Conspectus materiae tomi LIV, fasciculi 2

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires à l'adresse ci-dessus
The authors are requested to submit papers in two copies to the above address
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit an die obige Adresse
Рукописи статей редакция просит предлагать в двух экземплярах на вышеуказанный адрес

ISBN 83-01-09279-3 ISSN 0065-1036

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

Sur la loi de réciprocité des puissances l-èmes

par

GUY TERJANIAN (Toulouse)

1. Introduction. Pour ne pas allonger cet article, certains résultats qualifiés d'énoncés sont donnés sans démonstration. On se donne un nombre premier $l \geqslant 3$ et un entier relatif a et on pose $\zeta = \cos(2\pi/l) + i\sin(2\pi/l)$. Pour m entier $\geqslant 0$, on note α_m le nombre $a^m - \zeta^m$ et pour α et β non nuls de $\boldsymbol{Z}[\zeta]$, on note $[\alpha, \beta]$ l'élément du corps fini $\boldsymbol{F}_l$ qui est l'exposant de ζ du symbole de Hilbert de α et β relatif à l'idéal $(1-\zeta)$. Les paragraphes 2 à 5 ont pour but d'établir diverses formules relatives à des symboles tels que $[\alpha_m, \alpha_n]$. On montre au paragraphe 6, grâce à certaines de ces formules, que, si $l \geqslant 5$, les entiers a tels que $[\alpha_m, \alpha_n] = 0$ pour tous m et n non divisibles par l sont ceux qui sont divisibles par l^2 ou congrus à 1 ou à -1 modulo l.

Les trois derniers paragraphes concernent des propriétés de caractère conjectural sur lesquelles nos résultats sont bien moins complets et leur intérêt est quelque peu spéculatif. Voici de quoi il s'agit. On se donne un entier e non divisible par l et on définit à partir des seules données de l et de e, un système d'équations $S(l, e)$ linéaire et homogène à coefficients dans $\boldsymbol{F}_l$, formé de six familles d'équations. On montre que si a vérifie la congruence $a^{l-1} \equiv 1\ (l^2)$ et si f est l'ordre de a dans le groupe multiplicatif du corps $\boldsymbol{F}_l$, la famille $([\alpha_m, \alpha_n])_{(m,n)\in J(l,f)}$ où $J(l, f)$ est l'ensemble des couples (m, n) tels que $1 \leqslant m \leqslant fl$, $1 \leqslant n \leqslant fl$ et que $l \nmid m\ n$ est une solution de $S(l, f)$. On définit ensuite à partir du système $S(l, e)$ une propriété P du couple (l, e) et une propriété P du nombre premier l. Je sais très peu de choses sur le système $S(l, e)$ et sur les propriétés P ; essentiellement que les couples (l, e) tels que $e \leqslant 6$ possèdent la propriété P.

Nous introduisons ensuite une propriété de l ; on dit que l possède la propriété LC, si les entiers a tels qu'on ait $[\alpha_1, \omega] = 0$ pour toute unité cyclotomique ω sont les entiers congrus à 0, 1 ou -1 modulo l^2. On montre que tout nombre premier $l \geqslant 5$ qui possède la propriété P possède la propriété LC et on donne quelques énoncés qui, j'espère, convaincront le lecteur qu'il est raisonnable de conjecturer que tout nombre premier $\geqslant 5$ possède la propriété LC. On montre ensuite que, si $l \geqslant 5$ possède la propriété LC, le premier cas du théorème de Fermat relatif à l'équation $x^l + y^l + z^l = 0$ ne peut se présenter; enfin, on donne sous forme d'énoncé des résultats nouveaux sur le premier cas du théorème de Fermat.

La mise au point de cet article doit beaucoup aux rapporteurs et à Paulo Ribenboim que je tiens à remercier.

2. Les polynômes $A_m, \ldots, D_m$. Si a, b (resp. a, b, c) sont des entiers relatifs dont l'un est non nul, on note (a, b) (resp. (a, b, c)) leur p.g.c.d. On note μ la fonction de Möbius. Pour un entier $m \geqslant 1$, nous noterons $\varphi(m)$ l'indicateur d'Euler de m et $\varphi_1(m)$ la somme des entiers de l'intervalle $[1, m]$ qui sont premiers à m. Si p est un nombre premier, nous noterons v_p la valuation du corps $\boldsymbol{Q}$ des nombres rationnels pour laquelle on a $v_p(p) = 1$ et $v_p(0) = +\infty$.

DÉFINITION. (i) Soit $m \geqslant 0$ un entier, nous noterons A_m et B_m les éléments de l'anneau $\boldsymbol{Z}[X, Y]$ tels que $A_m = X^m - Y^m$ et que $A_m = A_1 B_m$ et a_m et b_m les éléments de $\boldsymbol{Z}[X]$ tels que $a_m = A_m(X, 1)$ et que $b_m = B_m(X, 1)$.

(ii) Soit $m \geqslant 1$ un entier, nous noterons C_m le polynôme cyclotomique d'indice m, c'est-à-dire l'élément de $\boldsymbol{Z}[X, Y]$ tel que

$$C_m = \prod_{\substack{1 \leqslant k \leqslant m \\ (k,m)=1}} (X - e^{2ki\pi/m} Y)$$

et c_m l'élément de $\boldsymbol{Z}[X]$ tel que $c_m = C_m(X, 1)$.

Je laisse au lecteur la démonstration des propositions qui suivent.

PROPOSITION 1. *On a $\varphi_1(1) = 1$ et si m est un entier $\geqslant 2$, on a $\varphi_1(m) = \frac{1}{2} m \varphi(m)$.*

PROPOSITION 2. *Soient m, n, a, b des entiers $\geqslant 0$.*

(i) $A_m = \sum_{i=1}^{m} \binom{m}{i} (X-Y)^i Y^{m-i}$, $\quad B_m = \sum_{i=0}^{m-1} \binom{m}{i+1} (X-Y)^i Y^{m-1-i}$.

(ii) $A_{m+n} = X^n A_m + Y^m A_n$, $\quad B_{m+n} = X^n B_m + Y^m B_n$.

(iii) *Si $m \equiv n(a)$, on a*

$$A_m \equiv X^{m-n} A_n \equiv Y^{m-n} A_n \ (A_a), \qquad B_m \equiv X^{m-n} B_n \equiv Y^{m-n} B_n \ (B_a).$$

(iv) *Si $m \equiv -n(b)$, on a*

$$X^n A_m \equiv -Y^m A_n \ (A_b), \qquad X^n B_m \equiv -Y^m B_n \ (B_b).$$

PROPOSITION 3. *Soient p un nombre premier et $n \geqslant 0$ un entier, on a*

$$A_{p^n} \equiv A_1^{p^n} \ (p), \qquad B_{p^n} \equiv A_1^{p^n - 1} \ (p).$$

PROPOSITION 4. *Soient $m \geqslant 0$ et $n \geqslant 0$ des entiers dont l'un est non nul.*

(i) *Les polynômes $X^{m+n-1} A_{(m,n)}$ et $Y^{m+n-1} A_{(m,n)}$ appartiennent à l'idéal de $\boldsymbol{Z}[X, Y]$ engendré par A_m et A_n.*

(ii) *Les polynômes $X^{m+n-1} B_{(m,n)}$ et $Y^{m+n-1} B_{(m,n)}$ appartiennent à l'idéal de $\boldsymbol{Z}[X, Y]$ engendré par B_m et B_n.*

Démonstration. (i) Montrons par récurrence sur $m+n$ que $X^{m+n-1} A_{(m,n)}$ appartient à l'idéal engendré par A_m et A_n. Si $m+n = 1$, c'est clair. Soient m et n des entiers tels que $m+n \geqslant 2$ et que la propriété soit vérifiée par tous les couples d'entiers de somme $< m+n$ et montrons que le couple (m, n) possède la propriété. On peut supposer $m \geqslant n$.

Si $n = 0$, c'est clair et l'on peut donc supposer $n \geqslant 1$. Posons $d = (m, n)$, on a $d = (m-n, n)$ et, puisque $(m-n)+n < m+n$, il y a des éléments a et b de $\boldsymbol{Z}[X, Y]$ tels qu'on ait $X^{m-1} A_d = a A_{m-n} + b A_n$.

Vu la proposition 2, on a

$$X^{m+n-1} A_d = a X^n A_{m-n} + b X^n A_n = a(A_m - Y^{m-n} A_n) + b X^n A_n$$

et le couple (m, n) possède la propriété.

Echangeant X et Y, on voit que $Y^{m+n-1} A_{(m,n)}$ appartient aussi à l'idéal engendré par A_m et A_n ; enfin, (ii) résulte de (i).

Dressons une liste de propriétés de C_m dans laquelle m désigne un entier $\geqslant 1$.

(C1) $C_1 = A_1 = X - Y$.

(C2) Si m est premier, on a

$$C_m = B_m = \sum_{i=0}^{m-1} X^{m-1-i} Y^i.$$

(C3) $A_m = \prod_{d|m} C_d$.

(C4) $B_m = \prod_{\substack{d|m \\ d \geqslant 2}} C_d$.

(C5) Si n est un entier $\geqslant 1$ et si n' est le plus grand diviseur de n dont tous les facteurs premiers divisent m, on a

$$C_m(X^n, Y^n) = \prod_{mn' | q | mn} C_q.$$

(C6) Si $n \geqslant 1$ est un entier dont tout facteur premier divise m, on a

$$C_{mn} = C_m(X^n, Y^n).$$

(C7) Si $n \geqslant 1$ est un entier tel que $(m, n) = 1$, on a

$$C_m(X^n, Y^n) = \prod_{m | q | mn} C_q.$$

(C8) Si p est un nombre premier et n un entier $\geqslant 1$, on a les relations

$$C_{p^n} = C_p(X^{p^{n-1}}, Y^{p^{n-1}}), \qquad C_{p^n} \equiv C_1^{\varphi(p^n)} \ (p).$$

(C9) C_m est non nul, homogène, de degré $\varphi(m)$, irréductible dans $\boldsymbol{Z}[X, Y]$ et a 1 pour coefficient de $X^{\varphi(m)}$ et $-\mu(m)$ pour coefficient de $X^{\varphi(m)-1}Y$.

(C10) Si $m \geqslant 2$, $C_m = C_m(Y, X)$.

Les propriétés (C1) à (C4) sont bien connues ; (C5) à (C7) sont dues à Netto [13] ; (C8) résulte de (C6) et de la proposition 3 ; enfin, pour (C9) et (C10), on peut consulter les articles de Möller [10], [11].

PROPOSITION 5. *Soient $m \geqslant 1$ et $n \geqslant 1$ des entiers ; dans l'anneau $\boldsymbol{Z}[X, Y]$, on a:*

(i) *$X^{m+n-1}A_{(m,n)}$ et $Y^{m+n-1}A_{(m,n)}$ appartiennent aux idéaux (A_m, C_n), (A_n, C_m) et (C_m, C_n).*

(ii) *Si $m \geqslant 2$, $X^{m+n-1}B_{(m,n)}$ et $Y^{m+n-1}B_{(m,n)}$ appartiennent à l'idéal (B_n, C_m).*

(iii) *Si $m < n$ et si $m \nmid n$, X^{m+n-1} et Y^{m+n-1} appartiennent à l'idéal (C_m, C_n).*

Démonstration. (i) et (ii) résultent de la proposition 4.

(iii) Supposons $m < n$ et $m \nmid n$ et posons $d = (m, n)$; on a $1 \leqslant d < m < n$. En vertu de la proposition 4, $X^{m+n-1}B_d$ et $Y^{m+n-1}B_d$ appartiennent à l'idéal (B_m, B_n) et vu la propriété (C4), B_m est un multiple de B_dC_m et B_n est un multiple de B_dC_n ; par suite, $X^{m+n-1}B_d$ et $Y^{m+n-1}B_d$ appartiennent à l'idéal (B_dC_m, B_dC_n) ; d'où le résultat.

PROPOSITION 6. *Soient $m \geqslant 3$ un entier et x et y des nombres réels.*

(i) $$C_m = \prod_{\substack{1 \leqslant k < m/2 \\ (k,m)=1}} \left(X^2 - 2\cos\frac{2k\pi}{m} XY + Y^2\right).$$

(ii) *Si $xy > 0$, on a*

$$(x-y)^{\varphi(m)} < C_m(x, y) < (x+y)^{\varphi(m)}.$$

(iii) *Si $xy < 0$, on a*

$$(x+y)^{\varphi(m)} < C_m(x, y) < (x-y)^{\varphi(m)}.$$

(iv) *Si $(x, y) \neq (0, 0)$, $C_m(x, y) > 0$.*

(v) *Si x et y sont des entiers relatifs tels que $C_m(x, y) = 1$, on a $|x| \leqslant 1$ et $|y| \leqslant 1$.*

Démonstration. (i) résulte de la définition de C_m et les autres points s'en déduisent.

PROPOSITION 7. *Soit $m \geqslant 1$ un entier.*

(i) *$c_1(0) = -1$ et si $m \geqslant 2$, $c_m(0) = 1$.*

(ii) *$c_1(1) = 0$; si $m \geqslant 2$ est une puissance d'un nombre premier p, $c_m(1) = p$; pour toute autre valeur de m, $c_m(1) = 1$.*

Cela se déduit facilement de (C1) à (C10).

PROPOSITION 8. *Soit $m \geqslant 1$ un entier ; dans l'anneau $\boldsymbol{Z}[V, W, X, Y]$, on a les congruences*

$$\prod_{\substack{i=1 \\ (i,m)=1}}^{m} (VX^i - WY^i) \equiv X^{\varphi_1(m)} C_m(V, W),$$

$$\prod_{\substack{i=1 \\ (i,m)=1}}^{m} (VX^i - WY^i) \equiv (-1)^{\delta_{2m}} Y^{\varphi_1(m)} C_m(V, W),$$

$$\prod_{i=1}^{m-1} (VX^i - WY^i) \equiv X^{m(m-1)/2} B_m(V, W),$$

$$\prod_{i=1}^{m-1} (VX^i - WY^i) \equiv (-1)^{m-1} Y^{m(m-1)/2} B_m(V, W),$$

$$\prod_{i=0}^{m-1} (VX^i - WY^i) \equiv X^{m(m-1)/2} A_m(V, W),$$

$$\prod_{i=0}^{m-1} (VX^i - WY^i) \equiv (-1)^{m-1} Y^{m(m-1)/2} A_m(V, W)$$

suivant le module C_m, δ_{2m} étant l'indice de Kronecker des nombres 2 et m.

Démonstration. Soient ζ une racine primitive m-ème de 1 et k un entier tel que $1 \leqslant k \leqslant m$ et que $(k, m) = 1$ et posons

$$P = \prod_{\substack{i=1 \\ (i,m)=1}}^{m} (VX^i - WY^i).$$

Dans l'anneau $\boldsymbol{C}[V, W, X, Y]$, on a

$$P \equiv \prod_{\substack{i=1 \\ (i,m)=1}}^{m} (VX^i - WX^i\zeta^{-ki})\ (X - Y\zeta^k).$$

D'où

$$P \equiv X^{\varphi_1(m)} C_m(V, W)\ (X - Y\zeta^k).$$

Cette congruence a lieu aussi suivant le produit des $X - Y\zeta^k$, k parcourant l'ensemble des entiers de l'intervalle $[1, m]$ premiers à m, produit qui est C_m ; d'où la première congruence de l'énoncé. La seconde s'en déduit à l'aide de la proposition 1. La troisième se démontre comme la première et les trois dernières s'en déduisent.

DÉFINITION. Soit $m \geqslant 3$ un entier, nous noterons D_m l'élément de $\boldsymbol{Z}[X, Y]$ tel que

$$C_m - C_1^{\varphi(m)} = c_m(1) XY D_m$$

et d_m l'élément de $\boldsymbol{Z}[X]$ tel que $d_m = D_m(X, 1)$.

Le polynôme $C_m - C_1^{\varphi(m)}$ est divisible par $c_m(1)$ pour tout entier $m \geqslant 1$ en vertu de la proposition 7 et de la propriété (C8), ce qui justifie la définition ci-dessus.

PROPOSITION 9. *Soit $m \geqslant 3$ un entier.*

(i) $D_m = D_m(Y, X)$.

(ii) $D_m(1, 1) = 1$.

(iii) $D_m(1, 0) = (\varphi(m) - \mu(m))/c_m(1)$.

(iv) *D_m est non nul, homogène et de degré $\varphi(m) - 2$.*

(v) *Si x et y sont des réels tels que $(x, y) \neq (0, 0)$, on a $D_m(x, y) > 0$.*

(vi) *Dans l'anneau $\boldsymbol{Z}[X, Y]$, on a*

$$XD_m \prod_{\substack{i=1 \\ (i,m)=1}}^{m} B_i \equiv -Y^{\varphi_1(m)-1} \ (C_m),$$

$$YD_m \prod_{\substack{i=1 \\ (i,m)=1}}^{m} B_i \equiv -X^{\varphi_1(m)-1} \ (C_m).$$

Démonstration. (i) résulte de C(10) ; (ii) résulte du fait que $c_m(1) > 0$; (iii) résulte de (C9) ; (iv) résulte de (ii) ; (v) résulte de la proposition 6.

(vi) En vertu de la proposition 8, on a

$$\prod_{\substack{i=1 \\ (i,m)=1}}^{m} (X^i - Y^i) \equiv X^{\varphi_1(m)} C_m(1, 1) \ (C_m).$$

D'où

$$C_1^{\varphi(m)} \prod_{\substack{i=1 \\ (i,m)=1}}^{m} B_i \equiv c_m(1) X^{\varphi_1(m)} \ (C_m),$$

$$-c_m(1) XYD_m \prod_{\substack{i=1 \\ (i,m)=1}}^{m} B_i \equiv c_m(1) X^{\varphi_1(m)} \ (C_m).$$

Comme on a $c_m(1) \geqslant 1$ et comme le terme en $Y^{\varphi(m)}$ de C_m est $Y^{\varphi(m)}$, on en déduit

$$-YD_m \prod_{\substack{i=1 \\ (i,m)=1}}^{m} B_i \equiv X^{\varphi_1(m)-1} \ (C_m).$$

D'où la première congruence ; la seconde s'en déduit en y échangeant X et Y.

ENONCÉ 1. *Soient $m \geqslant 3$ un entier et $e(m)$ l'entier 0 si $m = 3$ ou si $m = 2p^n$ avec p premier, $p \equiv 2$ (3) et $n \geqslant 0$ ou si $m = 6q^n$ avec q premier et $n \geqslant 0$, l'entier 2 si m est du type a ou $2^k a$ où $a > 1$ est un entier dont tous les facteurs premiers sont congrus à 1 modulo 6 et où k est un entier impair $\geqslant 3$ et l'entier 1 pour les autres valeurs de m.*

(i) *Il y a un élément E_m de $\boldsymbol{Z}[X, Y]$ tel que*

$$D_m = C_6^{e(m)} E_m.$$

(ii) *Pour tout nombre premier $p \geqslant 3$, E_m n'est divisible ni par C_p ni par C_{2p}.*

Notre démonstration de cet énoncé est très longue, en particulier en ce qui concerne la divisibilité de D_m par C_6 et c'est pourquoi je l'ai supprimée ; on peut se demander s'il existe des entiers $m \geqslant 3$ et $n \geqslant 1$ tels que E_m soit divisible par C_n et aussi si E_m est irréductible pour tout entier $m \geqslant 8$; on montre facilement que si E_m est irréducible, il n'est divisible par aucun C_n ; ces polynômes D_m et E_m ont déjà été étudiés dans le cas où m est un nombre premier par Mirimanoff [8] et Klösgen [5] ; Mirimanoff a conjecturé que pour tout nombre premier $p \geqslant 11$, E_p est irréductible, ce que Klösgen a vérifié pour $p \leqslant 31$. Mon collègue Jean-Louis Nicolas et son élève François Morain ont vérifié l'irréductibilité de E_m pour les entiers m tels que $8 \leqslant m \leqslant 264$.

3. La loi de réciprocité. Dans la suite de cet article, nous nommerons Hasse pour renvoyer à son traité [4] sur les lois de réciprocité et ferons usage des notations suivantes :

l est un nombre premier $\geqslant 3$,

si x est entier relatif non divisible par l, $q(x)$ est l'entier $(x^{l-1} - 1)/l$,

$\zeta = \cos(2\pi/l) + i \sin(2\pi/l)$,

$\lambda = 1 - \zeta$,

$\varepsilon = -\lambda^{l-1}/l$,

$\eta_i = 1 - \lambda^i$ pour i entier $\geqslant 1$,

$K = \boldsymbol{Q}(\zeta)$ est le corps engendré sur $\boldsymbol{Q}$ par ζ,

N est la norme de K par rapport à $\boldsymbol{Q}$,

G est le groupe de Galois de K sur $\boldsymbol{Q}$,

si n est un entier relatif non divisible par l, s_n est l'élément de G tel que $s_n(\zeta) = \zeta^n$,

A est l'anneau des entiers de K,

U est le groupe des unités de K,

C est le sous-groupe de U engendré par les unités cyclotomiques, i.e. les $b_n(\zeta)$ pour $n = 1, \ldots, l-1$,

Λ est le sous-monoïde du monoïde $A - \{0\}$ muni de la multiplication engendré par λ et C,

ΛU est le sous-monoïde du même $A - \{0\}$ engendré par Λ et U,

$\hat{K}$ est le complété λ-adique de K,

v_λ est la valuation de $\hat{K}$ telle que $v_\lambda(\lambda) = 1$ et que $v_\lambda(0) = +\infty$,

log est le logarithme λ-adique de $\hat{K}$ défini sur le groupe des éléments x de $\hat{K}$ tels que $v_\lambda(x) = 0$,

si α et β sont des éléments de $\hat{K}$ et si v est un entier relatif ou $+\infty$, on convient d'écrire $\alpha \equiv \beta\ (\lambda^v)$ lorsque $v_\lambda(\alpha-\beta) \geqslant v$,

si n est un entier tel que $1 \leqslant n \leqslant l-1$, on note l_n l'unique homomorphisme du groupe multiplicatif des éléments x de K tels que $v_\lambda(x) = 0$ dans le groupe additif $\boldsymbol{F}_l$ qui prolonge l'homomorphisme l_n que Hasse a défini à la page 109 sur le groupe des y de K tels que $v_\lambda(y-1) > 0$; cet homomorphisme l_n a déjà été introduit et étudié par Herbrand et Dénes,

si α et β sont des éléments ou des idéaux de A, on note (α, β) l'idéal de A qu'ils engendrent,

si α est un élément non nul de K, on note α_λ le nombre $\lambda^{-v_\lambda(\alpha)}\alpha$,

si $\mathfrak{a}$ est un idéal non nul de K, entier ou fractionnaire, on note $\mathfrak{a}_\lambda$ l'idéal $(\lambda)^{-a}\mathfrak{a}$ où a est l'exposant de (λ) dans la décomposition de $\mathfrak{a}$ en idéaux premiers,

enfin, si $i \geqslant 1$ est un entier et si x est un rationnel tel que $v_l(x) \geqslant 0$, on convient de noter η_i^x le nombre η_i^y où y est l'entier rationnel de l'intervalle $[0, l-1]$ tel que $v_l(x-y) \geqslant 1$.

Nous rassemblerons ci-dessous tout ce qui se rapporte à la loi de réciprocité; dans les définitions et les formules qui suivent, les lettres α, β, γ, α', β', γ' désignent des éléments de A, les lettres $a, a_0, a_1, b, b_0, b_1, \ldots, d, d_0, d_1$ désignent des entiers relatifs et les lettres $\mathfrak{a}$ et $\mathfrak{b}$ désignent des idéaux de A.

(R1) Nous dirons qu'un élément α de A est primaire si on a $\alpha^{l-1} \equiv 1\ (\lambda^l)$ et hyperprimaire si on a $\alpha^{l-1} \equiv 1\ (\lambda^{l+1})$.

(R2) Nous dirons qu'un élément de A est primaire au sens large (resp. hyperprimaire au sens large) s'il est le produit d'un élément primaire (resp. hyperprimaire) de A par une puissance de λ dont l'exposant est un multiple de l.

(R3) Les entiers relatifs a qui sont primaires (resp. hyperprimaires) sont ceux pour lesquels on a $a^{l-1} \equiv 1\ (l^2)$.

(R4) Si α et β sont des éléments non nuls de A, nous noterons (α, β) le symbole de Hilbert de α et β relatif à l'idéal (λ), symbole que Hasse note $\left(\frac{\alpha, \beta}{(\lambda)}\right)$.

(R5) Si $\alpha\beta \neq 0$, nous noterons $[\alpha, \beta]$ l'élément x du corps $\boldsymbol{F}_l$ tel que $(\alpha, \beta) = \zeta^x$.

(R6) Si $\alpha\beta \neq 0$, nous dirons que α et β sont orthogonaux si on a $(\alpha, \beta) = 1$.

(R7) Soient α un élément non nul de A et $\mathfrak{a}$ un idéal non nul de A tels que α et $\mathfrak{a}_\lambda$ soient premiers entre eux, nous appellerons symbole de reste de puissance l-ème de α par rapport à $\mathfrak{a}$ et nous noterons $\left(\frac{\alpha}{\mathfrak{a}}\right)$ ce que Hasse note $\left(\frac{\alpha}{\mathfrak{a}_\lambda}\right)$.

(R8) Si $\alpha \neq 0$, pour qu'on ait $(\alpha, \beta) = 1$ pour tout β de A tel que $\lambda \nmid \beta$, il faut et il suffit que α soit primaire au sens large.

(R9) Si $\alpha \neq 0$, pour qu'on ait $(\alpha, \beta) = 1$ pour tout β non nul de A, il faut et il suffit que α soit hyperprimaire au sens large.

(R10) Si $\lambda \nmid \alpha\alpha'\beta\beta'$, $\alpha \equiv \alpha'\ (\lambda^l)$, $\beta \equiv \beta'\ (\lambda^l)$, on a $(\alpha, \beta) = (\alpha', \beta')$.

(R11) Si $\lambda \nmid \alpha\alpha'$, $\alpha \equiv \alpha'\ (\lambda^{l+1})$, $\beta\beta' \neq 0$, $b = v_\lambda(\beta) = v_\lambda(\beta')$, $\beta \equiv \beta'\ (\lambda^{l+b})$, on a $(\alpha, \beta) = (\alpha', \beta')$.

(R12) Si $\alpha\alpha' \neq 0$, $a = v_\lambda(\alpha) = v_\lambda(\alpha')$, $\alpha \equiv \alpha'\ (\lambda^{l+a})$, $\lambda \nmid \beta\beta'$, $\beta \equiv \beta'\ (\lambda^{l+1})$, on a $(\alpha, \beta) = (\alpha', \beta')$.

(R13) Si $\alpha\alpha'\beta\beta' \neq 0$, $a = v_\lambda(\alpha) = v_\lambda(\alpha')$, $b = v_\lambda(\beta) = v_\lambda(\beta')$, $\alpha \equiv \alpha'\ (\lambda^{l+a+1})$, $\beta \equiv \beta'\ (\lambda^{l+b+1})$, on a $(\alpha, \beta) = (\alpha', \beta')$.

(R14) Si $\alpha\beta\gamma \neq 0$, $(\alpha\beta, \gamma) = (\alpha, \gamma)(\beta, \gamma)$ et $(\alpha, \beta\gamma) = (\alpha, \beta)(\alpha, \gamma)$.

(R15) Si $\alpha\beta \neq 0$, $(\beta, \alpha) = (\alpha, \beta)^{-1}$.

(R16) Si $\alpha \neq 0$, $(\alpha, \alpha) = 1$.

(R17) Si $\alpha\beta(\alpha+\beta) \neq 0$, on a $(\alpha, \beta) = (\alpha, \alpha+\beta)(\alpha+\beta, \beta)$.

(R18) Si $\alpha\beta(\alpha-\beta) \neq 0$, on a $(\alpha, \beta) = (\alpha, \alpha-\beta)(\alpha-\beta, \beta)$.

(R19) Si $\alpha\beta \neq 0$ et si $s \in G$, on a $(s(\alpha), s(\beta)) = s((\alpha, \beta))$.

(R20) Si k est un sous-corps de K distinct de K et si α et β sont des éléments non nuls de $A \cap k$, on a $(\alpha, \beta) = 1$.

(R21) Si $\lambda \nmid \alpha\beta$, $[\alpha, \beta] = \sum_{n=1}^{l-1} l_n(\alpha) l_{l-n}(\beta)$.

(R22) Si $\lambda \nmid \alpha\beta$, $\alpha \equiv a\ (\lambda^l)$, $\beta \equiv b_0 + b_1\lambda\ (\lambda^2)$, $[\alpha, \beta] = -q(a)\frac{b_1}{b_0}$.

(R23) Si $\lambda \nmid \alpha\beta$, $\alpha \equiv a_0 + a_1\lambda\ (\lambda^2)$, $\beta \equiv b\ (\lambda^l)$, $[\alpha, \beta] = q(b)\frac{a_1}{a_0}$.

(R24) Si $a \geqslant 1$, $b \geqslant 1$, on a $[\eta_a, \eta_b] = \sum_{\substack{c \geqslant 1, d \geqslant 1 \\ ca+db=l}} c_0 a + d_0 b$ où c_0 et d_0 vérifient $dc_0 - cd_0 = 1$.

(R25) Si $1 \leqslant a \leqslant l-1$, $[\eta_a, \eta_{l-a}] = a$.

(R26) Si $a \geqslant 0$, $b \geqslant 0$, $a+b \geqslant l+1$, $\alpha\beta \neq 0$, $\alpha \equiv 1\ (\lambda^a)$, $\beta \equiv 1\ (\lambda^b)$, on a $(\alpha, \beta) = 1$.

(R27) Si $a \geqslant 2$, $b \geqslant 2$, $a+b \geqslant l+1$, $\lambda \nmid \alpha\beta$, $\alpha \equiv a_0\ (\lambda^a)$, $\beta \equiv b_0\ (\lambda^b)$, on a $(\alpha, \beta) = 1$.

(R28) Si $\alpha \neq 0$, $[\alpha, \zeta] = (N(\alpha_\lambda) - 1)/l$.

(R29) Si $l \nmid a$, $[a, \lambda] = q(a)/2$.

(R30) Si $a \geqslant 1$, $a \neq l$, $(\eta_a, \lambda) = 1$.

(R31) $(\eta_l, \lambda) = \zeta$.

(R32) Si α et α' appartiennent à AU, $(\alpha, \alpha') = 1$.

(R33) Si $\alpha \neq 0$, $\mathfrak{a}\mathfrak{b} \neq (0)$, $(\alpha, \mathfrak{a}_\lambda \mathfrak{b}_\lambda) = (1)$, $\left(\frac{\alpha}{\mathfrak{a}\mathfrak{b}}\right) = \left(\frac{\alpha}{\mathfrak{a}}\right)\left(\frac{\alpha}{\mathfrak{b}}\right)$.

(R34) Si $\alpha\beta \neq 0$, $\mathfrak{a} \neq (0)$, $(\alpha\beta, \mathfrak{a}_\lambda) = (1)$, $\left(\frac{\alpha\beta}{\mathfrak{a}}\right) = \left(\frac{\alpha}{\mathfrak{a}}\right)\left(\frac{\beta}{\mathfrak{a}}\right)$.

(R35) Si $\alpha \neq 0$, $\mathfrak{a} \neq (0)$, $(\alpha, \mathfrak{a}_\lambda) = (1)$, $\alpha+\beta \neq 0$, $\mathfrak{a}_\lambda | \beta$, on a $\left(\frac{\alpha+\beta}{\mathfrak{a}}\right) = \left(\frac{\alpha}{\mathfrak{a}}\right)$.

(R36) Si $\alpha \neq 0$, $\mathfrak{a} \neq (0)$, $(\alpha, \mathfrak{a}_\lambda) = (1)$, $s \in G$, $\left(\frac{s(\alpha)}{s(\mathfrak{a})}\right) = s\left(\left(\frac{\alpha}{\mathfrak{a}}\right)\right)$.

(R37) Si k est un sous-corps de K distinct de K, α un élément non nul de $A \cap k$ et $\mathfrak{a}$ un idéal non nul de A tel que $(\alpha, \mathfrak{a}_\lambda) = (1)$ et que $\mathfrak{a}_\lambda$ soit engendré par des éléments de $A \cap k$, on a $\left(\frac{\alpha}{\mathfrak{a}}\right) = 1$.

(R38) Si $\alpha \in U$ et si β est primaire au sens large, on a $\left(\frac{\alpha}{\beta}\right) = 1$.

(R39) Si $\alpha \in \Lambda U$ et si β est hyperprimaire au sens large, on a $\left(\frac{\alpha}{\beta}\right) = 1$.

(R40) Si $\alpha\beta \neq 0$, $(\alpha_\lambda, \beta_\lambda) = (1)$, on a $(\alpha, \beta) = \left(\frac{\beta}{\alpha}\right)\left(\frac{\alpha}{\beta}\right)^{-1}$.

(R41) Si $\alpha \in \Lambda U$, $\beta \neq 0$, on a $\left(\frac{\alpha}{\beta}\right) = (\beta, \alpha)$.

Remarquons que nos définitions (R1) à (R7) sont plus proches des définitions classiques de Hilbert et Furtwängler que de celles de Hasse et que la définition (R7) du symbole de reste est une généralisation de la définition classique tout à fait différente de la généralisation que Hasse a introduite dans son traité ; quant aux propriétés et formules (R8) à (R41), elles figurent dans le traité de Hasse ou se déduisent facilement de ce qu'on y trouve ; démontrons cependant (R29) qui semble moins bien connu : si $l \nmid a$, on a, vu (R19), $[a, 1-\zeta^2] = 2[a, 1-\zeta]$; d'où, vu (R22),

$$[a, \lambda] = [a, 1+\zeta] = [a, 2-\lambda] = -q(a)\frac{-1}{2} = \frac{q(a)}{2},$$

ce qui démontre (R29) ; dans la suite, nous utiliserons souvent (R1) à (R41) sans référence.

PROPOSITION 10. *Soit $m \geqslant 0$ un entier.*
(i) $b_m(\zeta) = m\eta_1^{(m-1)/2}$ (λ^2).
(ii) *Si $l \geqslant 5$, on a*

$$b_m(\zeta) = m\eta_1^{(m-1)/2}\eta_2^{(1-m^2)/24} \ (\lambda^3).$$

Démonstration. (i) Vu la proposition 2, on a

$$b_m(\zeta) = \sum_{i=0}^{m-1} (-1)^i \binom{m}{i+1} \lambda^i = \sum_{i \geqslant 0} (-1)^i \binom{m}{i+1} \lambda^i.$$

D'où

$$b_m(\zeta) \equiv m - \binom{m}{2}\lambda + \binom{m}{3}\lambda^2 \ (\lambda^3).$$

On a

$$m\eta_1^{(m-1)/2} \equiv m\left(1 - \frac{(m-1)}{2}\lambda\right) \ (\lambda^2) \equiv m - \binom{m}{2}\lambda \ (\lambda^2).$$

D'où le résultat.

(ii) Si $l \geqslant 5$, on a

$$\eta_1^{(m-1)/2} \equiv 1 - \frac{(m-1)}{2}\lambda + \frac{1}{8}(m^2-4m+3)\lambda^2 \ (\lambda^3),$$

$$\eta_2^{(1-m^2)/24} \equiv 1 + \frac{(m^2-1)}{24}\lambda^2 \ (\lambda^3).$$

D'où

$$\eta_1^{(m-1)/2}\eta_2^{(1-m^2)/24} \equiv 1 - \frac{(m-1)}{2}\lambda + \frac{(m^2-3m+2)}{6}\lambda^2 \ (\lambda^3).$$

D'où le résultat.

PROPOSITION 11. *Soit $m \geqslant 0$ un entier, on a*

$$1 + \zeta^m \equiv 2\eta_1^{m/2}\eta_2^{-m^2/8} \ (\lambda^3).$$

Démonstration.

$$1 + \zeta^m = 1 + (1-\lambda)^m = 1 + \sum_{i=0}^{m} (-1)^i \binom{m}{i} \lambda^i = 2 + \sum_{i \geqslant 1} (-1)^i \binom{m}{i} \lambda^i.$$

D'où

$$1 + \zeta^m \equiv 2 - m\lambda + \frac{(m^2-m)}{2}\lambda^2 \ (\lambda^3).$$

On a aussi

$$\eta_1^{m/2} \equiv 1 - \frac{m}{2}\lambda + \frac{1}{8}(m^2-2m)\lambda^2 \ (\lambda^3),$$

$$\eta_1^{m/2}\eta_2^{-m^2/8} \equiv 1 - \frac{m}{2}\lambda + \frac{1}{4}(m^2-m)\lambda^2 \ (\lambda^3).$$

D'où le résultat.

PROPOSITION 12. (i) ε *appartient à* C.
(ii) $\varepsilon \equiv \eta_1^{-1/2}\ (\lambda^2)$.
(iii) *Si* $l \geqslant 5$, *on a*

$$\varepsilon \equiv \eta_1^{-1/2}\eta_2^{1/24}\ (\lambda^3).$$

Démonstration. (i) On a

$$l = b_l(1) = \prod_{i=1}^{l-1}(1-\zeta^i) = \lambda^{l-1}\prod_{i=1}^{l-1} b_i(\zeta).$$

D'où

$$1 = -\varepsilon\prod_{i=1}^{l-1} b_i(\zeta).$$

D'où le résultat.
(ii) et (iii). On a

$$\sum_{i=1}^{+\infty}\frac{\lambda^i}{i} = \log(1-\lambda) = \log(\zeta) = 0.$$

Pour $i \geqslant l+1$, on a $v_\lambda\left(\frac{\lambda^i}{i}\right) \geqslant l+1$; d'où

$$\sum_{i=1}^{l}\frac{\lambda^i}{i} \equiv 0\ (\lambda^{l+1}),$$

$$\sum_{i=1}^{l-1}\frac{\lambda^i}{i} - \lambda\varepsilon \equiv 0\ (\lambda^{l+1}),$$

$$\varepsilon \equiv \sum_{i=1}^{l-1}\frac{\lambda^{i-1}}{i}\ (\lambda^l).$$

On a donc

$$\varepsilon \equiv 1+\lambda/2 \equiv \eta_1^{-1/2}\ (\lambda^2)$$

et, pour $l \geqslant 5$, on vérifiera qu'on a

$$\varepsilon \equiv 1+\lambda/2+\lambda^2/3 \equiv \eta_1^{-1/2}\eta_2^{1/24}\ (\lambda^3).$$

PROPOSITION 13. *Soient* $m \geqslant 0$ *un entier et* $n \geqslant 1$ *un entier non divisible par* l.
(i) $[\eta_l, \varepsilon] = 0$,
$[\eta_l, 1+\zeta^m] = 0$,
$[\eta_l, 1-\zeta^n] = 1$.
(ii) $[\eta_{l-1}, \varepsilon] = 1/2$,
$[\eta_{l-1}, 1+\zeta^m] = -m/2$,
$[\eta_{l-1}, 1-\zeta^n] = (1-n)/2$.

(iii) *Si* $l \geqslant 5$, *on a*
$[\eta_{l-2}, \eta_1] = -1$,
$[\eta_{l-2}, \varepsilon] = 5/12$,
$[\eta_{l-2}, 1+\zeta^m] = (m^2-2m)/4$,
$[\eta_{l-2}, 1-\zeta^n] = (n^2-6n+5)/12$.

Démonstration.
(i) $[\eta_l, \varepsilon] = [1, \varepsilon] = 0$,
$[\eta_l, 1+\zeta^m] = [1, 1+\zeta^m] = 0$,
$[\eta_l, 1-\zeta^n] = [\eta_l, \lambda b_n(\zeta)] = [\eta_l, \lambda]+[\eta_l, b_n(\zeta)] = 1+0 = 1$.
(ii) Vu les propositions précédentes, on a
$[\eta_{l-1}, \varepsilon] = [\eta_{l-1}, \eta_1^{-1/2}] = 1/2$,
$[\eta_{l-1}, 1+\zeta^m] = [\eta_{l-1}, 2\eta_1^{m/2}] = -m/2$.
$[\eta_{l-1}, 1-\zeta^n] = [\eta_{l-1}, \lambda b_n(\zeta)] = [\eta_{l-1}, b_n(\zeta)] = [\eta_{l-1}, n\eta_1^{(n-1)/2}]$
$= (1-n)/2$.
(iii) Supposons $l \geqslant 5$. On obtient
$[\eta_{l-2}, \eta_1] = -1$
par application de (R24).
Vu les propositions précédentes, on a

$$[\eta_{l-2}, \varepsilon] = [\eta_{l-2}, \eta_1^{-1/2}\eta_2^{1/24}] = -\frac{1}{2}[\eta_{l-2}, \eta_1]+\frac{1}{24}[\eta_{l-2}, \eta_2]$$
$$= \frac{1}{2}-\frac{2}{24} = \frac{5}{12},$$

$$[\eta_{l-2}, 1+\zeta^m] = [\eta_{l-2}, 2\eta_1^{m/2}\eta_2^{-m^2/8}] = \frac{m}{2}[\eta_{l-2}, \eta_1]-\frac{m^2}{8}[\eta_{l-2}, \eta_2]$$
$$= -\frac{m}{2}+\frac{2m^2}{8} = \frac{m^2-2m}{4},$$

$$[\eta_{l-2}, 1-\zeta^n] = [\eta_{l-2}, \lambda b_n(\zeta)] = [\eta_{l-2}, b_n(\zeta)] = [\eta_{l-2}, n\eta_1^{(n-1)/2}\eta_2^{(1-n^2)/24}]$$
$$= \frac{n-1}{2}[\eta_{l-2}, \eta_1]+\frac{(1-n^2)}{24}[\eta_{l-2}, \eta_2] = \frac{1-n}{2}+\frac{2(n^2-1)}{24}$$
$$= \frac{n^2-6n+5}{12}. \blacksquare$$

4. Les nombres $\alpha_m, \ldots, \delta_m$. Dans la suite, nous adopterons les notations suivantes :

a est un entier relatif,
$v = v_l(a^{l-1}-1)$,
si $l \nmid a$, $b = q(a)$,
si $l \nmid a$, f est le plus petit des entiers $k \geqslant 1$ tels que $a^k \equiv 1\ (l)$,
si $m \geqslant 0$ est un entier, $\alpha_m = A_m(a, \zeta)$ et $\beta_m = B_m(a, \zeta)$,
si $m \geqslant 1$ est un entier, $\gamma_m = C_m(a, \zeta)$,
si $m \geqslant 3$ est un entier, $\delta_m = D_m(a, \zeta)$.

PROPOSITION 14. (i) *Si $m \geqslant 0$ est un entier, $\alpha_m = \alpha_1 \beta_m$.*
(ii) *Si $m \geqslant 1$ est un entier, on a*

$$\alpha_m = \prod_{d|m} \gamma_d, \quad \beta_m = \prod_{\substack{d|m \\ d \geqslant 2}} \gamma_d.$$

(iii) *Si $m \geqslant 0$ et $n \geqslant 0$ sont des entiers, on a*

$$\alpha_{m+n} = a^n \alpha_m + \zeta^m \alpha_n, \quad \beta_{m+n} = a^n \beta_m + \zeta^m \beta_n.$$

(iv) *Si $m \geqslant 3$ est un entier, on a*

$$\gamma_m - \alpha_1^{\varphi(m)} = c_m(1) a \zeta \delta_m.$$

Démonstration. (i) résulte des définitions ; (ii) résulte des propriétés (C3) et (C4) du paragraphe 2 ; (iii) résulte de la proposition 2 et (iv) résulte des définitions.

PROPOSITION 15. (i) *Soient $m, n, \boldsymbol{a}, \boldsymbol{b}$ des entiers $\geqslant 0$ tels que $m \equiv n\ (\boldsymbol{a})$ et que $m \equiv -n\ (\boldsymbol{b})$, on a les congruences*

$$\alpha_m \equiv a^{m-n} \alpha_n \equiv \zeta^{m-n} \alpha_n \ (\alpha_a),$$

$$\beta_m \equiv a^{m-n} \beta_n \equiv \zeta^{m-n} \beta_n \ (\beta_a),$$

$$a^n \alpha_m \equiv \zeta^m \alpha_n \ (\alpha_b),$$

$$a^n \beta_m \equiv -\zeta^m \beta_n \ (\beta_b).$$

(ii) *Soit $m \geqslant 3$ un entier, on a*

$$\delta_m \equiv \zeta^{\varphi(m)-2} \ (\alpha_1),$$

$$a\delta_m \prod_{\substack{i=1 \\ (i,m)=1}}^{m} \beta_i \equiv -\zeta^{\varphi_1(m)-1} \ (\gamma_m),$$

$$\zeta\delta_m \prod_{\substack{i=1 \\ (i,m)=1}}^{m} \beta_i \equiv -a^{\varphi_1(m)-1} \ (\gamma_m).$$

Démonstration. (i) résulte de la proposition 2 et (ii) résulte de la proposition 9.

PROPOSITION 16. *Dans l'anneau A, on a :*
(i) *Si $m \geqslant 1$ est un entier, on a*

$$(\alpha_m, a) = (\beta_m, a) = (\gamma_m, a) = (1).$$

(ii) *Si $m \geqslant 3$ est un entier, on a*

$$(\delta_m, \alpha_1) = (\delta_m, \gamma_m) = (1).$$

(iii) *Si $m \geqslant 0$ et $n \geqslant 0$ sont des entiers tels que $(m, n) = 1$, on a*

$$(\beta_m, \beta_n) = (1).$$

(iv) *Si $m \geqslant 2$ et $n \geqslant 1$ sont des entiers tels que $(m, n) = 1$, on a*

$$(\beta_n, \gamma_m) = (1).$$

(v) *Si m et n sont des entiers tels que $n > m \geqslant 1$ et que $m \nmid n$, on a*

$$(\gamma_m, \gamma_n) = (1).$$

Démonstration. (i) On a $\zeta^m = a^m - \alpha_m$; d'où $(\alpha_m, a) = (1)$ et, par suite, $(\beta_m, a) = (\gamma_m, a) = (1)$.
(ii) résulte des congruences de la proposition précédente.
(iii) Si $(m, n) = 1$, la proposition 4 montre que $\zeta^{m+n-1}\beta_1 = \zeta^{m+n-1}$ appartient à l'idéal (β_m, β_n) ; on a donc $(\beta_m, \beta_n) = (1)$.
(iv) résulte de (iii).
(v) La proposition 5 montre que ζ^{m+n-1} appartient à l'idéal (γ_m, γ_n) ; d'où $(\gamma_m, \gamma_n) = (1)$.

PROPOSITION 17. *Soit $m \geqslant 1$ un entier.*
(i) $\alpha_1 \neq 0$.
(ii) *Pour qu'on ait $\alpha_m = 0$ (resp. $\beta_m = 0$), il faut et il suffit qu'on ait $a = 1$ et $l|m$ ou bien qu'on ait $a = -1$ et $2l|m$.*
(iii) *Si on a $m \geqslant 3$ et $\delta_m = 0$, a vaut -1.*
(iv) *Si $|a| \geqslant 2$, on a $\alpha_m \neq 0$, $\beta_m \neq 0$, $\gamma_m \neq 0$ et lorsque $m \geqslant 3$, on a $\delta_m \neq 0$.*

Démonstration. (i) et (ii) sont immédiates.
(iii) Supposons $m \geqslant 3$ et $\delta_m = 0$; vu la proposition précédente, on a $(\alpha_1) = (\alpha_1, \delta_m) = (1)$; ainsi $\alpha_1 = a - \zeta$ est une unité de K ; par suite, on a $N(\alpha_1) = 1$; d'où $c_l(a) = 1$; vu la proposition 6, on a $|a| \leqslant 1$; si $a = 1$, $\alpha_1 = \lambda$, ce qui est absurde puisque λ n'est pas une unité de K ; si $a = 0$, on a

$$\delta_m = D_m(0, \zeta) = \frac{\varphi(m) - \mu(m)}{c_m(1)} \zeta^{\varphi(m)-2} \neq 0,$$

ce qui est absurde ; on a donc $a = -1$.
(iv) résulte de (ii) et (iii).

ENONCÉ 2. *Soit $m \geqslant 3$ un entier, pour que $\delta_m = 0$, il faut et il suffit qu'on ait $a = -1$ et $l = 3$ et que m ne soit ni 3 ni de la forme $2p^n$ avec p premier, $p \equiv 2\ (3)$ et $n \geqslant 0$ ni de la forme $6q^n$ avec q premier et $n \geqslant 0$.*

Cela résulte de la proposition précédente et de l'énoncé 1.

PROPOSITION 18. *Supposons que a ne soit pas divisible par l.*
(i) *On a $v \geqslant 1$ et f divise $l-1$.*
(ii) *Soient $m \geqslant 0$ et $n \geqslant 0$ des entiers. Si $m \not\equiv n\ (f)$, on a*

$$v_l(a^m - a^n) = 0$$

tandis que si $m \equiv n\ (f)$, on a

$$v_l(a^m - a^n) = v + v_l(m - n).$$

(iii) *On a* $v_l(c_f(a)) = v$; *si* $k \geqslant 1$ *est un entier, on a* $v_l(c_{fl^k}(a)) = 1$; *enfin, si* $m \geqslant 1$ *est un entier qui n'est pas de la forme* fl^r *pour un entier* $r \geqslant 0$, *on a* $v_l(c_m(a)) = 0$.

(iv) $v_l(c_f(a^l)) = v+1$.

(v) *Si* $m \geqslant 0$ *est un entier divisible par f, on a*

$$v_l(a^m-1) = v+v_l(m) \quad \text{et on a} \quad a^m \equiv 1-mbl \ (l^2).$$

(vi) *Si f est pair et si* $m \geqslant 0$ *est un entier divisible par f/2 et non par f, on a*

$$v_l(a^m+1) = v+v_l(m) \quad \text{et on a} \quad a^m \equiv -1+mbl \ (l^2).$$

Démonstration. (i) est classique ; je laisse (ii) au lecteur ; pour (iii), je le renvoie au théorème 8 d'un article de Richter [15] et (iv) résulte de (iii) et de (C7).

(v) Si m est divisible par f, il y a un entier x tel que $a^m = 1+xl$ et on a

$$a^{m(l-1)} = (1+xl)^{l-1} \equiv 1-xl \ (l^2),$$

$$a^{m(l-1)} = (1+bl)^m \equiv 1+mbl \ (l^2).$$

D'où $-x \equiv mb \ (l)$ et le résultat.

(vi) Vu ce qui précède, on a

$$v_l(a^m-1) = 0 \quad \text{et} \quad v_l(a^{2m}-1) = v+v_l(2m) = v+v_l(m) \ ;$$

d'où

$$v_l(a^m+1) = v+v_l(m).$$

Il y a un entier y tel que $a^m = -1+yl$; d'où $a^{2m} \equiv 1-2yl \ (l^2)$, d'où, vu le point (v), $2y \equiv 2mb \ (l)$; d'où le résultat.

Proposition 19. *Supposons que a ne soit pas divisible par l et soit* $m \geqslant 0$ *un entier.*

(i) *Si* $f \nmid m$, $v_\lambda(\alpha_m) = 0$; *si on a* $f \mid m$ *et* $l \nmid m$, $v_\lambda(\alpha_m) = 1$; *si* $fl \mid m$, $v_\lambda(\alpha_m) = (v+v_l(m))(l-1)$.

(ii) *Si* $fl \nmid m$, $v_\lambda(\alpha_m) \leqslant 1$.

(iii) *Si* $f \mid m$, *on a*

$$\alpha_m \equiv 1-\zeta^m \ (l^{v+v_l(m)})$$

et si, de plus, $l \geqslant 5$, *on a*

$$\alpha_m \equiv (1-\zeta^m)\eta_{l-2}^{-b}\eta_{l-1}^{-b(m-2)/2}\eta_l^{-b(m^2-3m+1)/12} \ (\lambda^{l+2}).$$

(iv) *Si on a f pair et m divisible par f/2 et non par f, on a*

$$\alpha_m \equiv -(1+\zeta^m) \ (l^{v+v_l(m)}),$$

$$\alpha_m \equiv -(1+\zeta^m)\eta_{l-1}^{-bm/2}\eta_l^{-bm(m-1)/4} \ (\lambda^{l+1}).$$

Démonstration. (i) et (ii) résultent facilement de la proposition précédente.

(iii) La première congruence résulte de la proposition précédente, puisque $\alpha_m-(1-\zeta^m) = a^m-1$. Supposons donc $l \geqslant 5$ et $f \mid m$. Si m est divisible par l, il résulte de (i) que α_m est divisible par λ^{2l-2}; d'où le résultat dans ce cas.

Si m n'est pas divisible par l, on a, vu la proposition précédente

$$\alpha_m \equiv 1-\zeta^m-mbl \equiv (1-\zeta^m)(1+mb\varepsilon^{-1}(b_m(\zeta))^{-1}\lambda^{l-2}) \ (l^2).$$

Vu les propositions 10 et 12, on a

$$\alpha_m \equiv (1-\zeta^m)(1+b\eta_1^{(2-m)/2}\eta_2^{(m^2-2)/24}\lambda^{l-2}) \ (\lambda^{l+2}).$$

On a aussi

$$\eta_1^{(2-m)/2} \equiv 1+\frac{(m-2)}{2}\lambda+\frac{(m^2-2m)}{8}\lambda^2 \ (\lambda^3),$$

$$\eta_1^{(2-m)/2}\eta_2^{(m^2-2)/24} \equiv 1+\frac{(m-2)}{2}\lambda+\frac{(m^2-3m+1)}{12}\lambda^2 \ (\lambda^3).$$

D'où

$$\alpha_m \equiv (1-\zeta^m)\left(1+b\lambda^{l-2}+\frac{b(m-2)}{2}\lambda^{l-1}+\frac{b(m^2-3m+1)}{12}\lambda^l\right) \ (\lambda^{l+2})$$

et le résultat dans ce cas aussi.

(iv) Supposons f pair et m divisible par $f/2$ et non par f. La première congruence résulte de la proposition précédente, puisque $\alpha_m+(1+\zeta^m) = a^m+1$.

Vu la proposition précédente, on a

$$\alpha_m \equiv -1-\zeta^m-mbl \equiv -(1+\zeta^m)(1+mb(1+\zeta^m)^{-1}\varepsilon^{-1}\lambda^{l-1}) \ (l^2).$$

Vu les propositions 11 et 12, on a

$$\alpha_m \equiv -(1+\zeta^m)\left(1+\frac{mb}{2}\eta_1^{(1-m)/2}\lambda^{l-1}\right) \ (\lambda^{l+1}),$$

$$\equiv -(1+\zeta^m)\left(1+\frac{bm}{2}\lambda^{l-1}+\frac{bm(m-1)}{4}\lambda^l\right) \ (\lambda^{l+1}).$$

D'où le résultat.

Proposition 20. *Soit* $m \geqslant 0$ *un entier.*

(i) *Si* $l \mid a$ *ou si* $f \nmid m$, $N(\alpha_m) \equiv 1 \ (l)$.

(ii) *Si on a* $l \geqslant 5$, $l \nmid a$, $f \mid m$ *et* $l \nmid m$, *on a*

$$N(\alpha_m) \equiv -\lambda^{l-1}\varepsilon^{-1}\eta_{l-1}^{bm/2}\eta_l^{-bm/4} \ (\lambda^{2l}).$$

Démonstration. (i) Si $l \mid a$ ou si $f \nmid m$, on a $\alpha_m \equiv a^m-1 \not\equiv 0 \ (\lambda)$; d'où

$$N(\alpha_m) \equiv (a^m-1)^{l-1} \equiv 1 \ (\lambda) \ ;$$

d'où le résultat.

(ii) Supposons $l \geqslant 5$, $l \nmid a$, $f \mid m$ et $l \nmid m$. Vu les propositions 2 et 18, on a

$$N(\alpha_m) = b_l(a^m) = \sum_{i=0}^{l-1} \binom{l}{i+1} (a^m-1)^i \equiv l + \frac{l(l-1)}{2}(a^m-1) \equiv l + \frac{mb}{2} l^2 \ (l^3)$$

$$\equiv l\left(1 - \frac{mb}{2}\varepsilon^{-1}\lambda^{l-1}\right) \ (\lambda^{2l}).$$

Vu la proposition 12, on a

$$N(\alpha_m) \equiv l\left(1 - \frac{bm}{2}\eta_1^{1/2}\lambda^{l-1}\right) \equiv l\left(1 - \frac{bm}{2}\lambda^{l-1} + \frac{bm}{4}\lambda^l\right) \ (\lambda^{2l})$$

$$\equiv l\eta_{l-1}^{bm/2}\eta_l^{-bm/4} \ (\lambda^{2l}).$$

D'où le résultat.

PROPOSITION 21. *Supposons que a ne soit pas divisible par l.*

(i) *Si m et n sont des entiers $\geqslant 0$ tels que $m \equiv n$ (f^l), on a*

$$\alpha_m \equiv \alpha_n \ (l^{v+1}).$$

(ii) *Si m et r sont des entiers tels que $0 \leqslant m \leqslant rf^l$, on a*

$$\alpha_{rf^l-m} \equiv -a^{rf^l-m}\zeta^{-m}\alpha_m \ (l^{v+1}).$$

(iii) *Si $m \geqslant 0$ et $n \geqslant 1$ sont des entiers tels que l ne divise pas n et que $n \equiv 1$ (f), on a*

$$\alpha_{mn} \equiv s_n(\alpha_m) \ (l^v).$$

Démonstration. On a

$$\alpha_m - \alpha_n = a^m - a^n,$$

$$\alpha_{rf^l-m} + a^{rf^l-m}\zeta^{-m}\alpha_m = \zeta^{-m}(a^{rf^l}-1),$$

$$\alpha_{mn} - s_n(\alpha_m) = a^{mn} - a^m,$$

d'où les résultats, vu la proposition 18.

PROPOSITION 22. *Supposons que a ne soit pas divisible par l et soit $m \geqslant 1$ un entier non divisible par f, on a les congruences*

$$\prod_{i=0}^{l-1} \alpha_{m+if} \equiv \alpha_{ml}, \qquad \prod_{\substack{i=0 \\ l \nmid m+if}}^{l-1} \alpha_{m+if} \equiv 1,$$

suivant le module $\lambda^{(v+1)(l-1)-1}$.

Démonstration. On a $\alpha_{fl} = \alpha_f B_l(a^f, \zeta^f)$; d'où

$$a^{fl} \equiv 1 \ (B_l(a^f, \zeta^f))$$

et, vu la proposition 19,

$$v_\lambda(B_l(a^f, \zeta^f)) = (v+1)(l-1) - 1.$$

Soient π et ϱ les produits de l'énoncé ; on a

$$\pi = \prod_{i=0}^{l-1} (a^m(a^f)^i - \zeta^m(\zeta^f)^i)$$

et, vu la proposition 8, on a

$$\pi \equiv (a^f)^{l(l-1)/2} A_l(a^m, \zeta^m) \ (C_l(a^f, \zeta^f))$$

d'où

$$\pi \equiv \alpha_{ml} \ (B_l(a^f, \zeta^f))$$

d'où la première congruence.

Soit j l'entier de l'intervalle $[0, l-1]$ tel que l divise $m+jf$, on a $m+jf \equiv ml$ (f^l); vu la proposition précédente, on $\alpha_{m+jf} \equiv \alpha_{ml}$ (l^{v+1});

On a alors

$$\varrho\alpha_{ml} \equiv \alpha_{ml} \ (\lambda^{(v+1)(l-1)-1})$$

d'où la seconde congruence, puisque, vu la proposition 19, α_{ml} n'est pas divisible par λ.

PROPOSITION 23. *Supposons que a ne soit pas divisible par l et soient $m \geqslant 0$, $g \geqslant 1$ et $h \geqslant 1$ des entiers tels que $f = gh$, on a*

$$\prod_{i=0}^{g-1} \alpha_{m+ihl} \equiv (-1)^{g-1}\alpha_{gm} \ (l^{v+1}).$$

Démonstration. Soit π le produit de l'énoncé; on a

$$\pi = \prod_{i=0}^{g-1} (a^m(a^{hl})^i - \zeta^m)$$

et la proposition 8 donne

$$\pi \equiv (-1)^{g-1} A_g(a^m, \zeta^m) \ (C_g(a^{hl}, 1)),$$

$$\pi \equiv (-1)^{g-1}\alpha_{gm} \ (c_g(a^{hl}))$$

et, vu (C5), on a

$$\pi \equiv (-1)^{g-1}\alpha_{gm} \ (c_f(a^l)),$$

d'où le résultat, vu la proposition 18.

5. Calcul de symboles.

PROPOSITION 24. *Soit $m \geqslant 1$ un entier non divisible par l.*

(i) *Si $a \neq 0$, $[\alpha_m, \zeta] = [\alpha_m, a] + m[a, \zeta]$.*

(ii) *Si a est hyperprimaire, $[\alpha_m, \zeta] = 0$.*

(iii) *Si $l \mid a$ ou si $f \nmid m$, on a $[\alpha_m, \zeta] = (a^{ml} - a^m)/l(a^m - 1)$.*

(iv) *Si on a $l \nmid a$ et $f \nmid m$, on a $[\alpha_m, \zeta] = (ma^m b)/(a^m - 1)$.*

(v) *Si on a $l \geqslant 5$, $l \nmid a$ et $f \mid m$, on a $[\alpha_m, \zeta] = mb/2$.*

Démonstration. (i) $[\alpha_m, \zeta^m] = [a^m-\zeta^m, \zeta^m] = [a^m-\zeta^m, a^m]+[a^m, \zeta^m]$. D'où

$$m[\alpha_m, \zeta] = m[\alpha_m, a]+m^2[a, \zeta]$$

et le résultat.

(ii) résulte de (i).

(iii) Dans chacun des deux cas, α_m n'est pas divisible par λ et comme $N(\alpha_m) = b_l(a^m)$, on a

$$[\alpha_m, \zeta] = \frac{b_l(a^m)-1}{l} = \frac{a^m b_{l-1}(a^m)}{l} = \frac{a^m(a^{m(l-1)}-1)}{l(a^m-1)} = \frac{a^{ml}-a^m}{l(a^m-1)}.$$

(iv) résulte de (iii), puisque dans le corps F_l, on a $q(a^m) = mq(a)$.

(v) Supposons $l \geqslant 5$, $l \nmid a$ et $f \mid m$; vu les propositions 19 et 13, on a

$$\alpha_m \equiv (1-\zeta^m)\eta_{l-2}^{-b}\eta_{l-1}^{-b(m-2)/2} \ (\lambda^{l+1}),$$

$$[\alpha_m, \zeta] = -b[\eta_{l-2}, \zeta]-\frac{b(m-2)}{2}[\eta_{l-1}, \zeta]$$

$$= -b[\eta_{l-2}, \eta_1]-\frac{b(m-2)}{2}[\eta_{l-1}, \eta_1] = b+\frac{b(m-2)}{2} = \frac{bm}{2}.$$

ENONCÉ 3. (i) *Si* $a \not\equiv 1$ (l),

$$[\alpha_1, \lambda] = \frac{a+1}{2(a-1)}q(a-1).$$

(ii) *Si on a* $l \geqslant 5$ *et* $a \equiv 1$ (l), *on a* $[\alpha_1, \lambda] = b/12$.

ENONCÉ 4. (i) *Si* $a^2 \not\equiv 1$ (l),

$$[\alpha_1, 1+\zeta] = \frac{a+1}{2(a-1)}q(a+1).$$

(ii) *Si* $a \equiv -1$ (l), $[\alpha_1, 1+\zeta] = b/4$.

(iii) *Si on a* $l \geqslant 5$ *et* $a \equiv 1$ (l), $[\alpha_1, 1+\zeta] = 0$.

Ces deux énoncés sont faciles à démontrer.

PROPOSITION 25. (i) *Si* $a \not\equiv 1$ (l), *on a*

$$[\alpha_1, N(\alpha_1)] = (a-a^l)/l(a-1)^2.$$

(ii) *Si on a* $l \geqslant 5$ *et* $a \equiv 1$ (l), *on a* $[\alpha_1, N(\alpha_1)] = b/3$.

Démonstration. (i) Vu la proposition 20, on a $N(\alpha_1) = b_l(a) \equiv 1$ (l). D'où

$$[\alpha_1, N(\alpha_1)] = [a-1+\lambda, b_l(a)] = \frac{(b_l(a))^{l-1}-1}{l(a-1)} = \frac{(b_l(a))^l-b_l(a)}{l(a-1)} = \frac{1-b_l(a)}{l(a-1)}$$

$$= -\frac{ab_{l-1}(a)}{l(a-1)} = -\frac{a(a^{l-1}-1)}{l(a-1)^2} = \frac{a-a^l}{l(a-1)^2}.$$

(ii) Vu les propositions 19 et 20, on a

$$\alpha_1 \equiv \lambda\eta_{l-2}^{-b}\eta_{l-1}^{b/2}\eta_l^{b/12} \ (\lambda^{l+2}),$$

$$N(\alpha_1) \equiv -\lambda^{l-1}\varepsilon^{-1}\eta_{l-1}^{b/2}\eta_l^{-b/4} \ (\lambda^{2l}).$$

D'où

$$[\alpha_1, N(\alpha_1)] = [\lambda\eta_{l-2}^{-b}\eta_{l-1}^{b/2}\eta_l^{b/12}, -\lambda^{l-1}\varepsilon^{-1}\eta_{l-1}^{b/2}\eta_l^{-b/4}]$$

$$= -\frac{b}{4}[\lambda, \eta_l]+b[\eta_{l-2}, \varepsilon]-\frac{b}{2}[\eta_{l-1}, \varepsilon]-\frac{b}{12}[\eta_l, \lambda]-\frac{b}{12}[\eta_l, \varepsilon].$$

Vu la proposition 13, on a

$$[\alpha_1, N(\alpha_1)] = \frac{b}{4}+\frac{5b}{12}-\frac{b}{4}-\frac{b}{12} = \frac{b}{3}.$$

PROPOSITION 26. *Supposons que a ne soit pas divisible par l et qu'on ait* $l \geqslant 5$ *ou a hyperprimaire et soient m, n, m', n' des entiers* $\geqslant 0$ *dont aucun n'est divisible par fl et tels que* $m \equiv m'$ (fl) *et que* $n \equiv n'$ (fl), *on a*

$$[\alpha_m, \alpha_n] = [\alpha_{m'}, \alpha_{n'}].$$

Démonstration. Vu la proposition 19, la valuation λ-adique de chacun des nombres α_m, α_n, $\alpha_{m'}$, $\alpha_{n'}$ est 0 ou 1.

Vu la proposition 21, on a

$$\alpha_m \equiv \alpha_{m'} \ (\lambda^{(v+1)(l-1)}),$$

d'où, vu les hypothèses,

$$\alpha_m \equiv \alpha_{m'} \ (\lambda^{l+3})$$

et, de même, $\alpha_n \equiv \alpha_{n'}$ (λ^{l+3}) ; d'où le résultat.

PROPOSITION 27. *Supposons que a ne soit pas divisible par l et soient m, n et r des entiers* $\geqslant 0$ *tels que ni m ni n ne soient divisibles par fl et qu'on ait* $n \leqslant rfl$.

(i) *Si on a* $l \geqslant 5$ *ou* $f \nmid m$, *on a*

$$[\alpha_m, \alpha_{rfl-n}] = [\alpha_m, \alpha_n]-n[\alpha_m, a]-n[\alpha_m, \zeta].$$

(ii) *Si on a* $l \nmid m$ *et a hyperprimaire, on a*

$$[\alpha_m, \alpha_{rfl-n}] = [\alpha_m, \alpha_n].$$

Démonstration. Vu la proposition 19, $v_\lambda(\alpha_m)$ et $v_\lambda(\alpha_{rfl-n})$ valent 0 ou 1 et, si $f \nmid m$, $v_\lambda(\alpha_m) = 0$.

(i) Vu la proposition 21, on a

$$\alpha_{rfl-n} \equiv -a^{rfl-n}\zeta^{-n}\alpha_n \ (\lambda^{2l-2}),$$

d'où, dans chacun des deux cas,

$$[\alpha_m, \alpha_{rfl-n}] = [\alpha_m, -a^{rfl-n}\zeta^{-n}\alpha_n]$$

et le résultat.

(ii) Si a est hyperprimaire, on a en vertu de la proposition 21

$$\alpha_{rfl-n} \equiv -a^{rfl-n}\zeta^{-n}\alpha_n \ (\lambda^{3l-3})$$

d'où

$$[\alpha_m, \alpha_{rfl-n}] = [\alpha_m, -a^{rfl-n}\zeta^{-n}\alpha_n] = [\alpha_m, \alpha_n] - n[\alpha_m, \zeta].$$

Si, de plus, $l \nmid m$, on a, vu la proposition 24,

$$[\alpha_m, \alpha_{rfl-n}] = [\alpha_m, \alpha_n].$$

PROPOSITION 28. (i) *Si* $l|a$, $[\alpha_1, \alpha_{l^2-l-1}] = a/l$.

(ii) *Si on a* $l \nmid a$ *et* $a \not\equiv 1$ (l), *on a*

$$[\alpha_1, \alpha_{l^2-l-1}] = (1+a)b/(1-a).$$

(iii) *Si on a* $l \geqslant 5$ *et* $a \equiv 1$ (l), $[\alpha_1, \alpha_{l^2-l-1}] = 0$.

Démonstration. (i) Supposons que l divise a; compte tenu de la proposition 24, on a

$$[\alpha_1, \alpha_{l^2-l-1}] = [\alpha_1, -\zeta] = \frac{a^l - a}{l(a-1)} = \frac{a}{l}.$$

(ii) et (iii). Sous les hypothèses de (ii) ou de (iii), a n'est pas divisible par l et on a $l \geqslant 5$ ou $f \nmid 1$; on peut donc appliquer la proposition précédente et on a

$$[\alpha_1, \alpha_{l^2-l-1}] = -[\alpha_1, a] - [\alpha_1, \zeta]$$

et, vu la proposition 24, on a

$$[\alpha_1, \alpha_{l^2-l-1}] = [a, \zeta] - 2[\alpha_1, \zeta] = b - 2[\alpha_1, \zeta].$$

Sous les hypothèses de (ii), on a, vu la proposition 24,

$$[\alpha_1, \alpha_{l^2-l-1}] = b - 2\frac{ab}{(a-1)} = \frac{(1+a)b}{1-a}.$$

Sous les hypothèses de (iii), on a, vu la proposition 24,

$$[\alpha_1, \alpha_{l^2-l-1}] = b - 2\frac{b}{2} = 0.$$

PROPOSITION 29. *Supposons que a ne soit pas divisible par l et qu'on ait* $l \geqslant 5$ *ou a hyperprimaire et soient m et n des entiers* $\geqslant 0$ *dont aucun n'est divisible par l.*

(i) *Si m et n sont divisibles par f,* $[\alpha_m, \alpha_n] = 0$.

(ii) *Si f est pair et si m et n sont divisibles par f/2,* $[\alpha_m, \alpha_n] = 0$.

Démonstration. (i) Supposons d'abord $l \geqslant 5$. Pour $k = m, n$, posons

$$\theta_k = \eta_{l-2}^{-b}\eta_{l-1}^{-b(k-2)/2}\eta_l^{-b(k^2-3k+1)/12}.$$

Vu la proposition 19, on a

$$\alpha_m \equiv (1-\zeta^m)\theta_m \ (\lambda^{l+2}), \quad \alpha_n \equiv (1-\zeta^n)\theta_n \ (\lambda^{l+2}).$$

D'où

$$[\alpha_m, \alpha_n] = [(1-\zeta^m)\theta_m, (1-\zeta^n)\theta_n] = [\theta_m, 1-\zeta^n] - [\theta_n, 1-\zeta^m].$$

Vu la proposition 13, $[\theta_m, 1-\zeta^n]$ vaut

$$-b[\eta_{l-2}, 1-\zeta^n] - \frac{b(m-2)}{2}[\eta_{l-1}, 1-\zeta^n] - \frac{b(m^2-3m+1)}{12}[\eta_l, 1-\zeta^n]$$

$$= -b\frac{(n^2-6n+5)}{12} - b\frac{(m-2)(1-n)}{4} - b\frac{(m^2-3m+1)}{12}$$

$$= -\frac{b}{12}(m^2-3mn+n^2).$$

De même, on a

$$[\theta_n, 1-\zeta^m] = -\frac{b}{12}(n^2-3nm+m^2),$$

d'où $[\alpha_m, \alpha_n] = 0$ et le résultat dans ce cas.

Supposons maintenant $l = 3$. Dans ce cas, a est hyperprimaire. Si on a $m \equiv n$ (3), on a $m \equiv n$ (fl) et, vu la proposition 26, on a $[\alpha_m, \alpha_n] = [\alpha_n, \alpha_n] = 0$. Si on n'a pas $m \equiv n$ (3), on a $m \equiv -n$ (3) ; soit alors r un entier tel que $rfl \geqslant n$, on a $m \equiv rfl - n$ (3) et, vu ce qui précède, on a $[\alpha_m, \alpha_{rfl-n}] = 0$; la proposition 27 donne alors $[\alpha_m, \alpha_n] = 0$, ce qui achève la démonstration de (i).

(ii) Supposons f pair et m et n divisibles par $f/2$. Si m et n sont divisibles par f, on a $[\alpha_m, \alpha_n] = 0$ vu ce qui précède.

Supposons que ni m ni n ne soient divisibles par f. Vu la proposition 19, on a

$$\alpha_m \equiv -(1+\zeta^m)\eta_{l-1}^{-bm/2} \ (\lambda^l),$$

$$\alpha_n \equiv -(1+\zeta^n)\eta_{l-1}^{-bn/2} \ (\lambda^l).$$

D'où, vu la proposition 13,

$$[\alpha_m, \alpha_n] = -\frac{bn}{2}[1+\zeta^m, \eta_{l-1}] - \frac{bm}{2}[\eta_{l-1}, 1+\zeta^n] = -\frac{bnm}{4} + \frac{bmn}{4} = 0.$$

Supposons que m soit divisible par f et que n ne le soit pas. Supposons d'abord $l \geqslant 5$. Vu la proposition 19, on a

$$\alpha_m \equiv (1-\zeta^m)\eta_{l-2}^{-b}\eta_{l-1}^{-b(m-2)/2} \quad (\lambda^{l+1}),$$

$$\alpha_n \equiv -(1+\zeta^n)\eta_{l-1}^{-bn/2}\eta_l^{-bn(n-1)/4} \ (\lambda^{l+1}).$$

D'où, vu la proposition 13,

$$[\alpha_m, \alpha_n] = -\frac{bn}{2}[1-\zeta^m, \eta_{l-1}] - \frac{bn(n-1)}{4}[1-\zeta^m, \eta_1]$$

$$-b[\eta_{l-2}, 1+\zeta^n] - \frac{b(m-2)}{2}[\eta_{l-1}, 1+\zeta^n]$$

$$= -\frac{bn(m-1)}{4} + \frac{bn(n-1)}{4} - \frac{b(n^2-2n)}{4} + \frac{b(m-2)n}{4} = 0.$$

Supposons maintenant $l = 3$. Dans ce cas, a est hyperprimaire et, vu la proposition 19, on a

$$\alpha_m \equiv 1-\zeta^m \quad (\lambda^4),$$

$$\alpha_n \equiv -(1+\zeta^n) \quad (\lambda^4).$$

D'où

$$[\alpha_m, \alpha_n] = [1-\zeta^m, -(1+\zeta^n)] = 0.$$

Enfin, si f divise n et non m, on a, vu ce qui précède, $[\alpha_m, \alpha_n] = -[\alpha_n, \alpha_m] = 0$, ce qui achève la démonstration.

PROPOSITION 30. *Supposons que a ne soit pas divisible par l et qu'on ait $l \geqslant 5$ ou a hyperprimaire et soient m et n des entiers $\geqslant 0$ tels que m ne soit pas divisible par fl et que n ne soit pas divisible par f, on a*

$$\sum_{\substack{i=0 \\ l\nmid n+if}}^{l-1} [\alpha_m, \alpha_{n+if}] = 0.$$

Démonstration. Vu la proposition 19, on a $\alpha_m \neq 0$ et vu la proposition 22, on a

$$\prod_{\substack{i=0 \\ l\nmid n+if}}^{l-1} \alpha_{n+if} \equiv 1 \quad (\lambda^{(v+1)(l-1)-1}),$$

d'où, vu les hypothèses,

$$\prod_{\substack{i=0 \\ l\nmid n+if}}^{l-1} \alpha_{n+if} \equiv 1 \quad (\lambda^{l+2}),$$

d'où

$$\left[\alpha_m, \prod_{\substack{i=0 \\ l\nmid n+if}}^{l-1} \alpha_{n+if}\right] = 0,$$

d'où le résultat.

PROPOSITION 31. *Supposons que a ne soit pas divisible par l et qu'on ait $l \geqslant 5$ ou a hyperprimaire et soient g et h des entiers $\geqslant 1$ tel que $f = gh$, $m \geqslant 0$ un entier non divisible par fl et $n \geqslant 0$ un entier non divisible par hl, on a*

$$[\alpha_m, \alpha_{gn}] = \sum_{i=0}^{g-1} [\alpha_m, \alpha_{n+ihl}].$$

Démonstration. Vu la proposition 19, les valuations λ-adiques de α_m et α_{gn} sont 0 ou 1 et, vu la proposition 23, on a

$$\prod_{i=0}^{g-1} \alpha_{n+ihl} \equiv (1)^{g-1}\alpha_{gn} \quad (l^{v+1}),$$

d'où, vu les hypothèses,

$$\prod_{i=0}^{g-1} \alpha_{n+ihl} \equiv (-1)^{g-1}\alpha_{gn} \quad (\lambda^{l+3}),$$

d'où

$$[\alpha_m, (-1)^{g-1}\alpha_n] = \left[\alpha_m, \prod_{i=0}^{g-1} \alpha_{n+ihl}\right],$$

d'où le résultat.

PROPOSITION 32. *Supposons a hyperprimaire et soient m, n, k des entiers $\geqslant 0$ tels que ni m ni n ne soit divisible par fl, que l ne divise pas k et qu'on ait $k \equiv 1$ (f), alors on a*

$$[\alpha_{km}, \alpha_{kn}] = k[\alpha_m, \alpha_n].$$

Démonstration. Si m et n sont divisibles par f, cela résulte de la proposition 29.

Si m n'est pas divisible par f, on a, en vertu de la proposition 19, $v_\lambda(\alpha_m) = 0$ et $v_\lambda(\alpha_n) \leqslant 1$; d'où $v_\lambda(s_k(\alpha_m)) = 0$ et $v_\lambda(s_k(\alpha_n)) \leqslant 1$; vu la proposition 21, on a

$$\alpha_{km} \equiv s_k(\alpha_m) \quad (\lambda^{l+1}),$$

$$\alpha_{kn} \equiv s_k(\alpha_n) \quad (\lambda^{l+1}),$$

d'où

$$[\alpha_{km}, \alpha_{kn}] = [s_k(\alpha_m), s_k(\alpha_n)] = k[\alpha_m, \alpha_n].$$

Enfin, si n n'est pas divisible par f, on a, vu ce qui précède

$$[\alpha_{km}, \alpha_{kn}] = -[\alpha_{kn}, \alpha_{km}] = -k[\alpha_n, \alpha_m] = k[\alpha_m, \alpha_n].$$

PROPOSITION 33. *Supposons a hyperprimaire et soient m, n des entiers $\geqslant 0$ tels qu'aucun des nombres m, n, $m+n$ ne soit divisible par l, on a*

$$[\alpha_m, \alpha_n] = [\alpha_m, \alpha_{m+n}] + [\alpha_{m+n}, \alpha_n].$$

Démonstration. Vu la proposition 24, on a

$$[a^n\alpha_m, \zeta^m\alpha_n] = [\alpha_m, \zeta^m\alpha_n] = [\alpha_m, \alpha_n]$$

et, vu les propositions 14 et 19, on a

$$\alpha_{m+n} = a^n\alpha_m + \zeta^m\alpha_n \neq 0,$$

d'où, vu la proposition 24,

$$[a^n\alpha_m, \zeta^m\alpha_n] = [a^n\alpha_m, \alpha_{m+n}] + [\alpha_{m+n}, \zeta^m\alpha_n] = [\alpha_m, \alpha_{m+n}] + [\alpha_{m+n}, \alpha_n],$$

d'où le résultat.

PROPOSITION 34. *Supposons a hyperprimaire et $|a| \geqslant 2$.*

(i) *Si $m \geqslant 1$ est un entier, on a*

$$\left(\frac{\alpha_m}{a}\right) = \left(\frac{\beta_m}{a}\right) = \left(\frac{\gamma_m}{a}\right) = 1,$$

$$\left(\frac{a}{\alpha_m}\right) = \left(\frac{a}{\beta_m}\right) = \left(\frac{a}{\gamma_m}\right) = 1.$$

(ii) *Si $m \geqslant 1$ est un entier non divisible par l, on a*

$$\left(\frac{\zeta}{\alpha_m}\right) = \left(\frac{\zeta}{\beta_m}\right) = \left(\frac{\zeta}{\gamma_m}\right) = 1.$$

(iii) *Soient m, n, d des entiers $\geqslant 1$ tels qu'on ait $m \equiv n$ (d) et $(m, d) = 1$, on a*

$$\left(\frac{\beta_m}{\beta_d}\right) = \left(\frac{\beta_n}{\beta_d}\right).$$

(iv) *Soient m, n, d des entiers $\geqslant 1$ tels qu'on ait $m+n \equiv 0$ (d) et $(ml, d) = 1$, on a*

$$\left(\frac{\beta_m}{\beta_d}\right) = \left(\frac{\beta_n}{\beta_d}\right).$$

(v) *Soit $m \geqslant 3$ un entier, on a*

$$\prod_{\substack{i=1\\(i,m)=1}}^{m} \left(\frac{\beta_i}{\gamma_m}\right) = (\alpha_1, \delta_m)^{\varphi(m)}(\zeta\delta_m, \gamma_m).$$

Démonstration. (i) Vu la proposition 17, α_m est non nul. On a

$$\left(\frac{\alpha_m}{a}\right) = \left(\frac{a^m - \zeta^m}{a}\right) = \left(\frac{-\zeta^m}{a}\right) = 1.$$

La proposition 14 nous donne $\alpha_m = \alpha_1\beta_m$; d'où l'on tire $\left(\frac{\beta_m}{a}\right) = 1$; la proposition 14 nous fournit encore la relation $\alpha_m = \prod_{d|m} \gamma_d$; d'où l'on déduit, par une récurrence, $\left(\frac{\gamma_m}{a}\right) = 1$.

On a

$$\left(\frac{a}{\alpha_m}\right) = (\alpha_m, a)\left(\frac{\alpha_m}{a}\right) = 1$$

et de même on obtient

$$\left(\frac{a}{\beta_m}\right) = \left(\frac{a}{\gamma_m}\right) = 1.$$

(ii) Vu la proposition 24, on a

$$\left(\frac{\zeta}{\alpha_m}\right) = (\alpha_m, \zeta) = 1$$

et on conclut grâce aux relations $\alpha_m = \alpha_1\beta_m$ et $\alpha_m = \prod_{d|m} \gamma_d$.

(iii) On peut supposer $m \geqslant n$. Vu la proposition 17, β_m, β_n et β_d sont non nuls; vu la proposition 16, β_m et β_d sont premiers entre eux; enfin, vu la proposition 15 et (i), on a

$$\left(\frac{\beta_m}{\beta_d}\right) = \left(\frac{a^{m-n}\beta_n}{\beta_d}\right) = \left(\frac{a}{\beta_d}\right)^{m-n}\left(\frac{\beta_n}{\beta_d}\right) = \left(\frac{\beta_n}{\beta_d}\right).$$

(iv) Vu la proposition 17, β_m, β_n et β_d sont non nuls et vu la proposition 15, on a

$$\left(\frac{a^n\beta_m}{\beta_d}\right) = \left(\frac{-\zeta^m\beta_n}{\beta_d}\right)$$

d'où le résultat, compte tenu de (i) et de (ii).

(v) La proposition 15 nous donne

$$\zeta\delta_m \prod_{\substack{i=1\\(i,m)=1}}^{m} \beta_i \equiv -a^{\varphi_1(m)-1} \ (\gamma_m).$$

Vu la proposition 17, γ_m est non nul ainsi que les deux membres de la congruence ci-dessus et vu la proposition 16, γ_m et a sont premiers entre eux; on a donc

$$\left(\frac{\zeta\delta_m}{\gamma_m}\right) \prod_{\substack{i=1\\(i,m)=1}}^{m} \left(\frac{\beta_i}{\gamma_m}\right) = \left(\frac{-a^{\varphi_1(m)-1}}{\gamma_m}\right).$$

Posons $s = \prod_{\substack{i=1\\(i,m)=1}}^{m} \left(\frac{\beta_i}{\gamma_m}\right)$; vu (i), on a

$$\left(\frac{\zeta\delta_m}{\gamma_m}\right)s = \left(\frac{a}{\gamma_m}\right)^{\varphi_1(m)-1} = 1, \quad (\gamma_m, \zeta\delta_m)\left(\frac{\gamma_m}{\delta_m}\right)s = 1.$$

Vu la proposition 14, $\gamma_m \equiv \alpha_1^{\varphi(m)}\ (\delta_m)$ et comme α_1 n'est pas nul, on a

$$(\gamma_m, \zeta\delta_m)\left(\frac{\alpha_1}{\delta_m}\right)^{\varphi(m)} s = 1, \quad (\gamma_m, \zeta\delta_m)(\delta_m, \alpha_1)^{\varphi(m)}\left(\frac{\delta_m}{\alpha_1}\right)^{\varphi(m)} s = 1.$$

Vu la proposition 15, $\delta_m \equiv \zeta^{\varphi(m)-2}\ (\alpha_1)$ et, vu (i), on a

$$\left(\frac{\delta_m}{\alpha_1}\right) = \left(\frac{\zeta}{\alpha_1}\right)^{\varphi(m)-2} = 1,$$

$$(\gamma_m, \zeta\delta_m)(\delta_m, \alpha_1)^{\varphi(m)} s = 1,$$

d'où le résultat.

PROPOSITION 35. *Supposons a hyperprimaire et $|a| \geqslant 2$ et soit $m \geqslant 1$ un entier.*

(i) *Si $m \geqslant 2$ est une puissance d'un nombre premier p, on a*

$$(\alpha_1, \gamma_m)^{\varphi(m)} = (\alpha_1, p)^{\varphi(m)}(p, \gamma_m) \prod_{\substack{i=1 \\ (i,p)=1}}^{m} \left(\frac{\beta_i}{\gamma_m}\right).$$

(ii) *Si m vaut 1 ou si m est divisible par deux nombres premiers différents, on a*

$$(\alpha_1, \gamma_m)^{\varphi(m)} = \prod_{\substack{i=1 \\ (i,m)=1}}^{m} \left(\frac{\beta_i}{\gamma_m}\right).$$

Démonstration. Si $m = 1$, la formule du (ii) est claire. Si $m = 2$, on a

$$(\alpha_1, \gamma_2) = (a-\zeta, a+\zeta) = (a-\zeta, 2a)(2a, a+\zeta)$$
$$= (a-\zeta, 2)(2, a+\zeta) = (\alpha_1, 2)(2, \gamma_2)$$

et la formule du (i) est vérifiée pour $m = 2$.

Supposons $m \geqslant 3$. Vu la proposition 17, α_1, γ_m et δ_m sont non nuls et vu la proposition 14, on a

$$\alpha_1^{\varphi(m)} - \gamma_m = -c_m(1)a\zeta\delta_m \neq 0.$$

On a alors

$$(\alpha_1^{\varphi(m)}, \gamma_m) = (\alpha_1^{\varphi(m)}, \alpha_1^{\varphi(m)} - \gamma_m)(\alpha_1^{\varphi(m)} - \gamma_m, \gamma_m),$$

$$(\alpha_1, \gamma_m)^{\varphi(m)} = (\alpha_1, \alpha_1^{\varphi(m)} - \gamma_m)^{\varphi(m)}(\alpha_1^{\varphi(m)} - \gamma_m, \gamma_m).$$

Vu la proposition 24, on a

$$(\alpha_1, \alpha_1^{\varphi(m)} - \gamma_m) = (\alpha_1, -c_m(1)a\zeta\delta_m) = (\alpha_1, c_m(1))(\alpha_1, \delta_m).$$

On a aussi

$$(\alpha_1^{\varphi(m)} - \gamma_m, \gamma_m) = (-c_m(1)a\zeta\delta_m, \gamma_m) = (c_m(1), \gamma_m)(\zeta\delta_m, \gamma_m).$$

On a donc

$$(\alpha_1, \gamma_m)^{\varphi(m)} = (\alpha_1, c_m(1))^{\varphi(m)}(c_m(1), \gamma_m)(\alpha_1, \delta_m)^{\varphi(m)}(\zeta\delta_m, \gamma_m)$$

et, vu la proposition précédente, on a

$$(\alpha_1, \gamma_m)^{\varphi(m)} = (\alpha_1, c_m(1))^{\varphi(m)}(c_m(1), \gamma_m) \prod_{\substack{i=1 \\ (i,m)=1}}^{m} \left(\frac{\beta_i}{\gamma_m}\right).$$

D'où (i) et (ii), vu la proposition 7.

PROPOSITION 36. *Supposons a hyperprimaire et $|a| \geqslant 2$.*

(i) *Si p est un nombre premier, on a*

$$(\alpha_1, \alpha_p)^{p-1} = (\alpha_1, p)^p (p, \alpha_p) \prod_{i=1}^{p-1} \left(\frac{\beta_i}{\beta_p}\right).$$

(ii) *Si on a $f \geqslant 2$ et si p est un nombre premier tel que $p \neq l$ et que $p \neq f$, on a*

$$(\alpha_1, \alpha_p)^{p-1} = \zeta^u \prod_{i=1}^{p-1} \left(\frac{\beta_i}{\beta_p}\right),$$

avec $u = pq(p)\dfrac{(a^p-a)}{(a-1)(a^p-1)}$.

(iii) *Si f est premier, on a*

$$(\alpha_1, \alpha_f)^{f-1} = \zeta^v \prod_{i=1}^{f-1} \left(\frac{\beta_i}{\beta_f}\right)$$

avec $v = fq(f)\dfrac{(a+1)}{2(a-1)}$.

(iv) $(\alpha_1, \alpha_l)^{-1} = \prod_{i=1}^{l-1} \left(\frac{\beta_i}{\beta_l}\right)$.

Démonstration. (i) résulte de la proposition précédente et des relations $\gamma_p = \beta_p$ et $\alpha_p = \alpha_1\beta_p$.

(ii) On a, sous les hypothèses $f \geqslant 2$, $p \neq l$, $p \neq f$,

$$[\alpha_1, p] = [a-1+\lambda, p] = q(p)/(a-1),$$

$$[p, \alpha_p] = [p, a^p-\zeta^p] = p[p, a^p-\zeta] = p[p, a^p-1+\lambda] = -pq(p)/(a^p-1).$$

D'où

$$p[\alpha_1, p] + [p, \alpha_p] = q(p)\frac{(a^p-a)}{(a-1)(a^p-1)}$$

d'où le résultat, vu (i).

(iii) Supposons f premier ; vu la proposition 19, on a

$$[\alpha_1, f] = [a-1+\lambda, f] = \frac{q(f)}{a-1}, \quad [f, \alpha_f] = [f, 1-\zeta^f] = f[f, 1-\zeta] = f\frac{q(f)}{2}.$$

D'où

$$f[\alpha_1, f]+[f, \alpha_f] = fq(f)\frac{(a+1)}{2(a-1)},$$

d'où le résultat, vu (i).

(iv) résulte de (i).

6. Applications.

PROPOSITION 37. *Supposons $l \geqslant 5$. Les propriétés suivantes sont équivalentes:*

(i) *a est divisible par l^2 ou hyperprimaire.*

(ii) $[\alpha_1, \zeta] = 0$.

(iii) $[\alpha_1, N(\alpha_1)] = 0$.

Démonstration. Il résulte de la proposition 24 que (i) et (ii) sont équivalentes et de la proposition 25 que (i) et (iii) le sont.

ENONCÉ 5. *Supposons $l = 3$.*

(i) *Pour qu'on ait $[\alpha_1, \zeta] = 0$, il faut et il suffit que a soit congru à 0, 1, 7 ou 8 modulo 9.*

(ii) *Pour qu'on ait $[\alpha_1, N(\alpha_1)] = 0$, il faut et il suffit que a soit congru à 0 ou 8 modulo 9 ou que a soit congru à 1, 13 ou 25 modulo 27.*

PROPOSITION 38. *Supposons $l \geqslant 5$. Les propriétés suivantes sont équivalentes :*

(i) $[\alpha_1, \alpha_{l^2-l-1}] = 0$.

(ii) *a est divisible par l^2 ou congru à 1 ou -1 modulo l ou hyperprimaire.*

Cela résulte de la proposition 28.

Pour $l = 3$ et $a = 4$, on a $(\alpha_1, \alpha_5) = \zeta^2$ et la proposition précédente ne peut être étendue au cas $l = 3$.

PROPOSITION 39. *Supposons a hyperprimaire, $|a| \geqslant 2$ et que, pour tous m et n entiers tels que $m \geqslant 1$, $n \geqslant 1$, $(m, n) = 1$ et $l \nmid mn$, on ait $(\alpha_m, \alpha_n) = 1$.*

(i) *Pour tous m et n entiers tels que $m \geqslant 1$, $n \geqslant 1$, $(m, n) = 1$ et $l \nmid mn$, $(\beta_m, \beta_n) = 1$.*

(ii) *Pour tous m et n entiers tels que $m \geqslant 1$, $n \geqslant 1$, $(m, n) = 1$ et $l \nmid n$, on a $\left(\frac{\beta_m}{\beta_n}\right) = 1$.*

Démonstration. (i) Soient m et n des entiers tels que $m \geqslant 1$, $n \geqslant 1$, $(m, n) = 1$ et $l \nmid mn$; vu la proposition 17, α_m et α_n sont non nuls et on a

$$(\alpha_m, \alpha_n) = (\alpha_1\beta_m, \alpha_1\beta_n) = (\alpha_1, \beta_n)(\beta_m, \alpha_1)(\beta_m, \beta_n) = (\alpha_1, \alpha_n)(\alpha_m, \alpha_1)(\beta_m, \beta_n),$$

d'où $(\beta_m, \beta_n) = 1$.

(ii) Nous raisonnerons par récurrence sur n. Pour $n = 1$, on a $\beta_n = 1$ et la propriété est immédiate. Il reste à montrer que si $n > 1$ est un entier tel que $l \nmid n$ et que la propriété soit vérifiée par tous les entiers de l'intervalle $[1, n-1]$ qui ne sont pas divisibles par l, n possède également la propriété.

Soit $m \geqslant 1$ un entier tel que $(m, n) = 1$. Soit r le reste de la division de m par n ; on a

$$1 \leqslant r < n, \quad 1 \leqslant n-r < n, \quad (r, n) = 1 \quad \text{et} \quad (n-r, n) = 1.$$

Si r n'est pas divisible par l, on a, vu (i) et la proposition 34,

$$\left(\frac{\beta_m}{\beta_n}\right) = \left(\frac{\beta_r}{\beta_n}\right) = (\beta_n, \beta_r)\left(\frac{\beta_n}{\beta_r}\right) = 1.$$

Si r est divisible par l, $n-r$ ne l'est pas et vu (i) et la proposition 34, on a

$$\left(\frac{\beta_m}{\beta_n}\right) = \left(\frac{\beta_r}{\beta_n}\right) = \left(\frac{\beta_{n-r}}{\beta_n}\right) = (\beta_n, \beta_{n-r})\left(\frac{\beta_n}{\beta_{n-r}}\right) = 1.$$

Ainsi n possède la propriété. ∎

THÉORÈME 1. *Supposons $l \geqslant 5$. Les propriétés suivantes sont deux à deux équivalentes:*

(i) *a est divisible par l^2 ou congru à 1 ou -1 modulo l.*

(ii) *Pour tous m et n entiers tels que $m \geqslant 1$, $n \geqslant 1$ et $l \nmid mn$, $[\alpha_m, \alpha_n] = 0$.*

(iii) *Pour tous m et n entiers tels que $m \geqslant 1$, $n \geqslant 1$, $l \nmid mn$ et $(m, n) = 1$, $[\alpha_m, \alpha_n] = 0$.*

(iv) *Pour tous m et n entiers de l'intervalle $[1, l^2-l-1]$ tels que $l \nmid mn$, $[\alpha_m, \alpha_n] = 0$.*

(v) *Pour tous m et n entiers de l'intervalle $[1, l^2-l-1]$ tels que $l \nmid mn$ et que $(m, n, l-1) = 1$, $[\alpha_m, \alpha_n] = 0$.*

Démonstration. Supposons (i) vérifiée et soient m et n des entiers $\geqslant 1$ tels que $l \nmid mn$. Si a est divisible par l^2,

$$[\alpha_m, \alpha_n] = [a^m-\zeta^m, a^n-\zeta^n] = [-\zeta^m, -\zeta^n] = 0.$$

Si a est congru à 1 ou -1 modulo l, f vaut 1 ou 2 et, vu la proposition 29, on a $[\alpha_m, \alpha_n] = 0$. Ainsi (ii) est vérifiée et (i) implique (ii).

Il est clair que (ii) implique (iii).

Montrons que (iii) implique (i). Nous raisonnerons par l'absurde en supposant que (iii) est vérifiée et que (i) ne l'est pas.

On a $[\alpha_1, \alpha_{l^2-l-1}] = 0$ et, vu la proposition 38, a est hyperprimaire; comme (i) n'est pas vérifiée, on a $f \geqslant 3$; d'où $|a| \geqslant 2$.

Soit p un nombre premier tel que $p \equiv fl-1$ (fl^2) dont l'existence résulte du théorème de Dirichlet; on a

$$p^{l-1} \equiv 1+fl \ (l^2),$$

ce qui montre que p n'est pas hyperprimaire.

Vu la proposition 36, on a

$$(\alpha_1, \alpha_p)^{p-1} = \zeta^u \prod_{i=1}^{p-1} \left(\frac{\beta_i}{\beta_p}\right) \quad \text{avec } u = pq(p)\frac{(a^p-a)}{(a-1)(a^p-1)}.$$

Vu la proposition 39, chacun des $\left(\frac{\beta_i}{\beta_p}\right)$ vaut 1 ; ainsi u est nul, $q(p)$ est divisible par l, p est hyperprimaire, ce qui est absurde.

Ainsi (iii) entraîne (i) et les propriétés (i), (ii) et (iii) sont deux à deux équivalentes.

Il est clair que (ii) entraîne (iv) et que (iv) entraîne (v) ; pour conclure, il suffira de montrer que (v) entraîne (ii).

Supposons (v) vérifiée. On a $[\alpha_1, \alpha_{l^2-l-1}] = 0$ et vu la proposition 38, (i) est vérifiée ou a est hyperprimaire ; comme (i) implique (ii), on peut supposer a hyperprimaire. Soient m et n des entiers $\geqslant 1$ tels que $l \nmid mn$ et que $(m, n) = 1$ et soient m' et n' les restes de division de m et n par l^2-l ; on a $(m', n', l-1) = (m, n, l-1) = 1$ et vu la proposition 26, on a $[\alpha_m, \alpha_n] = [\alpha_{m'}, \alpha_{n'}] = 0$.

Ainsi (iii) est vérifiée, donc (ii) l'est. ∎

On a déjà remarqué que pour $l = 3$ et $a = 4$, $(\alpha_1, \alpha_5) = \zeta^2$, le théorème précédent ne peut donc pas être étendu au cas $l = 3$.

7. Le système *S*. Dans la suite, nous ferons usage des notations suivantes :

e est un entier $\geqslant 1$ non divisible par l,

I ou $I(l, e)$ est l'ensemble des entiers de l'intervalle $[1, el]$ qui ne sont pas divisibles par l,

J ou $J(l, e)$ est l'ensemble $I \times I$,

S ou $S(l, e)$ est le système d'équations linéaire et homogène à coefficients dans F_l qui a pour inconnues les x_{mn} pour (m, n) dans J et pour équations celles des six familles suivantes où les indices qui dépassent el sont à remplacer par leurs restes de division par el.

(1) Pour $(m, n) \in J$, $x_{mn} + x_{nm} = 0$.

(2) Pour $(m, n) \in J$, $x_{m,el-n} = x_{mn}$.

(3) Pour $(m, n) \in J$ et $k \in I$ tel que $k \equiv 1$ (e), $x_{km,km} = kx_{mn}$.

(4) Pour $(m, n) \in J$ tel que $l \nmid m+n$, $x_{mn} = x_{m,m+n} + x_{m+n,n}$.

(5) Pour $(m, n) \in J$ tel que $e \nmid n$, $\sum_{\substack{i=0 \\ l \nmid n+ie}}^{l-1} x_{m,n+ie} = 0$.

(6) Pour g, h, m, n entiers tels que $g \geqslant 1$, $h \geqslant 1$, $e = gh$ et $(m, gn) \in J$

$$x_{m,gn} = \sum_{i=0}^{g-1} x_{m,n+ihl}.$$

PROPOSITION 40. *Supposons a hyperprimaire. La famille $([\alpha_m, \alpha_n])_{(m,n)\in J(l,f)}$ est solution du système $S(l, f)$.*

Démonstration. Il résulte de la proposition 19 que cette famille est bien définie; les équations (1) de $S(l, f)$ sont vérifiées en vertu de (R15); les équations (2) et (6) sont vérifiées en vertu des propositions 27 et 31 respectivement ; enfin, compte tenu de la proposition 26, les équations (3), (4) et (5) sont vérifiées en vertu des propositions 32, 33 et 30 respectivement.

PROPOSITION 41. *Soit $(x_{mn})_{(m,n)\in J}$ une solution du système S.*

(i) *Pour tout m de I, $x_{mm} = 0$.*

(ii) *Les propriétés suivantes sont deux à deux équivalentes :*

(a) *pour tous m et n de I tels que $m \equiv 1$ (e) et que $n \equiv 0$ (e), $x_{mn} = 0$,*

(b) *pour tous m et n de I tels que $m \equiv n \equiv 1$ (e), $x_{mn} = 0$,*

(c) *pour tous m, n, n' de I tels que $m \equiv 1$ (e) et que $n \equiv n' \equiv 0$ (e), $x_{mn} = x_{mn'}$.*

Démonstration. (i) Les équations (1) donnent $2x_{mm} = 0$; d'où $x_{mm} = 0$.

(ii) Supposons (a) vérifiée. Soient m et n des éléments de I tels que $m \equiv n \equiv 1$ (e) et que $m > n$; vu les équations (4) et (1), on a $x_{m-n,n} = x_{m-n,m} + x_{mn}$, $x_{mn} = x_{m,m-n} - x_{n,m-n}$, d'où $x_{mn} = 0$ et (a) entraîne (b).

Supposons (b) vérifiée. Soit $r \geqslant 0$ un entier tel que $r \equiv 1$ (e) et que $r \equiv 0$ (l). Pour $i = 1, \ldots, l-2$, on a, vu les équations (4), $x_{r+ie,e} = x_{r+ie,r+(i+1)e} + x_{r+(i+1)e,e}$, d'où $x_{r+ie,e} = x_{r+(i+1)e,e}$.

Ainsi, pour $j = 1, \ldots, l-1$, les $x_{r+je,e}$ sont égaux entre eux et, vu les équations (1) et (5), on a $\sum_{j=1}^{l-1} x_{r+je,e} = 0$; pour tout j entier de l'intervalle $[1, l-1]$, on a $(l-1)x_{r+je,e} = 0$, d'où $x_{r+je,e} = 0$.

Ainsi, pour tout m de I tel que $m \equiv 1$ (e), on a $x_{me} = 0$; si k est un entier tel que k soit dans I et que $k \equiv 1$ (e), on a, en vertu des équations (3), $x_{km,ke} = 0$; d'où, pour les mêmes m et k, $x_{m,ke} = 0$. Ainsi, (a) est vérifiée et (b) entraîne (a).

Supposons (c) vérifiée. Soit i un entier de l'intervalle $[1, l-1]$ tel que $1+ie$ ne soit pas divisible par l; vu les équations (1) et (4), on a $x_{1,1+ie} = x_{1,ie} - x_{ie+1,ie}$ et vu (c) et les équations (3), on a

$$x_{1,1+ie} = x_{1,ie} - x_{ie+1,(ie+1)e} = x_{1e} - (ie+1)x_{1e} = -iex_{1e}.$$

Vu les équations (5) et ce qui précède, on a

$$\sum_{\substack{i=0 \\ l \nmid 1+ie}}^{l-1} x_{1,1+ie} = 0, \quad \left(\sum_{i=0}^{l-1} -ie\right)x_{1e} = x_{1e},$$

d'où $x_{1e} = 0$; d'où $x_{1m} = 0$ pour tout m de I divisible par e; d'où, pour k dans I tel que $k \equiv 1$ (e), $x_{k,km} = 0$ en vertu des équations (3) ; ainsi (a) est vérifiée et (c) entraîne (a).

Comme il est clair que (a) entraîne (c), les propriétés (a), (b), (c) sont deux à deux équivalentes.

DÉFINITION. Nous dirons que le couple (l, e) *possède la propriété* P si toute solution $(x_{mn})_{(m,n)\in J}$ du système $S(l, e)$ qui appartient à F_l^J et qui vérifie $x_{mn} = 0$

pour tout (m, n) de J tel que $m \equiv 1$ (e) et que $n \equiv 0$ (e) est telle que $x_{uv} = 0$ pour tout élément (u, v) de J tel que $(u, v, e) = 1$. Nous dirons que l possède la propriété P si pour tout diviseur $d \geqslant 1$ de $l-1$, le couple (l, d) possède la propriété P.

ENONCÉ 6. (i) *Les systèmes $S(l, 1)$ et $S(l, 2)$ ont pour seule solution la solution nulle.*

(ii) *Lorsqu'on suppose $l \equiv 1$ (e) et que e ait l'une des valeurs* 1, 2, 3, 4, 5, 6, 8, 12, *le couple (l, e) possède la propriété* P.

Les équations (1), (2) et (3) suffisent à démontrer (i), ce qui prouve (ii) pour $e = 1$ et $e = 2$; notre démonstration de (ii) est très simple pour $e = 3$ et $e = 4$ et plus délicate pour les autres valeurs de e. La proposition 41 et l'énoncé 6 contiennent malheureusement l'essentiel de nos connaissances sur le système S et la propriété P.

8. La propriété LC.

PROPOSITION 42. *Supposons $l \geqslant 5$ et considérons les propriétés:*

(i) *a est congru à* 0, 1 *ou* -1 *modulo l^2,*

(ii) *α_1 est orthogonal à tout élément de ΛU,*

(iii) *α_1 est orthogonal à tout élément de Λ,*

(iv) *α_1 est orthogonal à tout élément de C,*

(v) *α_1 est orthogonal à chacun de ses conjugués,*

(vi) *a est divisible par l^2 ou hyperprimaire.*

La propriété (i) *entraîne* (ii) ; (ii) *entraîne* (iii), (iv) *et* (v) ; (iii), (iv) *et* (v) *sont deux à deux équivalentes et chacune d'entre elles entraîne* (vi).

Démonstration. Si (i) est vérifiée, α_1 est congru modulo l^2 à λ où à un élément de C et, par suite, est congru modulo λ^{l+3} à λ ou à un élément de U ; il résulte alors de (R10) à (R13) et de (R32) que α_1 est orthogonal à λ et à tout élément de U et comme ΛU est engendré par Λ et U, α_1 est orthogonal à tout élément de ΛU. Ainsi (i) entraîne (ii).

Il est clair que (ii) entraîne (iii) et que (iii) entraîne (iv).

Supposons (iii) vérifiée et soient m et m' des entiers de l'intervalle $[2, l-1]$ tels que $mm' \equiv 1$ (l), on a

$$[a-\zeta,\ a-\zeta^m] = [a-\zeta,\ \zeta^m-\zeta]+[\zeta^m-\zeta,\ a-\zeta^m]$$
$$= [\zeta^m-\zeta,\ a-\zeta^m] = m[\zeta-\zeta^{m'},\ a-\zeta] = 0.$$

Ainsi (iii) entraîne (v). Par suite, (ii) entraîne (iii), (iv) et (v).

Si (iv) est vérifiée, α_1 est orthogonal à ζ et, vu la proposition 37, (vi) est vérifiée ; ainsi (iv) entraîne (vi). Si (v) est vérifiée, α_1 est orthogonal à sa norme et, vu la proposition 37, (vi) est vérifiée; ainsi (v) entraîne (vi). Par suite, chacune des propriétés (iii), (iv) et (v) entraîne (vi).

Il reste à montrer l'équivalence de (iii), (iv) et (v) et, vu ce qui précède, on peut se restreindre au cas où a est hyperprimaire. Les propriétés (iii), (iv) et (v) s'expriment alors en termes de la famille $([\alpha_m, \alpha_n])_{(m,n)\in J(l,f)}$ qui, en vertu de la proposition 40, est une solution du système $S(l, f)$.

En effet, (iii) équivaut à $[\alpha_1, 1-\zeta^m] = 0$ pour tout m de $I(l, f)$ divisible par f, ce qui, vu la proposition 19 équivaut à $[\alpha_1, \alpha_m] = 0$ pour les mêmes m ; vu les équations (3) du système $S(l, f)$, cette dernière condition équivaut à $[\alpha_m, \alpha_n] = 0$ pour toŭs m et n de $I(l, f)$ tels que $m \equiv 1$ (f) et que $n \equiv 0$ (f).

De même, (iv) équivaut à $[\alpha_1, 1-\zeta^m] = [\alpha_1, 1-\zeta^n]$ pour tous m et n de $I(l, f)$ divisibles par f, ce qui, vu la proposition 19, équivaut à $[\alpha_1, \alpha_m] = [\alpha_1, \alpha_n]$ pour les mêmes m et n ; vu les équations (3), cette dernière condition équivaut à $[\alpha_m, \alpha_n] = [\alpha_m, \alpha_{n'}]$ pour tous m, n, n' de $I(l, f)$ tels que $m \equiv 1$ (f) et que $n \equiv n' \equiv 0$ (f).

De même, (v) équivaut à $[\alpha_1, a-\zeta^m] = 0$ pour tout m de $I(l, f)$ tel que $m \equiv 1$ (f), ce qui, vu la proposition 21, équivaut à $[\alpha_1, \alpha_m] = 0$ pour les mêmes m ; ce qui, vu les équations (3), équivaut à $[\alpha_m, \alpha_n] = 0$ pour tous m et n de $I(l, f)$ tels que $m \equiv n \equiv 1$ (f).

L'équivalence de (iii), (iv) et (v) résulte alors de la proposition 41.

DÉFINITION. Nous dirons que l *possède la propriété* LC si les deux propriétés suivantes sont équivalentes :

(i) a est congru à 0, 1 ou -1 modulo l^2.

(ii) α_1 est orthogonal à tout élément de C.

Nous avons baptisé LC cette propriété parce que, lorsqu' elle est vérifiée, elle constitue une sorte de loi complémentaire à la loi de réciprocité des puissances l-èmes. Pour $l = 3$, on a $7-\zeta = \lambda(5+2\zeta)$ et $(7-\zeta, \zeta) = 1$ et $7-\zeta$ est orthogonal à tout élément de C ; par suite, 3 ne possède pas la propriété LC. Si $l \geqslant 5$ possède la propriété LC, les propriétés (i) à (v) de la proposition précédente sont deux à deux équivalentes.

PROPOSITION 43. (i) *Supposons $l \geqslant 5$, $l \nmid a$, $f \geqslant 3$ et que le couple (l, f) possède la propriété* P, *alors il existe un élément de C auquel α_1 n'est pas orthogonal.*

(ii) *Tout nombre premier $\geqslant 5$ qui possède la propriété* P *possède la propriété* LC.

Démonstration. (i) On raisonne par l'absurde en supposant $l \geqslant 5$, $l \nmid a$, $f \geqslant 3$, que (l, f) possède la propriété P et que α_1 soit orthogonal à tout élément de C. Vu la proposition précédente, a est hyperprimaire et α_1 est orthogonal à tout élément de Λ. Vu la proposition 40, la famille $([\alpha_m, \alpha_n])_{(m,n)\in J(l,f)}$ est une solution de $S(l, f)$. On a $[\alpha_1, 1-\zeta^m] = 0$ pour tout m de $I(l, f)$ divisible par f; d'où $[\alpha_1, \alpha_m] = 0$ pour les mêmes m ; d'où, vu les équations (3), $[\alpha_m, \alpha_n] = 0$ pour tous m et n de $I(l, f)$ tels que $m \equiv 1$ (f) et que $n \equiv 0$ (f). Puisque le couple (l, f) possède la propriété P, on a $[\alpha_m, \alpha_n] = 0$ pour tout (m, n) de $J(l, f)$ tel que $(m, n, f) = 1$. Soient m et n des entiers $\geqslant 1$ tels que $(m, n) = 1$ et que

$l \nmid mn$; si m' et n' sont leurs restes de division par fl, on a $(m', n', f) = 1$ et (m', n') appartient à $I(l, f)$; vu la proposition 26, on a $[\alpha_m, \alpha_n] = [\alpha_{m'}, \alpha_{n'}] = 0$. La propriété (iii) du théorème 1 est vérifiée et vu ce théorème, a est congru à 1 ou -1 modulo l; par suite, f vaut 1 ou 2 ; ce qui est absurde.

(ii) Supposons que $l \geqslant 5$ possède la propriété P. Si a est congru à 0, 1 ou -1 module l^2, α_1 est orthogonal à tout élément de C, en vertu de la proposition précédente. Inversement, supposons α_1 orthogonal à tout élément de C; en vertu de la proposition précédente, a est divisible par l^2 ou hyperprimaire; si a est hyperprimaire, le couple (l, f) possède la propriété P, puisque f divise $l-1$ et, vu (i), on a $f = 1$ ou $f = 2$ et vu la proposition 18, a est congru à 1 ou à -1 module l^2. Ainsi, l possède la propriété LC; d'où le résultat.

Introduisons des notations conformes à celles de Frobenius [1], mais non cohérentes avec ce qui précède :

la suite $(b_n)_{n \geqslant 0}$ des nombres de Bernoulli est définie par la relation

$$\frac{X}{e^X - 1} = \sum_{n=0}^{+\infty} \frac{b_n}{n!} X^n$$

et la suite $(f_n)_{n \geqslant 1}$ des polynômes de Mirimanoff est définie par la relation

$$f_n = \sum_{r=0}^{l-1} r^{n-1} X^r.$$

ENONCÉ 7. *Supposons $a \not\equiv 1$ (l), les propriétés suivantes sont équivalentes:*

(i) *α_1 est orthogonal à tout élément de Λ.*

(ii) *On a $[\alpha_1, \lambda] = 0$ et pour tout entier $n = 1, \ldots, l-2$, on a*

$$b_n l_{l-n}(\alpha_1) = 0.$$

(iii) *On a les congruences*

$$a^l \equiv a \ (l^2),$$

$$(a+1) f_{l-1}(a) \equiv 0 \ (l)$$

et pour tout entier pair n tel que $2 \leqslant n \leqslant l-3$, on a

$$b_n f_{l-n}(a) \equiv 0 \ (l).$$

La démonstration est essentiellement celle que Hasse utilise aux pages 118 et 119 de son traité [4] pour obtenir ce qu'il appelle le critère de Kummer.

ENONCÉ 8. *Si $l \geqslant 5$ ne possède pas la propriété* LC, *on a*

$$2^{l-1} \equiv 1 \ (l^2) \quad \text{et} \quad b_{l-3} \equiv 0 \ (l).$$

Cela se démontre à partir de l'énoncé précédent en se servant des arguments de Mirimanoff [9].

ENONCÉ 9. *Tout nombre premier de l'intervalle $[5, 6 \cdot 10^9]$ possède la propriété* LC.

En effet, il résulte des calculs de D. H. Lehmer [7] que les seuls nombres premiers $l \leqslant 6 \cdot 10^9$ qui vérifient $2^{l-1} \equiv 1 \ (l^2)$ sont 1093 et 3511 et il résulte des tables de nombres premiers irréguliers dont la dernière est celle de Wagstaff [16] que pour ces deux nombres, on a $b_{l-3} \not\equiv 0 \ (l)$.

Les énoncés qui précèdent me conduisent à conjecturer que tout nombre premier $\geqslant 5$ possède la propriété LC.

9. Le théorème de Fermat.

PROPOSITION 44. *Soient x, y, z des entiers relatifs tels qu'on ait $(x, y) = 1$ et $l \nmid y$ et $B_l(x, y) = z^l$; on a $x \not\equiv y$ (l), tout diviseur de y est hyperprimaire et $x - y\zeta$ est orthogonal à tout élément de ΛU.*

Démonstration. Supposons $x \equiv y \ (l)$; vu la proposition 1, on a $B_l(x, y) \equiv l y^{l-1} \ (l^2)$; ainsi $B_l(x, y)$ est divisible par l, mais non par l^2, ce qui est absurde puisque $B_l(x, y)$ est une puissance l-ème. Ceci montre qu'on a $x \not\equiv y \ (l)$.

On a

$$\prod_{i=1}^{l-1} (x - y\zeta^i) = z^l.$$

Le nombre z est non nul et, puisqu'on a $x \not\equiv y \ (l)$, les nombres $x - y\zeta^i$ pour $i = 1, \ldots, l-1$ sont premiers entre eux ; par suite, pour tout entier i de l'intervalle $[1, l-1]$, il y a un idéal non nul $\mathfrak{a}_i$ de A tel qu'on ait

$$(x - y\zeta^i) = \mathfrak{a}_i^l.$$

Soit d un diviseur de y. Si x est nul, y vaut 1 ou -1 et d est hyperprimaire. Si x est non nul, posons

$$\alpha = x\zeta^y - y\zeta^x = \zeta^y (x - y\zeta^{x-y}),$$

vu ce qui précède, il y a un idéal non nul $\mathfrak{a}$ de A tel que $(\alpha) = \mathfrak{a}^l$; on a aussi $(\alpha, d) = (x\zeta^y, d) = (1)$ et on a

$$\alpha = x(1-\lambda)^y - y(1-\lambda)^x \equiv x - y \ (\lambda^2).$$

D'où $(\alpha, d) = 1$ et, par suite,

$$\left(\frac{\alpha}{d}\right) = \left(\frac{d}{\alpha}\right) = \left(\frac{d}{\mathfrak{a}^l}\right) = \left(\frac{d}{\mathfrak{a}}\right)^l = 1.$$

On a aussi

$$\left(\frac{\alpha}{d}\right) = \left(\frac{x\zeta^y - y\zeta^x}{d}\right) = \left(\frac{x\zeta^y}{d}\right) = \left(\frac{\zeta}{d}\right)^y.$$

D'où $\left(\frac{\zeta}{d}\right) = 1$ et $(d, \zeta) = 1$ et d est hyperprimaire.

Soit μ un élément de ΛU, on a

$$(x-y\zeta,\ \mu)=\left(\frac{\mu}{x-y\zeta}\right)=\left(\frac{\mu}{a_1^l}\right)=\left(\frac{\mu}{a_1}\right)^l=1.\ \blacksquare$$

PROPOSITION 45. *Supposons $l\geqslant 5$ et soient x, y, z des entiers relatifs tels qu'on ait $(x,\ y)=1$ et $B_l(x,\ y)=z^l$.*

(i) *Si $r\geqslant 3$ est un diviseur de $l-1$ tel que le couple (l, r) possède la propriété* P, $C_r(x,\ y)\not\equiv 0\ (l)$.

(ii) *Si l possède la propriété* LC, *l'un des nombres x, y, $x+y$ est divisible par l^2.*

Démonstration. On peut supposer que y n'est pas divisible par l. Soit u un entier relatif tel qu'on ait $x\equiv yu\ (l^2)$. Vu la proposition précédente, on a $u\not\equiv 1\ (l)$, y est hyperprimaire et $x-y\zeta$ est orthogonal à tout élément de C. Par suite, $yu-y\zeta$ est orthogonal à tout élément de C et $u-\zeta$ est orthogonal à tout élément de C.

(i) Raisonnons par l'absurde en supposant que $r\geqslant 3$, que r divise $l-1$, que (l, r) possède la propriété P et que $C_r(x,\ y)\equiv 0\ (l)$. Alors $C_r(yu,\ y)$ est divisible par l ; donc l divise $c_r(u)$; en vertu du (iii) de la proposition 18, r est le plus petit des entiers $k\geqslant 1$ tels que $u^k\equiv 1\ (l)$. Vu la proposition 43, il existe un élément de C auquel $u-\zeta$ n'est pas orthogonal; ce qui est absurde.

(ii) Puisque l possède la propriété LC, u est congru à 0, 1 ou -1 modulo l^2 ; par suite, u est congru à 0 ou -1 modulo l^2 et x ou $x+y$ est divisible par l^2. $\blacksquare$

THÉORÈME 2. *Supposons que $l\geqslant 5$ possède la propriété* LC *et soient x, y, z des entiers relatifs tels que $x^l+y^l+z^l=0$, l'un des nombres x, y, z est divisible par l^3.*

Démonstration. On peut supposer x, y, z premiers entre eux, ils sont alors deux à deux premiers entre eux. Supposons d'abord qu'aucun de x, y, z ne soit divisible par l, on a

$$(x+y)B_l(x,\ -y)=-z^l$$

et comme $x+y$ et $B_l(x,\ -y)$ sont premiers entre eux, il y a un entier u tel que $B_l(x,\ -y)=u^l$. La proposition précédente nous donne $x-y\equiv 0\ (l^2)$ et, par symétrie, on a $x\equiv y\equiv z\ (l^2)$; d'où $3x^l\equiv 0\ (l^2)$; ainsi x est divisible par l, ce qui est absurde.

L'un des nombres x, y, z est divisible par l et le théorème de Vandiver, c'est-à-dire le théorème 1046 de [6] permet de conclure.

ENONCÉ 10. *Supposons $l\geqslant 5$ et soient x, y, z des entiers relatifs tels que $(x,\ y,\ z)=1$, que $l\nmid z$ et que $x^l+y^l+z^l=0$, on a $C_n(x,-y)\not\equiv 0\ (l)$ pour $n=3,\ 4,\ 5,\ 6,\ 8$ et 12.*

Cela résulte de la proposition 45 et de l'énoncé 6. Les cas $n=3,\ 4,\ 6$ du résultat ci-dessus ont déjà été obtenus par Pollaczek [14] et Morishima [12] dont les démonstrations difficiles et peut-être incomplètes ont été reprises par Gunderson [3] et Granville [2] dans leurs thèses, tandis que les cas $n=5,\ 8,\ 12$ sont nouveaux.

Bibliographie

[1] F. G. Frobenius, *Über den Fermatschen Satz III*, Sitzungsber. K. Pr. Akad. Wiss. Berlin. (1914), 653–681 et aussi Ges. Abh., Bd. III, 648–676.

[2] A. J. Granville, *Diophantine equations with varying exponents*, Thèse, Queen's University, Kingston, Ontario, 1987, non publiée.

[3] N. Gunderson, *Derivation of criteria for the first case of Fermat's last theorem and the combination of these criteria to produce a new lower bound for the exponent*, Thèse, Cornell University, 1948, non publiée.

[4] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II, Reziprozitätsgesetz. Ergänzungsband 6 zum Jahresbericht der D.M.V., (1930), IV+204 pages, Réimpression Physica-Verlag, Würzburg, 1970.

[5] W. Klösgen, *Untersuchungen über die Fermatsche Kongruenzen*, Gesell. f. Math. und Datenverarbeitung. n° 36, Bonn 1970, 124 pages.

[6] E. Landau, *Vorlesungen über Zahlentheorie*, Chelsea, New-York 1969.

[7] D. H. Lehmer, *On Fermat's quotient, base two*, Math. Comp. 36 (1981), 289–290.

[8] D. Mirimanoff, *Sur l'équation* $(x+1)^l-x^l-1=0$, Nouv. Annales de Math., 4^e série, 3 (1903), 385–397.

[9] — *Sur le dernier théorème de Fermat et le critérium de M.A. Wieferich*, L'enseignement mathématique 11 (1909), 455–459.

[10] H. Möller, *Über die i-ten Koeffizienten der Kreisteilungspolynome*, Math. Ann. 188 (1970), 26–38.

[11] — *Über die Koeffizienten des n-ten Kreisteilungspolynoms*, Math. Z. 119 (1971), 33–40.

[12] T. Morishima, *Über den Fermatschen Quotienten*, Japan. J. Math. 8 (1931), 159–173.

[13] E. Netto, *Notiz über die Kreisteilungs-Polynome*, Arch. Math. Physik, 3^e série, 4 (1903), 65–67.

[14] F. Pollaczek, *Über den grossen Fermatschen Satz*, Sitzungsber. K. Akad. Wiss. Wien, Abt. II A, 126 (1917), 45–59.

[15] B. Richter, *Die Primfaktorzerlegung der Werte der Kreisteilungspolynome*, II, J. für Math. 267 (1974), 77–89.

[16] S. S. Wagstaff, *The irregular primes to* 125000, Math. Comp. 32(142) (1978), 583–591.

U.F.R. DE MATHÉMATIQUES
UNIVERSITÉ PAUL SABATIER
118 route de Narbonne
31062 Toulouse Cédex
France

Reçu le 26.11.1987
et dans la forme modifiée le 13.7.1988 (1568)