donc il est cyclique. □

Lemme A.5.4. $L(U_K) \subset H$.

Démonstration. Soit $\nu \in U_K$. Montrons que $L(\nu) \in H$. On a :

$$\prod_{k=1}^{r} \sigma_k(\nu) \prod_{k=r+1}^{r+s} |\sigma_k(\nu)|^2 \quad = \quad N(\nu) = 1$$

On prend le logarithme

$$\sum_{k=1}^{r} \log|\sigma_k(\nu)| + 2 \sum_{k=r+1}^{r+s} \log|\sigma_k(\nu)| \quad = \quad \log\sqrt{N(\nu)} = \log 1 = 0$$

Donc $L(\nu) = (\log|\sigma_1(\nu)|, \ldots, \log|\sigma_r(\nu)|, \log|\sigma_{r+1}(\nu)|, \ldots, \log|\sigma_{r+s}(\nu)|) \in H$. □

Lemme A.5.5. *$L(U_K)$ est un sous module de $\mathbb{R}^{r+s}$ de rang inférieur ou égal à $r+s-1$.*

Démonstration. $L(U_K) \subset H$ et H est un sous espace vectoriel de $\mathbb{R}^{r+s}$ de dimension $r+s-1$. □

Soit, dans ce qui suit, $A \geq 2^n(2\pi)^{-s}\sqrt{|D|}$.

Lemme A.5.6. *A une suite de nombres positifs $\gamma = (c_1, \ldots, c_r, c_{r+1}, \ldots, c_{r+s-1}) \in \mathbb{R}^{r+s-1}$, on associe c_{r+s} tel que $c_1 \ldots c_r\,(c_{r+1} \ldots c_{r+s})^2 = A$. Alors il existe un entier $\alpha_\lambda \in O_K$ tel que, pour $1 \leq i \leq r+s$, on ait :*

$$0 \leq \log c_i - \log|\sigma_i(\lambda_\lambda)| \leq \log A$$

Démonstration.

1. Soit $S_\lambda \subset \mathbb{R}^{r+2s}$, l'ensemble des vecteurs x tels que :

   $$|x_i| \leq c_i \text{ pour } 1 \leq i \leq r \quad , \quad |x_i|^2 + |x_{i+s}|^2 \leq c_i^2 \text{ pour } r \leq i \leq r+s$$

   On a : $\mu(S_\lambda) = 2^r\pi^s A \geq 2^r\pi^s 2^{r+2s}(2\pi)^{-s}\sqrt{|D|} = 2^n 2^{-s}\sqrt{|D|}$. Rappelons que : $V(C(O_K)) = 2^{-s}\sqrt{|D|}$ d'après A.4.8. Donc $\mu(S_\lambda) > 2^n V(C(O_K))$. L'ensemble S_λ est symétrique par rapport à l'origine, borné et $\mu(S_\lambda) > 2^n V(C(O_K))$. On applique A.6.6 : $\alpha_\lambda \in S_\lambda \bigcap C(O_K)$ n'est pas réduit à 0. Il existe α_λ non nul dans O_K tel que $C(\alpha_\lambda) \in S_\lambda$.

2. α_λ est tel que $1 \leq |N(\alpha_\lambda)| \leq A$; en effet, α_λ est entier et $|N(\alpha_\lambda)| \geq 1$; et pour $i \leq r$, $|\sigma_i(\alpha_\lambda)| \leq c_i$, pour $r+1 \leq i \leq r+s$,

$|\sigma_i(\alpha_\lambda)|^2 \leq c_i^2$. Donc $N(\alpha_\lambda) = \prod_{k=1}^{r} \sigma_k(\alpha_\lambda) \prod_{k=r+1}^{r+s} |\sigma_k(\alpha_\lambda)| \leq A$. D'autre part : pour tout i

$$|\sigma_i(\alpha_\lambda)| \quad = \quad N(\alpha_\lambda) \prod_{j \neq i} \frac{1}{\sigma_i(\alpha_\lambda)} \geq \prod_{j \neq i} \frac{1}{c_j} = \frac{A}{c_i}$$

Donc $c_i/A \leq |\sigma_i(\alpha_\lambda)| \leq c_i$. Et : $0 \leq \log c_i - \log |\sigma_i(\lambda_\lambda)| \leq \log A$.

□

Lemme A.5.7. *Soit f une forme linéaire sur W définie par $f(y_1, \dots y_{r+s}) = e_1 y_1 + \cdots + e_{r+s-1} y_{r+s-1}$, alors on a :*

$$\left| f(L(\alpha_\lambda)) - \sum_{i=1}^{r+s-1} e_i \log c_i \right| \quad \leq \quad \log A \sum_{i=1}^{r+s-1} |e_i|$$

Démonstration. On développe et on utilise le lemme précédent :

$$\begin{aligned} \left| f(L(\alpha_\lambda)) - \sum_{i=1}^{r+s-1} e_i \log c_i \right| &= \left| \sum_{i=1}^{r+s-1} e_i \log |\sigma_i(\alpha_\lambda)| - \sum_{i=1}^{r+s-1} e_i \log c_i \right| \\ &\leq \sum_{i=1}^{r+s-1} |e_i| \left| \log |\sigma_i(\alpha_\lambda)| - e_i \right| \leq \sum_{i=1}^{r+s-1} |e_i| \log A \end{aligned}$$

□

Lemme A.5.8. *Il existe une une unité ν telle que $f(L(nu)) \neq 0$.*

Démonstration. 1. Soit : $B > \log A \sum_{i=1}^{r+s-1} |e_i|$.

2. Soit h entier positif. On lui associe $r + s - 1$ nombres c_i tels que $\sum_i e_i \log c_i = 2Bh$. On considère l'entier associé à ces nombres selon le lemme A.5.6 ; on note α_h cet entier. Il est de norme inférieure à A.
3. On a, d'après le lemme précédent : $|f(L(\alpha_h)) - 2Bh| \leq B$. Donc : $(2h-1)B < f(L(\alpha_h)) < (2h+1)B$. Donc les nombres $f(L(\alpha_h))$ sont tous différents.
4. Les idéaux principaux de O_K de norme $\leq A$ sont en nombre fini. Il existe donc deux nombres différents h et k tels que $(\alpha_h) = (\alpha_k)$. Donc une unité ν telle que $\alpha_h = \nu\alpha_k$. On a alors $f(L(\nu)) = f(L(\alpha_h)) - f(L(\alpha_k)) \neq 0$: il existe une une unité ν telle que $f(L(\nu)) \neq 0$.

□

□

A.6 Réseaux de $\mathbb{R}^n$

Definition A.6.1. *Un **réseau** de $\mathbb{R}^n$ en est un sous groupe additif discret (son intersection avec un sous ensemble borné est un ensemble fini), qui est aussi un sous module libre de rang n. Une **base** E d'un réseau en est une partie libre et génératrice $(e_1, \ldots, e_n)$.*

Definition A.6.2. *Soit $E = (e_1, \ldots, e_n)$ une base d'un réseau réseau. Le **parallélépipède fondamental** est l'ensemble $\{x = \sum_i x_i e_j \mid 0 \leq x_i < 1\}$.*

Definition A.6.3. *Le **volume** d'un réseau R est égal au volume de son parallélépipède fondamental. Il vaut : $V(R) = |\det(E)|$.*

Lemme A.6.4. *Le volume d'un réseau ne dépend pas de la base choisie.*

Démonstration. Si on a une autre base F, il existe une application linéaire de déterminant ± 1 transformant l'une en l'autre. Alors $|\det(E)| = |\det(MF)| = |\det(M)\det(F)| = |\det(F)|$ □

Théoreme A.6.5. *Soient R un réseau de $\mathbb{R}^n$ et B un sous-ensemble mesurable de $\mathbb{R}^n$. Si $\mu(B) > V(R)$, il existe x, y distincts dans B tels que $x - y \in R$.*

Démonstration. Soit E une base. Soit P le parallélépipède correspondant.

1. Comme B est la réunion disjointe des $B \bigcap (h + P)$, $h \in R$, on a : $\mu(B) = \sum_h \mu(B \bigcap (h + P))$.
2. Mais on a : $B \bigcap (h + P) = (-h + B) \bigcap P$
3. Les ensembles $B \bigcap (-h + P)$ ne sont pas sont disjoints : sinon on a aurait $\nu(R) = \mu(P) \geq \sum_h \mu(B \bigcap (-h + P)) \geq \mu(B)$. Ce qui contredit l'hypothèse du lemme.
4. Donc, il existe h et h' tels que $B \bigcap (-h + P) \bigcap (-h' + P) \neq \emptyset$. Il existe $x, y \in B$ tels que $-h + x = -h' + y$. Alors $x - y = h - h' \in R$ et $x \neq y$.

□

Théoreme A.6.6. *Soient R un réseau et B un sous-ensemble mesurable de $\mathbb{R}^n$ convexe et symétrique par rapport à l'origine. Si $\mu(B) > 2^n V(R)$. Alors $B \bigcap R \neq \{0\}$.*

Démonstration. On applique A.6.5 à l'ensemble $(1/2)B$. On a : $\mu((1/2)B) = \mu(B)/2^n$. Il existe $x, y \in (1/2)B$, tels que $x - y \in R$. Alors $x - y \in B \bigcap R$. □

Lemme A.6.7. *Soit H un $\mathbb{R}$-espace vectoriel sur de dimensions n. Soit G un sous groupe discret de H.*

1. *Soit P une partie bornée de H, alors $G \bigcap P$ est fini.*
2. *G est un $\mathbb{Z}$-module de rang $< n$.*
3. *S'il existe $M \subset H$ bornée telle que $M + G = H$, alors G est est un $\mathbb{Z}$-module de rang n.*

Lemme A.6.8. *Soit B une partie compacte de $\mathbb{R}^m$, alors $L^{-1}(B) \bigcap U_k$ est un ensemble fini.*

Démonstration. Soit $\alpha \in L^{-1}(B) \bigcap U_k$. Il existe M tel que $e^{-M} < \log|\sigma_i(\alpha)| < M$ pour $1 \leq i \leq m$. Soit $|\sigma_i(\alpha)| < e^M$. Les $\sigma_i(\alpha)$ sont racines dans $\mathbb{C}$ du polynôme minimal de α. Les coefficients de ce polynôme sont les fonctions symétriques élémentaires des $\sigma_i(\alpha)$; ils sont bornés. Ils sont entiers, le degré de α est inférieur à $l - 1$, il n'y a qu'un nombre fini de polynômes satisfaisant à ces conditions. Il n'y a qu'un nombre fini de valeurs de α possibles. □